DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,202,156

EXHIBIT E

US7917444B1 ("Bursch '444"), WO2003015043A1 ("Codron '043"), US20060165060A1 ("Dua '060"), US6636833B1 ("Flitcroft '833"), JP2004295365A("Hanada '365"), US20010013542A1 ("Horowitz '542"), KR20000036744A ("Jo '744"), US5418837A ("Johansson '837"), US20080194200A1 ("Keen '200"), US20070057073A1 ("Mamba '073"), JP2000115373A ("Oishi '373"), Contactless Payments ("SCAR PT-04002"), US20050187882A1 ("Sovio '882"), US20050015275A1 ("Takekawa '275"), i-mode FeliCa ("Yoshinaga 2004"), and US20050097038A1 ("Yu '038")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under 35 U.S.C. § 103 as obvious over each of Bursch '444, Codron '043, Dua '060, Flitcroft '833, Hanada '365, Horowitz '542, Jo '744, Johansson '837, Keen '200, Mamba '073, Oishi '373, SCAR PT-04002, Sovio '882, Takekawa '275, Yoshinaga 2004, and Yu '038 and (b) under 35 U.S.C. § 103(a) as obvious over Bursch '444, Codron '043, Dua '060, Flitcroft '833, Hanada '365, Horowitz '542, Jo '744, Johansson '837, Keen '200, Mamba '073, Oishi '373, SCAR PT-04002, Sovio '882, Takekawa '275, Yoshinaga 2004, and Yu '038 combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations**
1[pre]. A mobile device comprising:	Bursch '444 at Fig.4A–B, 2:60–61, 7:50–54, and 8:37–42. Codron '043 at Abstract, 2:19–3:10, 4:1–18, 4:19–27, 5:4–23, 6:5–8, 6:19–20, 8:6–10, Fig. 1, and Fig. 2. Dua '060 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 5, Fig. 6A–B, Fig. 7A–B, [0023], [0026], [0038], [0039], [0041], [0046], [0048], [0053], [0057], [0126], [0128], [0179], [0288], [0293], [0295], [0315], [0317], [0392], [0417], [0433], claim 1, claim 50, claim 79, and claim 92.

Patent Owner's Ex. 2020
Samsung v. iCashe (IPR2025-00643)
Page 001

Claim Element	Exemplary Citations
	Flitcroft ’833 at Fig. 1, 9:40–63, and 18:25–37. Hanada ’365 at [0007], [0008], [0012], [0013], [0014], and [0019]. Horowitz ’542 at Figure 2, [0025], [0027], claim 8, claim 14, and claim 15. Jo ’744 at Abstract, 3, 4, 5, and 14. Johansson ’837 at Abstract, Fig 1.a, Fig. 2A, Fig. 3, 1:6–12, 2:30–41, 2:42–49, 2:50–57, 3:34–46, 4:34–50, 5:15–30, 5:31–42, 6:29–42, 8:25–27, 9:40–42, and 10:30–32. Keen ’200 at Abstract, Fig. 1, Fig. 7, [0004], [0026], [0101], [0102], [0103], [0104], and claim 22. Mamba ’073 at Abstract, Fig. 1A, Fig. 1B, [0007], [0015], [0016], [0021], [0022], [0041], and [0048]. Oishi ’373 at [0001], [0014], [0036], [0037], Fig. 4, and Fig. 5. SCAR PT-04002 at 6, PayPass Figure (p. 8), 8, ExpressPay Figure (p. 9), Table 1, and 13. Sovio ’882 at Abstract, Fig. 1, Fig. 2, [0004], [0010], [0011], [0012], [0013], [0016], [0020], [0021], [0040], [0041], [0043], [0044], and [0073]. Takekawa ’275 at Abstract, Fig. 1, Fig. 2, Fig. 5, Fig. 7, Fig. 9, Fig. 11, Fig. 13, Fig. 15, FIg. 16, Fig. 25, [0002], [0017], [0018], [0023], [0025], [0027], [0029], [0031], [0033], [0035], [0037], [0043], [0047], [0048], [0051], [0053], [0055], [0057], [0059], [0061], [0062], [0066], [0072], [0081], [0082], [0083], [0084], [0085], [0086], [0087], [0098], [0102], [0103], [0104], [0105], [0107], [0108], [0112], [0114], [0129], [0130], [0131], [0140], [0161], [0163], claim 1, claim 2, claim 3, claim 14, and claim 20. Yoshinaga 2004 at 24, Figure 1, and 26. Yu ’038 at Figure 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 17, Fig. 19, [0001], [0003], [0005], [0006], [0007], [0010], [0033], [0039], [0046], [0054]–[0056], [0077], [0090], [0091], claim 1, claim 7, claim 12, claim 14, claim 17, and claim 20.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Dua ’060 at Figure 8, [0009], [0011], [0013], [0016], [0290], [0291], [0293], [0315], [0317], [0318], [0336], [0353], [0354], [0382], [0392], [0395], [0405], [0417], [0433], and claim 20. Flitcroft ’833 at 8:11–29 and 10:26–56. Jo ’744 at 1, 2, 3, 6, and 14.

Claim Element	Exemplary Citations
	Keen ’200 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, [0002], [0003], [0012], [0013], [0026], [0028]–[0029], [0030], [0032], [0063], [0069], [0074], [0076], [0083], [0085], [0086], [0095], [0098], [0106], claim 1, claim 4, and claim 9. Mamba ’073 at [0001]. SCAR PT-04002 at 4, 7–8, PayPass Figure (p. 8), 8, ExpressPay Figure (p. 9), 9, 10, Table 1, 22, 23, 24, 37, 38, 39, and 40. Sovio ’882 at Abstract, Fig. 1, Fig. 2, [0010], [0017], [0020], [0041], [0043], [0045], [0049], [0073], and [0080]. Yoshinaga 2004 at 26–27. Yu ’038 at Fig. 2, Fig. 3, Fig. 4, Figure 18, Fig. 19, [0034], [0036], [0039], [0046], [0054]–[0056], [0093], [0096], [0097], and claim 20.
[1b] a memory to hold transaction data; and	Dua ’060 at [0041]. Flitcroft ’833 at 9:64–10:19. Hanada ’365 at [0007], [0009], and [0019]. Horowitz ’542 at Abstract, [0002], [0011], [0012], [0015], [0016], [0025], [0027], claim 1, claim 2, claim 3, claim 5, claim 6, claim 14, claim 15, claim 17, and claim 21. Jo ’744 at 1. Keen ’200 at [0028]–[0029], [0049], and [0084]. Oishi ’373 at [0029]. Sovio ’882 at [0045]. Yu ’038 at [0033].
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic	Dua ’060 at Figure 8, [0009], [0011], [0013], [0016], [0041], [0290], [0291], [0293], [0315], [0317], [0318], [0336], [0353], [0354], [0382], [0392], [0395], [0405], [0417], [0433], and claim 20. Flitcroft ’833 at 8:11–29 and 10:26–56.

Patent Owner's Ex. 2020
Page 003

Claim Element	Exemplary Citations
field that represents the transaction data;	Hanada ’365 at [0019]. Horowitz ’542 at [0012]. Jo ’744 at 1, 2, 3, 6, and 14. Keen ’200 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, [0002], [0003], [0012], [0013], [0015], [0026], [0028]–[0029], [0030], [0032], [0034], [0055], [0063], [0069], [0074], [0076], [0083], [0084], [0085], [0086], [0095], [0098], [0106], claim 1, claim 4, and claim 9. Mamba ’073 at Abstract, Fig. 2, [0001], [0011]–[0012], [0026], [0029], [0030], [0034], and [0041]. SCAR PT-04002 at 4, 7–8, PayPass Figure (p. 8), 8, ExpressPay Figure (p. 9), 9, 10, Table 1, 22, 23, 24, 37, 38, 39, and 40. Sovio ’882 at Abstract, Fig. 1, Fig. 2, [0010], [0017], [0020], [0041], [0043], [0045], [0048], [0049], [0073], and [0080]. Yoshinaga 2004 at 25 and 26–27. Yu ’038 at Fig. 2, Fig. 3, Fig. 4, Fig. 12, Fig. 13, Figure 18, Fig. 19, [0034], [0036], [0039], [0046], [0054]–[0056], [0093], [0096], [0097], claim 2, and claim 20.
[1d] wherein the mobile device comprises a mobile phone.	Bursch ’444 at Fig.4A–B, 2:60–61, 7:50–54, and 8:37–42. Codron ’043 at Abstract, 2:19–3:10, 4:1–18, 4:19–27, 5:4–23, 6:5–8, 6:19–20, 8:6–10, Fig. 1, and Fig. 2. Dua ’060 at Fig. 1, Fig. 2, Fig. 3, Fig. 5, Fig. 6A–B, Fig. 7A–B, [0023], [0026], [0039], [0041], [0046], [0048], [0053], [0057], [0126], [0128], [0179], [0295], [0315], [0317], [0417], [0433], claim 1, claim 44, claim 79, and claim 92. Flitcroft ’833 at 9:40–63 and 18:25–37. Hanada ’365 at [0014], [0017], and [0019]. Horowitz ’542 at Figure 2, Figure 3A, [0025], [0027], claim 14, and claim 21. Jo ’744 at Abstract, 3, 4, 5, and 14. Johansson ’837 at Abstract, Fig 1.a, Fig. 2A, Fig. 3, 1:6–12, 2:30–41, 2:42–49, 2:50–57, 3:34–46, 4:34–50, 5:15–30, 5:31–42, 6:29–42, 8:25–27, 9:40–42, and 10:30–32.

Claim Element	Exemplary Citations
	Keen ’200 at Fig. 7, [0004], [0026], [0101], [0102], [0103], and [0104]. Mamba ’073 at Abstract, Fig. 1A, Fig. 1B, [0001], [0007], [0015], [0016], [0021], [0022], [0022]–[0023], [0028], [0041], and [0048]. Oishi ’373 at [0001], [0014], [0036], [0037], Fig. 4, and Fig. 5. SCAR PT-04002 at 6, 8, Table 1, and 13. Sovio ’882 at Abstract, Fig. 1, Fig. 2, [0004], [0011], [0012], [0013], [0016], [0020], [0021], [0040], [0041], [0043], [0044], and [0073]. Takekawa ’275 at Abstract, Fig. 1, Fig. 2, Fig. 5, Fig. 7, Fig. 9, Fig. 11, Fig. 13, Fig. 15, FIg. 16, Fig. 25, [0002], [0017], [0018], [0023], [0025], [0027], [0029], [0031], [0033], [0035], [0037], [0043], [0047], [0048], [0051], [0053], [0055], [0057], [0059], [0061], [0062], [0066], [0072], [0081], [0082], [0083], [0084], [0085], [0086], [0087], [0098], [0102], [0103], [0104], [0105], [0107], [0108], [0112], [0114], [0129], [0130], [0131], [0140], [0161], [0163], claim 1, claim 2, claim 14, and claim 20. Yoshinaga 2004 at 24, Figure 1, and 26. Yu ’038 at Figure 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 17, Fig. 19, [0001], [0003], [0005], [0006], [0007], [0010], [0033], [0039], [0046], [0054]–[0056], [0077], [0090], [0091], claim 1, claim 12, claim 14, claim 17, and claim 20.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Dua ’060 at [0011], [0013], [0290], [0293], [0315], [0317], [0336], [0392], [0395], [0405], [0417], and claim 20. Flitcroft ’833 at 8:11–29 and 10:26–56. Horowitz ’542 at Figure 2, Figure 3A, and [0021]. SCAR PT-04002 at 7–8, 8, ExpressPay Figure (p. 9), 9, 10, Table 1, 22, 23, and 24. Yu ’038 at [0036] and [0046].
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Dua ’060 at [0293], [0422], claim 75, claim 88, and claim 89. Flitcroft ’833 at 8:35–39.

Patent Owner's Ex. 2020
Page 005

Claim Element	Exemplary Citations
	Horowitz ’542 at Abstract, Figure 2, Figure 3A, [0011], [0012], [0015], [0021], [0024], [0025], claim 1, claim 2, and claim 17. SCAR PT-04002 at 4 and 8. Yu ’038 at Fig. 12.
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Bursch ’444 at 7:55–8:3. Dua ’060 at [0293], [0422], claim 75, claim 88, and claim 89. Flitcroft ’833 at 4:59–5:4, 5:20–25, and 8:35–39. Horowitz ’542 at Abstract, Figure 2, Figure 3A, [0011], [0012], [0015], [0021], [0024], [0025], claim 1, claim 2, and claim 17. SCAR PT-04002 at 4 and 8. Yu ’038 at Fig. 12.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Codron ’043 at 4:19–27. Dua ’060 at [0007], [0295], and [0433]. Flitcroft ’833 at Fig. 1 and 10:26–56. Hanada ’365 at [0019]. Horowitz ’542 at Abstract, Figure 2, Figure 3A, [0002], [0003], [0007], [0011], [0012], [0015], [0016], [0025], claim 1, claim 3, claim 5, claim 6, claim 14, claim 15, and claim 21. Jo ’744 at Abstract, 1, 3, 4, 5, and 14. Johansson ’837 at Abstract, Fig 1.a, Fig. 1B, Fig. 2A, Fig. 2B, Fig. 3, 1:6–12, 2:30–41, 2:42–49, 2:50–57, 3:34–46, 3:47–62, 4:34–50, 4:51–5:3, 5:4–14, 5:15–30, 5:31–42, 6:17–28, 6:29–42, 6:58–68, 8:29–30, 9:28–32, 9:49–52, and 10:30–32. Keen ’200 at Abstract, Fig. 5, [0028]–[0029], [0046]–[0047], [0049], [0055], [0084], [0098], [0101], [0103], and claim 1.

Claim Element	Exemplary Citations
	Mamba ’073 at Abstract, Fig. 1A, Fig. 1B, Fig. 2, [0001], [0007], [0008], [0009], [0011]–[0012], [0016], [0021], [0022], [0026], [0027], [0029], [0034], [0041], and [0046]. Oishi ’373 at [0014], [0029], [0036], [0037], Fig. 4, and Fig. 5. SCAR PT-04002 at 4, Fig. 1., 7–8, 8, ExpressPay Figure (p. 9), 9, 11, and Table 1. Sovio ’882 at Abstract, Fig. 1, Fig. 2, Fig. 3, [0010], [0016], [0020], [0021], [0023], [0041], [0043], and [0045]. Takekawa ’275 at Abstract, Fig. 1, Fig. 2, Fig. 5, Fig. 7, Fig. 9, Fig. 10, Fig. 11, Fig. 12, Fig. 15, FIg. 16, Fig. 25, [0002], [0017], [0018], [0023], [0025], [0027], [0029], [0031], [0033], [0035], [0037], [0043], [0047], [0048], [0051], [0053], [0055], [0056], [0057], [0058], [0061], [0062], [0066], [0072], [0081], [0082], [0083], [0084], [0085], [0086], [0087], [0098], [0102], [0103], [0104], [0105], [0107], [0108], [0111], [0112], [0113], [0130], [0131], [0140], [0161], [0163], claim 1, claim 2, and claim 14. Yoshinaga 2004 at Abstract, 24, Figure 1, and 26. Yu ’038 at Figure 1, Fig. 2, Fig. 3, Fig. 4, Figure 16, Fig. 19, [0001], [0005], [0006], [0010], [0033], [0039], [0046], [0054]–[0056], [0060], [0077], claim 1, claim 8, claim 14, claim 17, and claim 20.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Dua ’060 at Figure 8, [0011], [0013], [0290], [0293], [0315], [0317], [0336], [0353], [0405], and [0433]. Flitcroft ’833 at 8:11–29 and 10:26–56. Jo ’744 at 2. SCAR PT-04002 at 4, 8, 10, Table 1, 22, 23, and 24. Sovio ’882 at [0010]. Yoshinaga 2004 at 25 and 26–27. Yu ’038 at Fig. 3, Fig. 4, [0034], and [0046].
9[pre]. A mobile device comprising:	*See* above at 1[pre].

Claim Element	Exemplary Citations
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	*See* above at [1a].
[9b] smartcard circuitry for performing transactions; and	Codron ’043 at 4:19–27. Dua ’060 at [0007], [0009], [0295], and [0433]. Flitcroft ’833 at Fig. 1 and 10:26–56. Horowitz ’542 at Abstract, Figure 2, Figure 3A, [0003], [0007], [0011], [0012], [0025], claim 1, claim 2, claim 3, claim 5, claim 6, claim 14, claim 15, and claim 21. Jo ’744 at Abstract, 1, 3, 4, 5, and 14. Johansson ’837 at Abstract, Fig 1.a, Fig. 1B, Fig. 2B, Fig. 3, 1:6–12, 2:30–41, 2:42–49, 2:50–57, 3:34–46, 3:47–62, 4:34–50, 4:51–5:3, 5:4–14, 5:15–30, 5:31–42, 6:17–28, 6:29–42, 8:29–30, 9:28–32, and 10:30–32. Keen ’200 at Abstract, Fig. 5, [0046]–[0047], [0084], [0101], [0103], and claim 1. Mamba ’073 at Abstract, Fig. 1A, Fig. 1B, Fig. 2, [0001], [0007], [0008], [0009], [0016], [0021], [0022], [0026], [0027], [0041], and [0046]. Oishi ’373 at [0014], [0036], [0037], Fig. 4, and Fig. 5. SCAR PT-04002 at 4, Fig. 1., 7–8, 8, ExpressPay Figure (p. 9), 9, 11, and Table 1. Sovio ’882 at Abstract, Fig. 1, Fig. 2, Fig. 3, [0010], [0016], [0020], [0023], [0041], and [0045]. Takekawa ’275 at Fig. 1, Fig. 2, Fig. 5, Fig. 7, Fig. 9, Fig. 10, Fig. 11, Fig. 15, FIg. 16, Fig. 25, [0002], [0017], [0018], [0023], [0025], [0027], [0029], [0031], [0033], [0035], [0037], [0043], [0047], [0048], [0051], [0053], [0055], [0056], [0057], [0058], [0061], [0062], [0066], [0072], [0081], [0082], [0083], [0084], [0085], [0086], [0087], [0098], [0102], [0103], [0104], [0105], [0107], [0108], [0111], [0112], [0113], [0130], [0131], [0140], [0161], [0163], claim 1, claim 2, and claim 14. Yoshinaga 2004 at Abstract, 24, 24–25, 25, Figure 1, and 26. Yu ’038 at Figure 1, Fig. 2, Fig. 3, Fig. 4, Figure 16, Fig. 19, [0001], [0005], [0006], [0010], [0033], [0036], [0039], [0046], [0054]–[0056], [0060], [0077], claim 1, claim 8, claim 14, claim 17, and claim 20.

Claim Element	Exemplary Citations
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Dua ’060 at Figure 8, [0009], [0011], [0016], [0041], [0290], [0291], [0315], [0317], [0318], [0336], [0353], [0354], [0382], [0392], [0395], [0405], [0417], and [0433]. Flitcroft ’833 at 10:26–56. Hanada ’365 at [0019]. Horowitz ’542 at [0012]. Jo ’744 at 1, 2, 3, 6, and 14. Keen ’200 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, [0002], [0003], [0012], [0013], [0015], [0026], [0028]–[0029], [0030], [0032], [0034], [0055], [0063], [0069], [0074], [0076], [0083], [0084], [0085], [0086], [0095], [0098], [0106], claim 1, claim 4, and claim 9. Mamba ’073 at Abstract, Fig. 2, [0001], [0011]–[0012], [0026], [0029], [0030], [0034], and [0041]. SCAR PT-04002 at 4, 7–8, PayPass Figure (p. 8), 8, ExpressPay Figure (p. 9), 9, 10, Table 1, 22, 23, 24, 37, 38, 39, and 40. Sovio ’882 at Abstract, Fig. 1, Fig. 2, [0010], [0017], [0020], [0041], [0043], [0045], [0049], [0073], and [0080]. Yoshinaga 2004 at 26–27. Yu ’038 at Fig. 2, Fig. 3, Fig. 4, Figure 18, Fig. 19, [0034], [0036], [0039], [0046], [0054]–[0056], [0093], [0096], [0097], and claim 20.
[9d] wherein the mobile device comprises a mobile phone.	*See* above at [1d].
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Dua ’060 at [0007], [0009], and [0433]. Flitcroft ’833 at Fig. 1 and 10:26–56. Hanada ’365 at [0018]. Horowitz ’542 at Figure 2, Figure 3A, [0003], [0011], [0012], [0015], [0025], claim 1, claim 2, claim 5, claim 6, claim 14, and claim 15.

Patent Owner's Ex. 2020
Page 009

Claim Element	Exemplary Citations
	Keen ’200 at Fig. 5. SCAR PT-04002 at 4, Fig. 1., 7–8, 8, 9, 11, and Table 1. Sovio ’882 at Fig. 1, Fig. 2, [0010], [0020], and [0045]. Yoshinaga 2004 at 24, 24–25, 25, Figure 1, 26, and 26–27. Yu ’038 at Fig. 4, Figure 18, [0001], [0036], [0039], [0046], [0090], [0091], [0092], [0093], [0096], [0097], and claim 7.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	*See* above at claim 3.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	*See* above at claim 2.

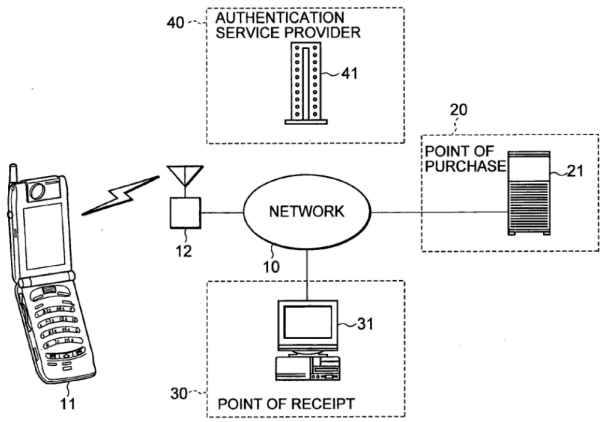
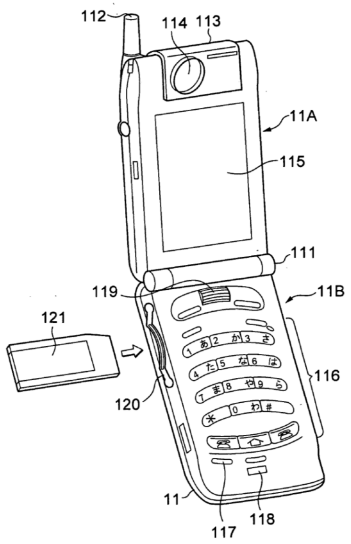
DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,202,156

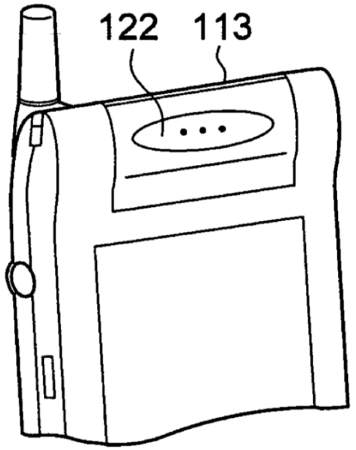
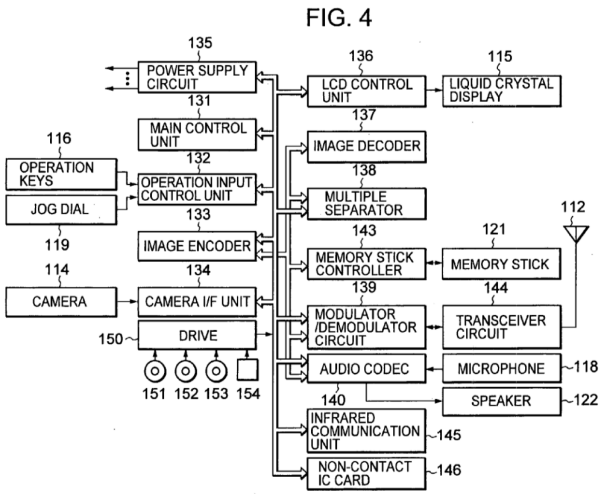
EXHIBIT E1: US20050086171A1 ("Abe '171")

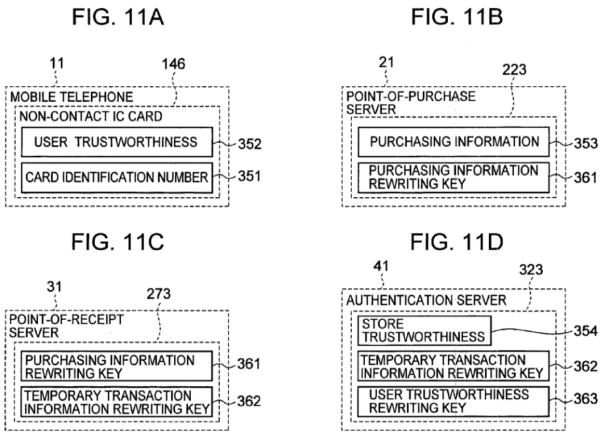
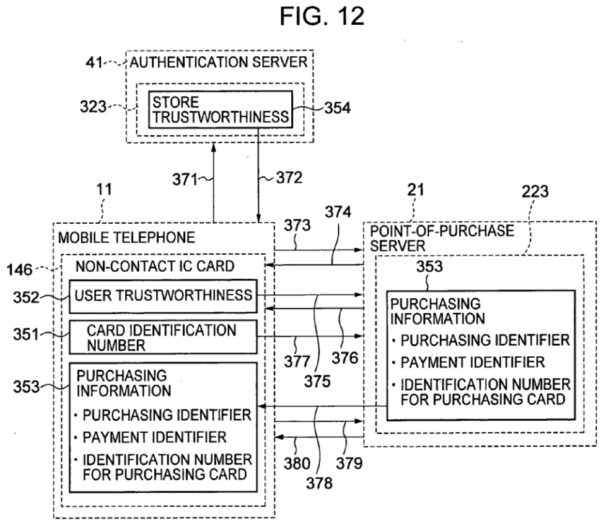
As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Abe '171 and (b) under 35 U.S.C. § 103(a) as obvious over Abe '171 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

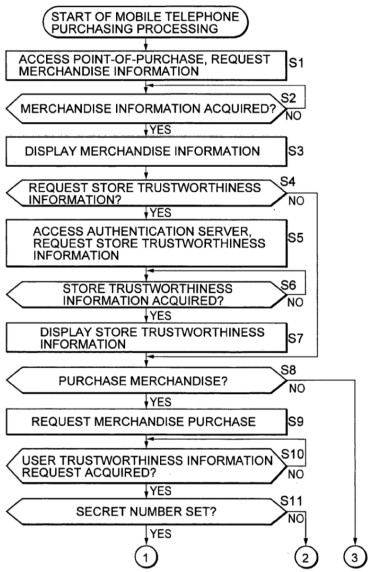
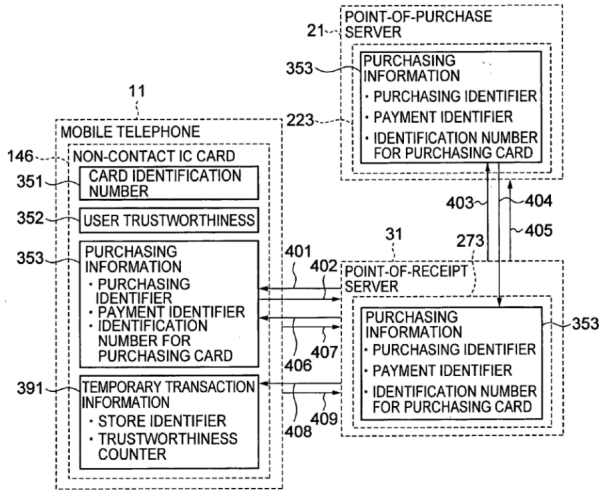
Claim Element	**Exemplary Citations to US20050086171A1 ("Abe '171")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Abe '171 discloses or renders obvious "[a] mobile device." For example: Abe '171 at Abstract The present invention relates to an information processing system, information communication terminal and method, information processing apparatus and method, recording medium, and program capable of enabling safer electronic commercial transactions in a straightforward manner. A point-of-purchase server 21 generates purchasing information using a card Identification number allotted to a non-contact IC-card of a mobile telephone 11. A point-of-receipt server 31 acquires this purchasing information and confirms the card identification number allotted to the non-contact IC card of the mobile telephone 11 and a purchasing card identification number. The authentication server 41 calculates user trustworthiness and store trustworthiness based on temporary commercial transaction information stored in the non-contact IC card of the mobile telephone 11. The calculated user trustworthiness and store trustworthiness is then reference by the mobile telephone 11 and point-of-purchase server 21 in the next commercial transaction. The present invention can be applied to electronic commercial transaction services.

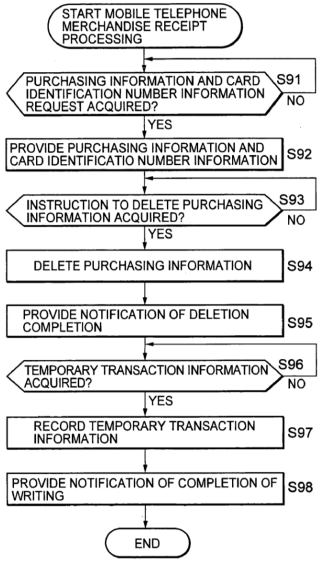
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at Figure 1 FIG. 1  Abe '171 at Figure 2 FIG. 2 

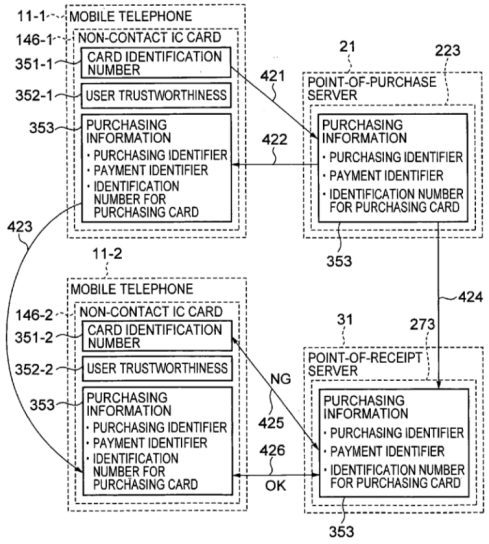
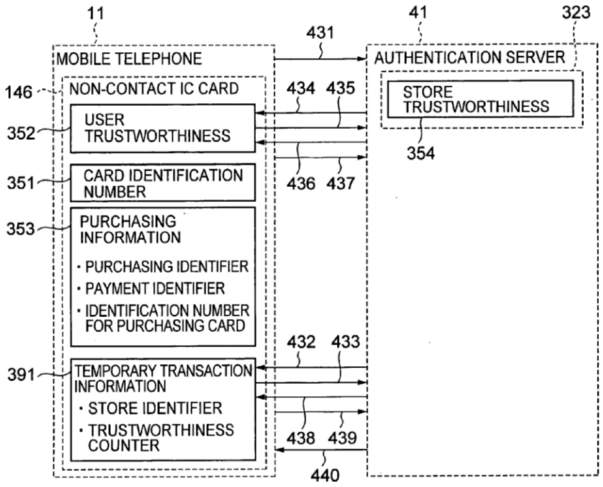
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at Fig. 3 FIG. 3  Abe ’171 at Figure 4 FIG. 4 

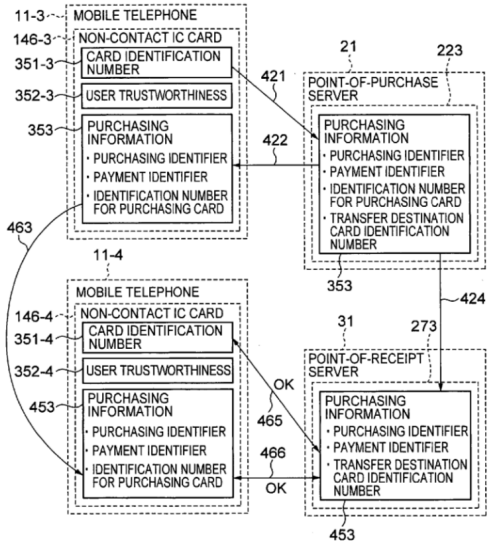
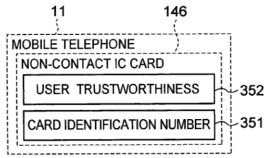
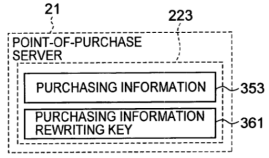
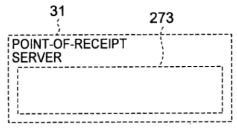
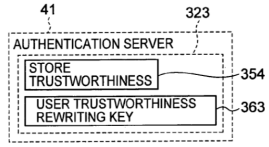
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at Fig.11A–D  Abe ’171 at Fig. 12  Abe ’171 at Fig. 13

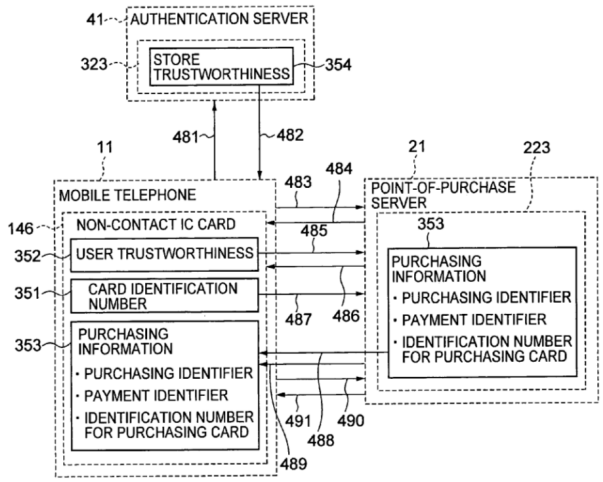
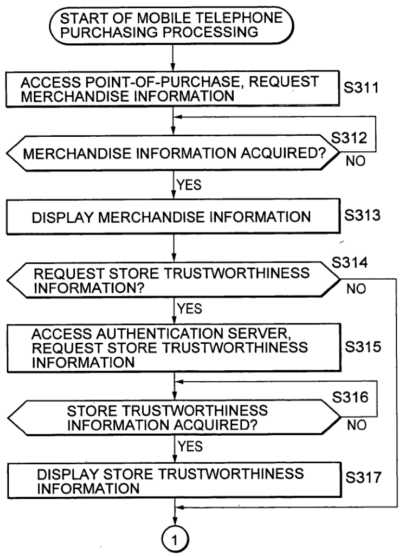
Patent Owner's Ex. 2020
Page 014

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 13  Abe '171 at Fig. 18 FIG. 18 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at Fig. 19 FIG. 19  Abe '171 at Fig. 23

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 23  Abe '171 at Fig. 24 FIG. 24 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at Fig. 29 FIG. 29  Abe '171 at Fig. 35A–D FIG. 35A  FIG. 35B  FIG. 35C  FIG. 35D  Abe '171 at Fig. 36

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 36  Abe '171 at Fig. 37 FIG. 37 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0006] An information processing system of the present invention is characterized by an information communication terminal connected to a network, for holding information relating to a commercial transaction and an information processing apparatus connected to the network, for managing information relating to the commercial transaction, wherein the information communication terminal comprises first acquiring means for acquiring information relating to the commercial transaction from the information processing apparatus during merchandise purchasing, first storage means for storing information relating to the commercial transaction acquired by the first acquiring means, and first providing means for providing information relating to the commercial transaction stored by the first storage means to the information processing apparatus during receipt of merchandise, wherein the information processing apparatus comprises second providing means for providing information relating to the commercial transaction to the information communication terminal during merchandise sales, second storage means for storing information relating to the commercial transaction, second acquiring means for acquiring information relating to the commercial transaction from the information communication terminal during merchandise delivery, and authentication means for authenticating information relating to said commercial transaction acquired by the second acquiring means using information relating to the commercial transaction stored by the second storage means. Abe '171 at [0031] A second information processing system of the present invention is characterized by: an information communication terminal connected to a network, for holding information relating to a commercial transaction; a first information processing apparatus connected to said network, for managing information relating to said commercial transaction; and a second information processing apparatus connected to said network, for managing information relating to trustworthiness of a first user constituting a user of said information communication terminal and information relating to trustworthiness of a second user constituting a user of said first information processing apparatus. At the information communication terminal, information relating to trustworthiness of the first user is stored, stored information relating to the trustworthiness of the first user is provided to the first information storage device, information relating to trustworthiness of the second user is acquired from the second information processing apparatus, information relating to a commercial transaction is acquired from the first information processing apparatus, the stored trustworthiness of the first user and acquired information relating to the commercial transaction are provided to the second processing device, and information relating to trustworthiness of the first user updated by the second information processing apparatus is acquired. At the first information

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	processing apparatus, information relating to trustworthiness of the first user is acquired from the information communication terminal and information relating to the commercial transaction is provided to the information communication terminal. At the second information processing apparatus, information relating to the trustworthiness of the second user is stored, stored information relating to the trustworthiness of the second user is provided to the information communication terminal, information relating to the trustworthiness of the first user from the information communication terminal and information relating to the commercial transaction is acquired, information relating to the trustworthiness of the first user and information relating to the trustworthiness of the second user is updated based on the acquired information relating to the commercial transaction, and information relating to the updated first user trustworthiness is provided to the information communication terminal. Abe '171 at [0036] FIG. 1 is a view showing an example configuration for an electronic commercial transaction system to which the present invention is applied. Abe '171 at [0037] FIG. 2 is a view showing an example configuration for the external appearance of the mobile telephone of FIG. 1. Abe '171 at [0051] FIG. 13 is a flowchart illustrating purchasing processing by a mobile telephone. Abe '171 at [0051]–[0052] FIG. 14 is a flowchart continuing on from the flowchart of FIG. 13 illustrating purchasing processing by a mobile telephone. Abe '171 at [0057] FIG. 19 is a flowchart illustrating merchandise receipt processing carried out by a mobile telephone Abe '171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10,

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe '171 at [0093] The mobile telephone 11 is operated by the user so as to carry out wireless communication with the nearest base station 12, access the point-of-purchase server 21 via the network 10, and carry out merchandise purchasing processing. The mobile telephone 11 is operated by the user so as to access the authentication server 41 of the authentication service provider 40, trustworthiness of the point-of-purchase 20 is acquired, and this is provided to the user to enable a determination to be made as to whether or not to purchase the merchandise (product). Abe '171 at [0100] As shown in FIG. 2, the mobile telephone 11 is constructed from a display unit 11A and main body 11B, capable of being folded up using a central hinge 111. Abe '171 at [0101] The display unit 11A has an antenna 112 for transmitting and receiving signals that is capable of being pulled out or stored provided at an upper part of a left end. The mobile telephone 11 transmits and receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112. Abe '171 at [0111] The memory stick 121 is a kind of flash memory card developed by the current applicant, Sony Corporation. This memory stick 121 is an item storing a type of EEPROM (Electrically Erasable and Programmable Read Only Memory) flash memory element constituted by non-volatile memory capable of being rewritten and erased electrically within a small, thin plastic case and is capable of reading and writing various types of data such as images, speech, and music etc. via ten pin terminals. Abe '171 at [0113]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	It is possible to extend the functions of the mobile telephone 11 still further by incorporating a module (chip) for extending prescribed functions into the memory stick 121 and installing this in the memory stick slot 120. Abe '171 at [0114] For example, as described in the following, by installing the memory stick 121 incorporating a non-contact IC (Integrated Circuit) card in the mobile telephone 11, it is possible to extend the functions so as to give the same electronic commercial transaction functions as for non-contact IC cards even when, for example, these modules are not built-into the mobile telephone 11. Abe '171 at [0115] FIG. 4 shows an example configuration of the inside of the mobile telephone 11. Abe '171 at [0116] A power supply circuit 135, operation input control unit 132, image encoder 133, camera interface (I/F) unit 134, LCD control unit 136, multiple separator 138, modulator/demodulator circuit 139, audio codec 140, infrared communication unit 145 and non-contact IC card 146 (in this example, a dedicated non-contact IC card (Felica chip (registered trademark)) is provided but it is also possible to provide non-contact IC card functions in the memory stick 121) are connected to a main control unit 131 for providing overall control of each part of the display unit 11A and body 11B via a main bus 141, and the image encoder 133, image decoder 137, multiple separator 138, a memory stick controller 143, the modulator/demodulator circuit 139, and the audio codec 140 are connected via a synchronous bus 142. Abe '171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. Abe '171 at [0178] The mobile telephone 11 shown in FIG. 11A holds information for a card identification number 351 and user trustworthiness 352 in the built-in non-contact IC card 146. Abe '171 at [0202]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	The following is a description with reference to the flowcharts of FIG. 13 and FIG. 14 of purchasing processing of the mobile telephone 11. Abe '171 at [0203] First, in step S1, the main control unit 131 of the mobile telephone 11 carries out wireless communication with the nearest base station 12 via the antenna 112, accesses the point-of-purchase server 21 via the network 10, and requests purchasing information. The point-of-purchase server 21 that has acquired this request then provides the requested purchasing information to the mobile telephone 11 as described in the following. Abe '171 at [0236] First, in step S61, the CPU 201 of the point-of-purchase server 21 controls the communication unit 224 and determines whether or not a request for merchandise information has been acquired. When it is determined that a request for merchandise information has been acquired (when merchandise information is requested by the mobile telephone 11), the CPU 201 advances processing to step S62, the requested merchandise information stored in the storage unit 223 is acquired, and is provided to the mobile telephone 11 via the network 10 by controlling the communication unit 224. Abe '171 at [0244] In step S71 of FIG. 17, the CPU 201 controls the communication unit 224 so as to make a request for card identification number information of the non-contact IC card 146 built-into the mobile telephone 11. This processing corresponds to the processing of arrow 376 of FIG. 12. Abe '171 at [0248] When purchasing/charging processing is complete, in step S74, the CPU 201 generates purchasing information relating to sale of merchandise on this occasion, and controls the communication unit 224 so that this generated purchasing information is provided to the mobile telephone 11 via the network 10 so as to be stored in the non-contact IC card 146. This processing corresponds to the processing of arrow 378 of FIG. 12. Abe '171 at [0257] In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance by the point-of-purchase 20. The user then positions the mobile telephone 11 in the

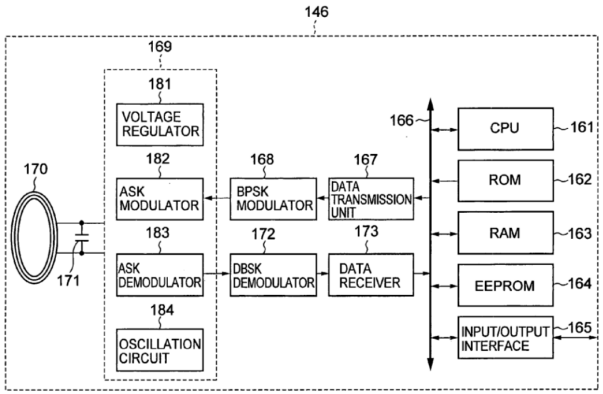
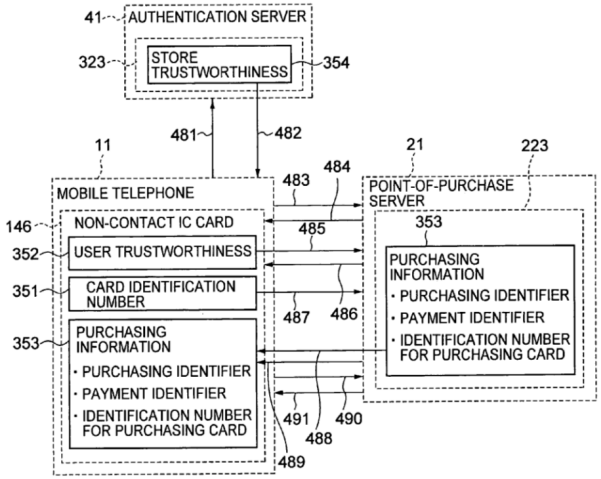
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	vicinity of the IC card reader/writer 275 of the point-of-receipt server 31 installed at the point of receipt 30, and positions the non-contact IC card 146 built-into the mobile telephone 11 in the vicinity of the IC card reader/writer 275. Abe '171 at [0266] The mobile telephone 11 then records the provided temporary commercial transaction information 391 in the non-contact IC card 146 using the acquired temporary commercial transaction information rewriting key 362. When recording is complete, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362, and provides the notification of completion of writing to the point-of-receipt server 31 (arrow 409) so as to complete processing relating to handing over of the merchandise. Abe '171 at [0271] When it is determined that a request for the purchasing information 353 and the card identification number information has been acquired, the main control unit 131 advances processing to step S92, controls the CPU 161 of the non-contact IC card 146, and provides card identification number information containing the requested purchasing information 353, and card identification number 351 to the point-of-receipt server 31. This processing corresponds to the processing of arrow 402 of FIG. 18. Abe '171 at [0282] When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0307] For example, as shown in FIG. 23, when a user of a mobile telephone 11-1 purchases merchandise from the point-of-purchase 20, the point-of-purchase server 21 generates purchasing information 353 (arrow 421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422). Abe '171 at [0313]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	The mobile telephone 11 then updates the stored user information 352 using the acquired user information rewriting key 363. When updating is complete, the mobile telephone 11 erases the user information rewriting key 363 and gives notification of completion of rewriting to the authentication server 41 (arrow 437). Abe '171 at [0319] The authentication server 41 that has accessed the mobile telephone 11 then, as described in the following, requests temporary commercial transaction information 391 stored in the non-contact IC card 146 of the mobile telephone 11. Abe '171 at [0347] The main control unit 131 of the mobile telephone 11 that has acquired the user trustworthiness information then updates the user trustworthiness 352 stored in the non-contact IC card 146 and provides this to the authentication server 41 using the processing of step S181 of FIG. 26. Abe '171 at [0350] When the main control unit 131 of the mobile telephone 11 deletes the temporary commercial transaction information 391 using the acquired temporary commercial transaction information rewriting key 362 based on the instruction from the authentication server 41, the processing advances to step S184 of FIG. 26, and deletion completion notification is provided to the authentication server 41. Abe '171 at [0360] For example, as shown in FIG. 29, when a purchaser mobile telephone 11-3 constituting a mobile telephone used when purchasing merchandise transfers purchasing information 353 stored in a non-contact IC card 146-3 to a transfer destination mobile telephone 11-4, a transfer destination card identification number (i.e. card identification number 351-4) is overwritten (taken to be purchasing information 453) with a purchasing card identification number 353 (i.e. card identification number 351-3) contained in the purchasing information 353, and stored in a non-contact IC card 146-4 of the transfer destination mobile telephone 11-4 (arrow 463). Abe '171 at [0364] First, in step S231, the main control unit 131 of the purchaser mobile telephone 11-3 makes a request to the point-of-purchase server 21 via the network 10 for permission to transfer the purchasing information 353.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0370] When it is determined that a request for the card identification number information of the transfer destination has been acquired, the main control unit 131 advances processing to step S235, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0371] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-4 is positioned within the communication range of the non-contact IC card 146-3, the CPU 161 of the non-contact IC card 146-3 detects the non-contact IC card 146-4 and notifies the main control unit 131 via antenna 170. Abe '171 at [0378] When it is determined that the updated purchasing information 453 and purchasing information rewriting key 361 have been acquired, the main control unit 131 advances processing to step S241 of FIG. 31, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0380] As described in the following, the transfer destination mobile telephone 11-4 provided with the purchasing information 453 and the purchasing information rewriting key 361 records the updated purchasing information 453 in the non-contact IC card 146-4 using the acquired purchasing information rewriting key 361. When recording is complete, the purchasing information rewriting key 361 is deleted, and completion of writing is provided to the purchaser mobile telephone 11-3. Abe '171 at [0395] In step S238 of FIG. 30, the purchaser mobile telephone 11-3 provides the requested card identification number information of the transfer destination to the point-of-purchase server 21. Abe '171 at [0412]–[0413]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-3 is positioned within the communication range of the non-contact IC card 146-4, the CPU 161 of the non-contact IC card 146-4 detects the non-contact IC card 146-3 and notifies the main control unit 131 via the antenna 170. When it is determined that the purchaser mobile telephone 11-3 is within communication range based on information provided by the CPU 161, the main control unit 131 of the transfer destination mobile telephone 11-4 advances processing to step S293, and card identification number information containing the requested card identification number 351-4 is provided to the purchaser mobile telephone 11-3 using short-range wireless communication by the non-contact IC card 146-4. Abe '171 at [0446] When it is determined that notification of completion of writing has been acquired, the CPU 201 advances processing to step S364, controls the communication unit 224, provides the purchasing information rewriting key 361 to the purchaser mobile telephone 11, and makes a request for deletion of purchasing information for which commercial transaction completion is finished to the purchaser mobile telephone 11. Abe '171 at [0454] In the case in FIG. 42, as in the case in FIG. 18, when the non-contact IC card 146 is positioned with communication range of short-range wireless communication of the IC card reader/writer 275, the point-of-receipt server 31 the mobile telephone 11 is in the proximity of makes a request to (arrow 501) and acquires from (arrow 502) the mobile telephone 11 purchasing information 353 and the card identification number 351. Abe '171 at [0460] Namely, in step S381, the main control unit 131 of the mobile telephone 11 controls the non-contact IC card 146 so as to determine whether or not a request for card identification number information containing the purchasing information 353 and card identification number 351 has been acquired from the point-of-receipt server 31, and waits until it is determined that acquisition has taken place. Abe '171 at [0481] In FIG. 47, as with the case in FIG. 24, the mobile telephone 11 accesses the authentication server 41 (arrow 511), but in a point of difference with the case of FIG. 24, the authentication server 41 does not request temporary commercial transaction information, but does request (arrow 512) and acquire (arrow

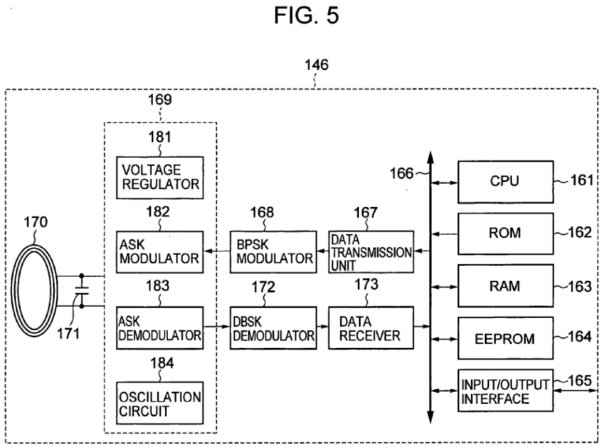
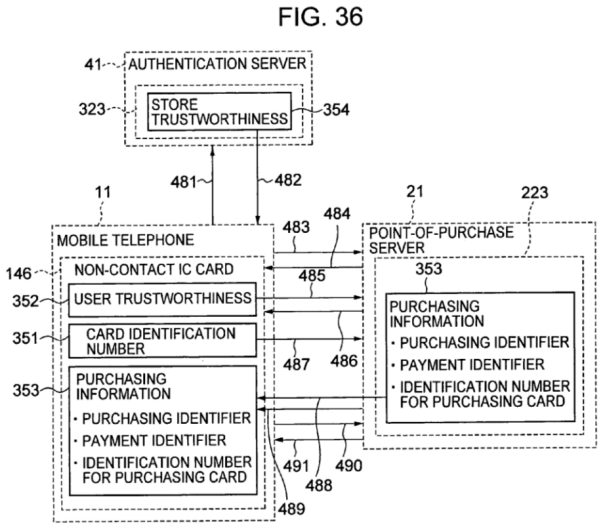
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	513) user trustworthiness information. The authentication server 41 then updates the user trustworthiness 352 contained in the acquired user trustworthiness information based on the purchasing information 353 provided by the point-of-purchase server 21 and provides this to (arrow 514) and stores this in the mobile telephone 11. Abe '171 at [0484] First, in step S471, as in the case of step S171 of FIG. 25, the main control unit 131 of the mobile telephone 11 accesses the authentication server 41 via the network 10. Abe '171 at [0504] In the above, a description is given where the purchaser of the merchandise acquires purchasing information 353 using the mobile telephone 11, and authentication processing is then carried out using the acquired purchasing information 353 when receiving the merchandise. However, the device used by the purchase may be any mobile communication terminal device such as, for example, a PDA (Personal Digital Assistant) etc. Abe '171 at claim 25 an information communication terminal connected to a network, for holding information relating to a commercial transaction; Abe '171 at claim 26 26. An information communication terminal, connected to a network, for communicating with a first information processing apparatus, characterized by: Abe '171 at claim 27 27. An information communication terminal, connected to a network, for communicating with a first information processing apparatus, characterized by: Abe '171 at claim 30 30. An information communication terminal, connected to a network, for communicating with a first information processing apparatus, characterized by: To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Abe '171 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Abe '171 at Figure 5 FIG. 5  Abe '171 at Fig. 36 FIG. 36  Abe '171 at [0009]

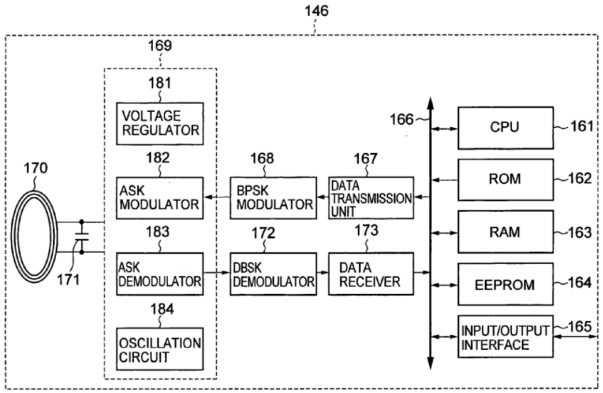
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	The information communication device is further characterized by wireless communication means for carrying out short-range wireless communication via electromagnetic radiation with the first information processing apparatus in close proximity. The first providing means is then capable of providing information relating to the commercial transaction to the first information processing apparatus using short-range wireless communication by the wireless communication means. Abe '171 at [0030] The first information processing system of the present invention is provided with an information communication terminal connected to a network, for holding information relating to a commercial transaction and an information processing apparatus connected to the network, for managing information relating to the commercial transaction. At the information communication terminal, information relating to the commercial transaction is acquired from the information processing apparatus during merchandise purchasing. Acquired information relating to the commercial transaction is then stored. Information relating to the stored commercial transaction is then provided to the information processing apparatus during receipt of the merchandise. At the information processing apparatus, information relating to the commercial transaction is provided to the information communication terminal during merchandise sales and stored. Information relating to the commercial transaction is then acquired from the information communication terminal during merchandise delivery. Information relating to the acquired commercial transaction is then authenticated using information relating to the stored commercial transaction. Abe '171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe '171 at [0101] The display unit 11A has an antenna 112 for transmitting and receiving signals that is capable of being pulled out or stored provided at an upper part of a left end. The mobile telephone 11 transmits and

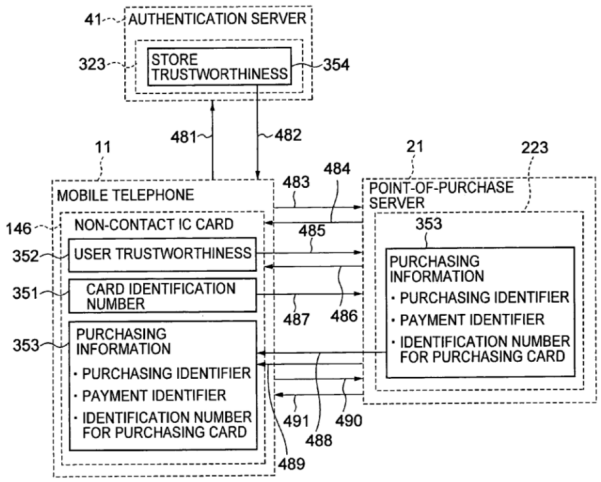
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112. Abe '171 at [0134] The non-contact IC card 146 may then be brought close to another information processing apparatus having an IC card reader/writer so that when electromagnetic waves radiated from the IC card reader/writer are received, various information is provided to the IC card reader/writer in response to this. Abe '171 at [0137] The non-contact IC card 146 is comprised of, for example, an antenna (loop antenna) 170 and capacitor 171 shown in the drawing, and an IC storing other aspects of the configuration on one chip. The non-contact IC card 146 then communicates various types of data with an IC card reader/writer provided at another information processing apparatus in a half-duplex manner by utilizing electromagnetic induction, and does not by any means have to be card-shaped. Further, "IC card" is a name given for convenience of description, and is intended to mean functions described above or described in the following. Further, for example, a Felica chip (registered trademark) may also be given as a device providing substantially the same functions as the non-contact IC card 146. Abe '171 at [0140] At the interface 169, an alternating magnetic field excited at the antenna 170 is rectified by the ASK demodulator 183, and this is stabilized at a voltage regulator 181 and supplied to each part as a direct current power source. The electric power of electromagnetic waves radiated from the IC card reader/writer is regulated to as to generate an electric field covering the required electric power at the non-contact IC card as described in the following. Abe '171 at [0169]–[0170] When response data from the non-contact IC card 146 is supplied from the demodulation unit 294, the SPU 306 subjects this data to, for example, BPSK demodulation (decoding of Manchester code) etc., and provides the acquired data to the CPU 301. Further, when a command sent to the non-contact IC card 146 is provided via the bus 305, the SPU 306 subjects this command to BPSK modulation (encoding to Manchester code), and the acquired data is outputted to the modulator 292. The modulator 292 ASK modulates a carrier wave of a prescribed frequency (for example, 13.56 MHz) supplied by an oscillating circuit (OSC) 293 based on data supplied by the SPU 306, and outputs the generated modulated wave from an antenna 295 as electromagnetic radiation. On the other hand, the

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	demodulator 294 demodulates a modulated wave (ASK modulated wave) acquired via the antenna 295 and outputs the demodulated data to the SPU 296. Abe '171 at [0282] When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0370] When it is determined that a request for the card identification number information of the transfer destination has been acquired, the main control unit 131 advances processing to step S235, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0371] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-4 is positioned within the communication range of the non-contact IC card 146-3, the CPU 161 of the non-contact IC card 146-3 detects the non-contact IC card 146-4 and notifies the main control unit 131 via antenna 170. Abe '171 at [0378] When it is determined that the updated purchasing information 453 and purchasing information rewriting key 361 have been acquired, the main control unit 131 advances processing to step S241 of FIG. 31, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
[1b] a memory to hold transaction data; and	Abe '171 discloses or renders obvious "a memory to hold transaction data." For example: Abe '171 at Figure 5  Abe '171 at Fig. 36  Abe '171 at [0111]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	The memory stick 121 is a kind of flash memory card developed by the current applicant, Sony Corporation. This memory stick 121 is an item storing a type of EEPROM (Electrically Erasable and Programmable Read Only Memory) flash memory element constituted by non-volatile memory capable of being rewritten and erased electrically within a small, thin plastic case and is capable of reading and writing various types of data such as images, speech, and music etc. via ten pin terminals. Abe '171 at [0116] A power supply circuit 135, operation input control unit 132, image encoder 133, camera interface (I/F) unit 134, LCD control unit 136, multiple separator 138, modulator/demodulator circuit 139, audio codec 140, infrared communication unit 145 and non-contact IC card 146 (in this example, a dedicated non-contact IC card (Felica chip (registered trademark)) is provided but it is also possible to provide non-contact IC card functions in the memory stick 121) are connected to a main control unit 131 for providing overall control of each part of the display unit 11A and body 11B via a main bus 141, and the image encoder 133, image decoder 137, multiple separator 138, a memory stick controller 143, the modulator/demodulator circuit 139, and the audio codec 140 are connected via a synchronous bus 142. Abe '171 at [0138] A CPU 161 expands a control program stored in ROM 162 into RAM 163, and controls all of the operations of the non-contact IC card 146. For example, when electromagnetic waves radiated from the IC card reader/writer provided at another information processing apparatus are received by an antenna 170, the CPU 161 notifies the IC card reader/writer of a card identification number set at the non-contact IC card 146 in response to this, and processing relating to receiving merchandise is carried out. Abe '171 at [0147] Electronic money information is stored in the EEPROM 164. The user is then able to settle fees for purchased products and services etc. by utilizing this electronic money. The settlement history is also stored in an EEPROM 164. Abe '171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143.

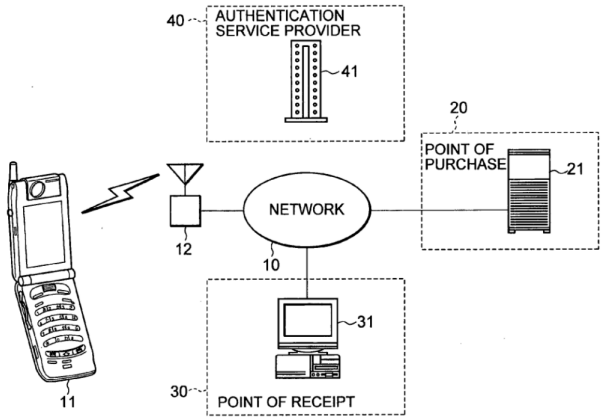
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Abe '171 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Abe '171 at Figure 5 FIG. 5  Abe '171 at Fig. 36

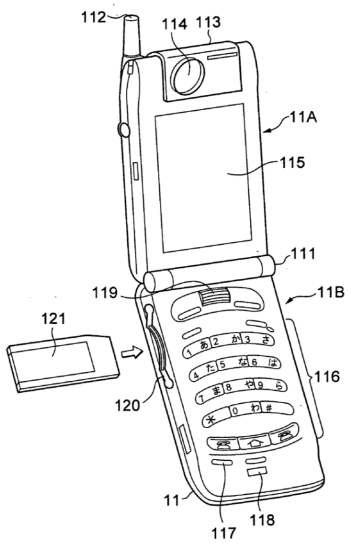
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 36  Abe '171 at [0009] The information communication device is further characterized by wireless communication means for carrying out short-range wireless communication via electromagnetic radiation with the first information processing apparatus in close proximity. The first providing means is then capable of providing information relating to the commercial transaction to the first information processing apparatus using short-range wireless communication by the wireless communication means. Abe '171 at [0030] The first information processing system of the present invention is provided with an information communication terminal connected to a network, for holding information relating to a commercial transaction and an information processing apparatus connected to the network, for managing information relating to the commercial transaction. At the information communication terminal, information relating to the commercial transaction is acquired from the information processing apparatus during merchandise purchasing. Acquired information relating to the commercial transaction is then stored. Information relating to the stored commercial transaction is then provided to the information processing apparatus during receipt of the merchandise. At the information processing apparatus, information relating to the commercial transaction is provided to the information communication terminal during merchandise sales and stored. Information relating to the commercial transaction is then acquired from the information

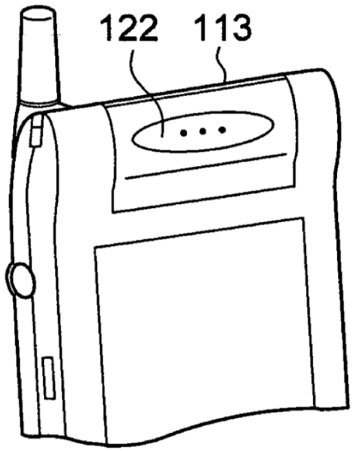
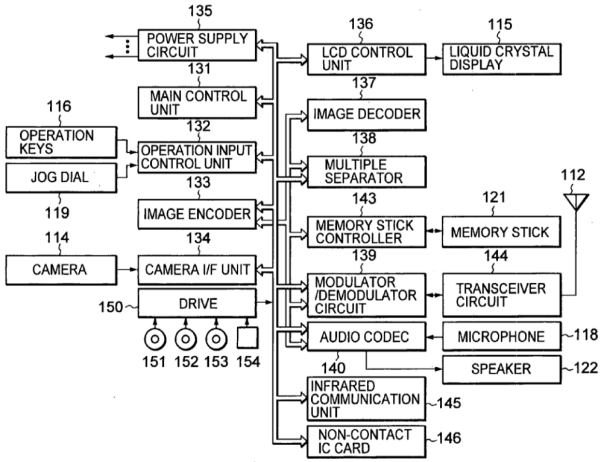
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	communication terminal during merchandise delivery. Information relating to the acquired commercial transaction is then authenticated using information relating to the stored commercial transaction. Abe ’171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe ’171 at [0101] The display unit 11A has an antenna 112 for transmitting and receiving signals that is capable of being pulled out or stored provided at an upper part of a left end. The mobile telephone 11 transmits and receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112. Abe ’171 at [0118] The main control unit 131 constituted by a CPU (Central Processing Unit), ROM (Read Only Memory) and RAM (Random Access Memory) etc. converts an audio signal collected by the microphone 118 into a digital audio signal using the audio codec 140 at the time of audio call mode. The digital audio data is subjected to spectrum diffusion processing by the modulator/demodulator circuit 139, subjected to digital/analog conversion processing and frequency conversion processing by a transceiver circuit 144, and is transmitted via the antenna 112. Abe ’171 at [0134] The non-contact IC card 146 may then be brought close to another information processing apparatus having an IC card reader/writer so that when electromagnetic waves radiated from the IC card reader/writer are received, various information is provided to the IC card reader/writer in response to this. Abe ’171 at [0137]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	The non-contact IC card 146 is comprised of, for example, an antenna (loop antenna) 170 and capacitor 171 shown in the drawing, and an IC storing other aspects of the configuration on one chip. The non-contact IC card 146 then communicates various types of data with an IC card reader/writer provided at another information processing apparatus in a half-duplex manner by utilizing electromagnetic induction, and does not by any means have to be card-shaped. Further, “IC card” is a name given for convenience of description, and is intended to mean functions described above or described in the following. Further, for example, a Felica chip (registered trademark) may also be given as a device providing substantially the same functions as the non-contact IC card 146. Abe ’171 at [0140] At the interface 169, an alternating magnetic field excited at the antenna 170 is rectified by the ASK demodulator 183, and this is stabilized at a voltage regulator 181 and supplied to each part as a direct current power source. The electric power of electromagnetic waves radiated from the IC card reader/writer is regulated to as to generate an electric field covering the required electric power at the non-contact IC card as described in the following. Abe ’171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. Abe ’171 at [0169]–[0170] When response data from the non-contact IC card 146 is supplied from the demodulation unit 294, the SPU 306 subjects this data to, for example, BPSK demodulation (decoding of Manchester code) etc., and provides the acquired data to the CPU 301. Further, when a command sent to the non-contact IC card 146 is provided via the bus 305, the SPU 306 subjects this command to BPSK modulation (encoding to Manchester code), and the acquired data is outputted to the modulator 292. The modulator 292 ASK modulates a carrier wave of a prescribed frequency (for example, 13.56 MHz) supplied by an oscillating circuit (OSC) 293 based on data supplied by the SPU 306, and outputs the generated modulated wave from an antenna 295 as electromagnetic radiation. On the other hand, the demodulator 294 demodulates a modulated wave (ASK modulated wave) acquired via the antenna 295 and outputs the demodulated data to the SPU 296. Abe ’171 at [0282]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0370] When it is determined that a request for the card identification number information of the transfer destination has been acquired, the main control unit 131 advances processing to step S235, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0371] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-4 is positioned within the communication range of the non-contact IC card 146-3, the CPU 161 of the non-contact IC card 146-3 detects the non-contact IC card 146-4 and notifies the main control unit 131 via antenna 170. Abe '171 at [0378] When it is determined that the updated purchasing information 453 and purchasing information rewriting key 361 have been acquired, the main control unit 131 advances processing to step S241 of FIG. 31, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	Abe '171 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: Abe '171 at Abstract The present invention relates to an information processing system, information communication terminal and method, information processing apparatus and method, recording medium, and program capable of

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	enabling safer electronic commercial transactions in a straightforward manner. A point-of-purchase server 21 generates purchasing information using a card Identification number allotted to a non-contact IC-card of a mobile telephone 11. A point-of-receipt server 31 acquires this purchasing information and confirms the card identification number allotted to the non-contact IC card of the mobile telephone 11 and a purchasing card identification number. The authentication server 41 calculates user trustworthiness and store trustworthiness based on temporary commercial transaction information stored in the non-contact IC card of the mobile telephone 11. The calculated user trustworthiness and store trustworthiness is then reference by the mobile telephone 11 and point-of-purchase server 21 in the next commercial transaction. The present invention can be applied to electronic commercial transaction services. Abe '171 at Figure 1 FIG. 1  Abe '171 at Figure 2

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	FIG. 2  Abe ’171 at Fig. 3

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	FIG. 3  Abe ’171 at Figure 4 FIG. 4  Abe ’171 at Fig.11A–D

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")

FIG. 11A

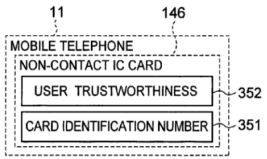


FIG. 11B

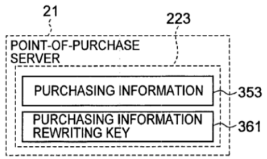


FIG. 11C

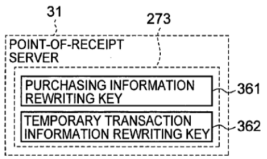
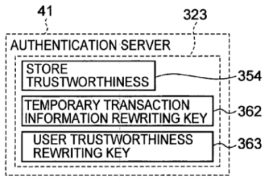
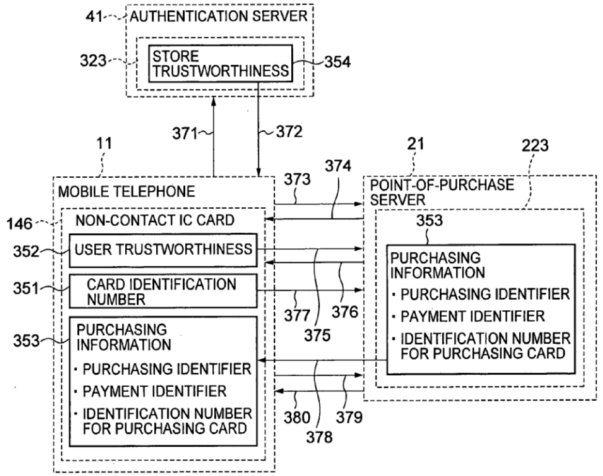


FIG. 11D

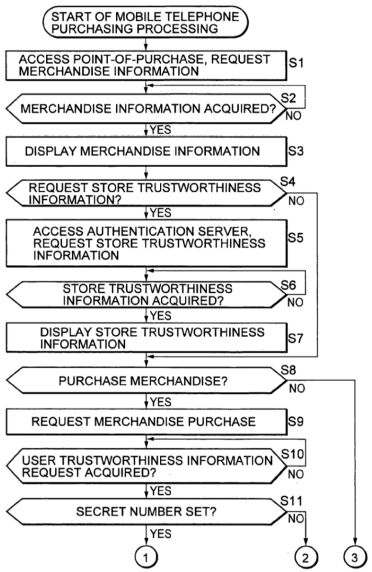
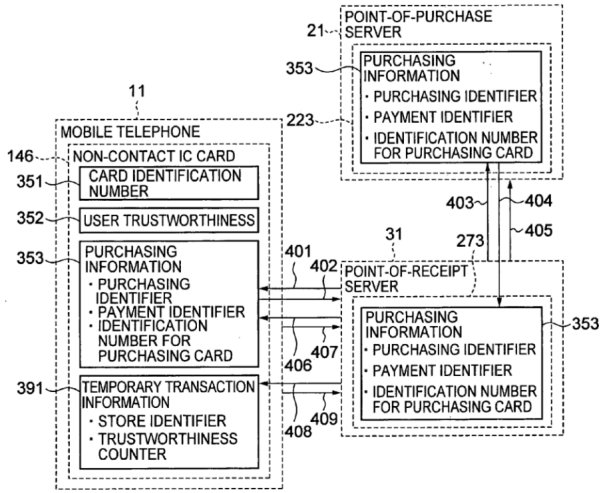


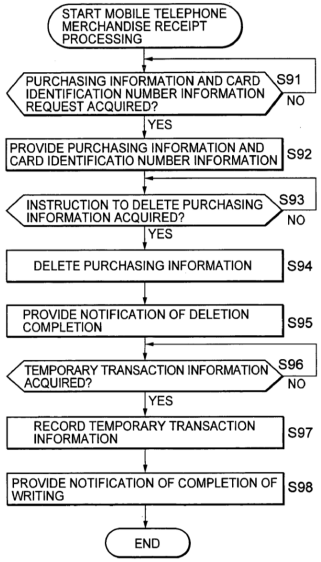
Abe '171 at Fig. 12

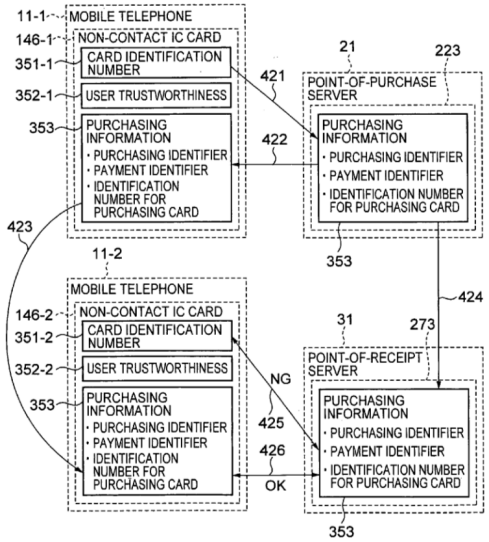
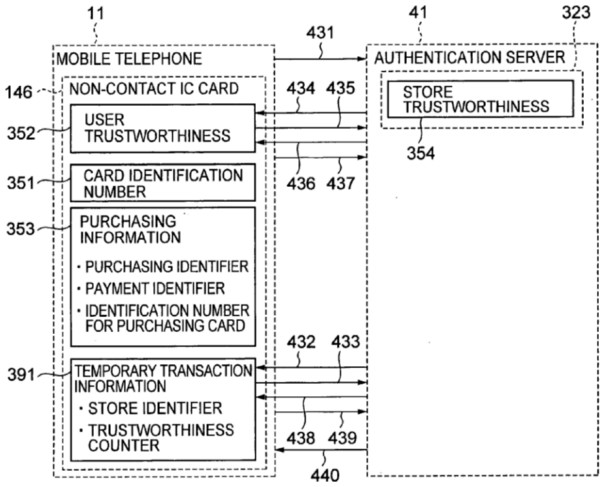
FIG. 12

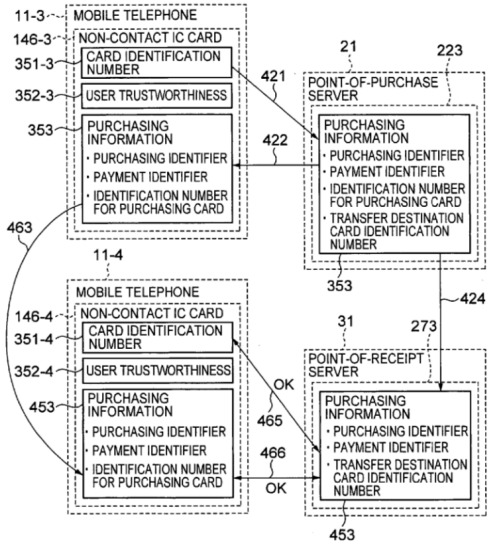
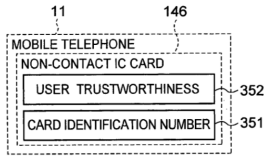
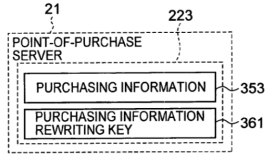
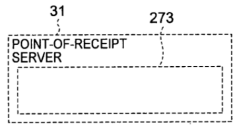
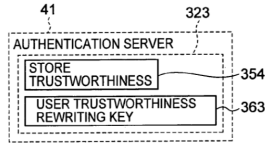


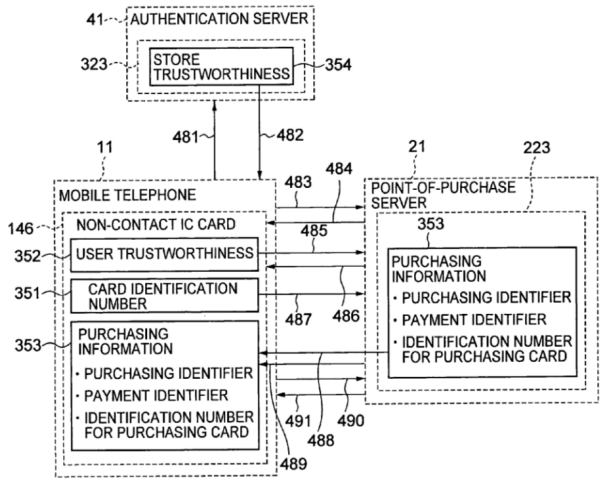
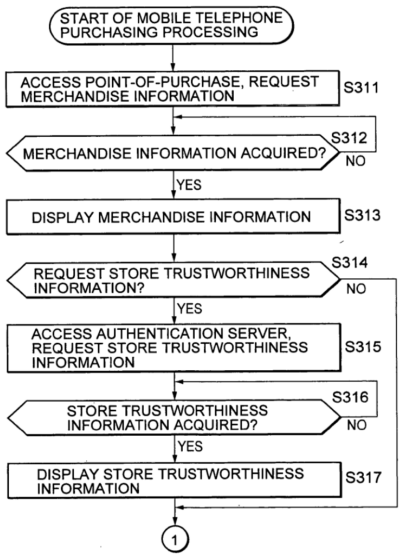
Abe '171 at Fig. 13

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 13  Abe '171 at Fig. 18 FIG. 18 

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at Fig. 19 FIG. 19  Abe ’171 at Fig. 23

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 23  Abe '171 at Fig. 24 FIG. 24 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at Fig. 29 FIG. 29  Abe '171 at Fig. 35A–D FIG. 35A  FIG. 35B  FIG. 35C  FIG. 35D  Abe '171 at Fig. 36

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 36  Abe '171 at Fig. 37 FIG. 37 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0030] The first information processing system of the present invention is provided with an information communication terminal connected to a network, for holding information relating to a commercial transaction and an information processing apparatus connected to the network, for managing information relating to the commercial transaction. At the information communication terminal, information relating to the commercial transaction is acquired from the information processing apparatus during merchandise purchasing. Acquired information relating to the commercial transaction is then stored. Information relating to the stored commercial transaction is then provided to the information processing apparatus during receipt of the merchandise. At the information processing apparatus, information relating to the commercial transaction is provided to the information communication terminal during merchandise sales and stored. Information relating to the commercial transaction is then acquired from the information communication terminal during merchandise delivery. Information relating to the acquired commercial transaction is then authenticated using information relating to the stored commercial transaction. Abe '171 at [0036] FIG. 1 is a view showing an example configuration for an electronic commercial transaction system to which the present invention is applied. Abe '171 at [0037] FIG. 2 is a view showing an example configuration for the external appearance of the mobile telephone of FIG. 1. Abe '171 at [0051] FIG. 13 is a flowchart illustrating purchasing processing by a mobile telephone. Abe '171 at [0051]–[0052] FIG. 14 is a flowchart continuing on from the flowchart of FIG. 13 illustrating purchasing processing by a mobile telephone. Abe '171 at [0057] FIG. 19 is a flowchart illustrating merchandise receipt processing carried out by a mobile telephone Abe '171 at [0092]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe '171 at [0093] The mobile telephone 11 is operated by the user so as to carry out wireless communication with the nearest base station 12, access the point-of-purchase server 21 via the network 10, and carry out merchandise purchasing processing. The mobile telephone 11 is operated by the user so as to access the authentication server 41 of the authentication service provider 40, trustworthiness of the point-of-purchase 20 is acquired, and this is provided to the user to enable a determination to be made as to whether or not to purchase the merchandise (product). Abe '171 at [0100] As shown in FIG. 2, the mobile telephone 11 is constructed from a display unit 11A and main body 11B, capable of being folded up using a central hinge 111. Abe '171 at [0101] The display unit 11A has an antenna 112 for transmitting and receiving signals that is capable of being pulled out or stored provided at an upper part of a left end. The mobile telephone 11 transmits and receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112. Abe '171 at [0111] The memory stick 121 is a kind of flash memory card developed by the current applicant, Sony Corporation. This memory stick 121 is an item storing a type of EEPROM (Electrically Erasable and Programmable Read Only Memory) flash memory element constituted by non-volatile memory capable of being rewritten and erased electrically within a small, thin plastic case and is capable of reading and writing various types of data such as images, speech, and music etc. via ten pin terminals.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0113] It is possible to extend the functions of the mobile telephone 11 still further by incorporating a module (chip) for extending prescribed functions into the memory stick 121 and installing this in the memory stick slot 120. Abe '171 at [0114] For example, as described in the following, by installing the memory stick 121 incorporating a non-contact IC (Integrated Circuit) card in the mobile telephone 11, it is possible to extend the functions so as to give the same electronic commercial transaction functions as for non-contact IC cards even when, for example, these modules are not built-into the mobile telephone 11. Abe '171 at [0115] FIG. 4 shows an example configuration of the inside of the mobile telephone 11. Abe '171 at [0116] A power supply circuit 135, operation input control unit 132, image encoder 133, camera interface (I/F) unit 134, LCD control unit 136, multiple separator 138, modulator/demodulator circuit 139, audio codec 140, infrared communication unit 145 and non-contact IC card 146 (in this example, a dedicated non-contact IC card (Felica chip (registered trademark)) is provided but it is also possible to provide non-contact IC card functions in the memory stick 121) are connected to a main control unit 131 for providing overall control of each part of the display unit 11A and body 11B via a main bus 141, and the image encoder 133, image decoder 137, multiple separator 138, a memory stick controller 143, the modulator/demodulator circuit 139, and the audio codec 140 are connected via a synchronous bus 142. Abe '171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. Abe '171 at [0178] The mobile telephone 11 shown in FIG. 11A holds information for a card identification number 351 and user trustworthiness 352 in the built-in non-contact IC card 146.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0202] The following is a description with reference to the flowcharts of FIG. 13 and FIG. 14 of purchasing processing of the mobile telephone 11. Abe '171 at [0203] First, in step S1, the main control unit 131 of the mobile telephone 11 carries out wireless communication with the nearest base station 12 via the antenna 112, accesses the point-of-purchase server 21 via the network 10, and requests purchasing information. The point-of-purchase server 21 that has acquired this request then provides the requested purchasing information to the mobile telephone 11 as described in the following. Abe '171 at [0236] First, in step S61, the CPU 201 of the point-of-purchase server 21 controls the communication unit 224 and determines whether or not a request for merchandise information has been acquired. When it is determined that a request for merchandise information has been acquired (when merchandise information is requested by the mobile telephone 11), the CPU 201 advances processing to step S62, the requested merchandise information stored in the storage unit 223 is acquired, and is provided to the mobile telephone 11 via the network 10 by controlling the communication unit 224. Abe '171 at [0244] In step S71 of FIG. 17, the CPU 201 controls the communication unit 224 so as to make a request for card identification number information of the non-contact IC card 146 built-into the mobile telephone 11. This processing corresponds to the processing of arrow 376 of FIG. 12. Abe '171 at [0248] When purchasing/charging processing is complete, in step S74, the CPU 201 generates purchasing information relating to sale of merchandise on this occasion, and controls the communication unit 224 so that this generated purchasing information is provided to the mobile telephone 11 via the network 10 so as to be stored in the non-contact IC card 146. This processing corresponds to the processing of arrow 378 of FIG. 12. Abe '171 at [0257]

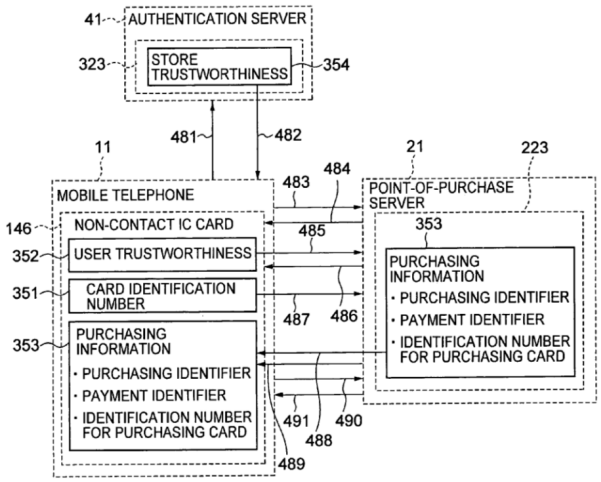
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance by the point-of-purchase 20. The user then positions the mobile telephone 11 in the vicinity of the IC card reader/writer 275 of the point-of-receipt server 31 installed at the point of receipt 30, and positions the non-contact IC card 146 built-into the mobile telephone 11 in the vicinity of the IC card reader/writer 275. Abe '171 at [0266] The mobile telephone 11 then records the provided temporary commercial transaction information 391 in the non-contact IC card 146 using the acquired temporary commercial transaction information rewriting key 362. When recording is complete, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362, and provides the notification of completion of writing to the point-of-receipt server 31 (arrow 409) so as to complete processing relating to handing over of the merchandise. Abe '171 at [0271] When it is determined that a request for the purchasing information 353 and the card identification number information has been acquired, the main control unit 131 advances processing to step S92, controls the CPU 161 of the non-contact IC card 146, and provides card identification number information containing the requested purchasing information 353, and card identification number 351 to the point-of-receipt server 31. This processing corresponds to the processing of arrow 402 of FIG. 18. Abe '171 at [0282] When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0307] For example, as shown in FIG. 23, when a user of a mobile telephone 11-1 purchases merchandise from the point-of-purchase 20, the point-of-purchase server 21 generates purchasing information 353 (arrow 421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422).

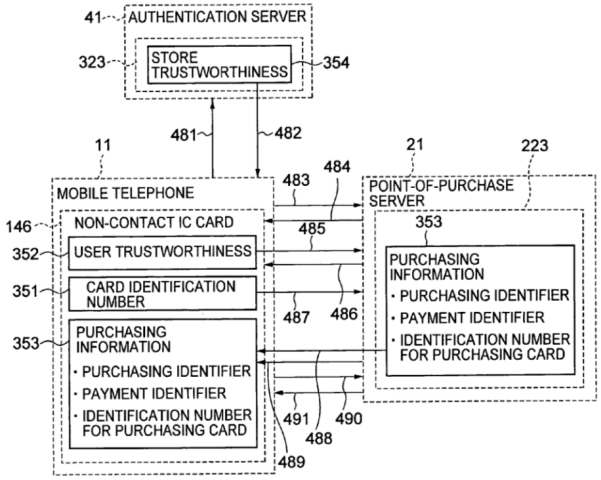
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0313] The mobile telephone 11 then updates the stored user information 352 using the acquired user information rewriting key 363. When updating is complete, the mobile telephone 11 erases the user information rewriting key 363 and gives notification of completion of rewriting to the authentication server 41 (arrow 437). Abe '171 at [0319] The authentication server 41 that has accessed the mobile telephone 11 then, as described in the following, requests temporary commercial transaction information 391 stored in the non-contact IC card 146 of the mobile telephone 11. Abe '171 at [0347] The main control unit 131 of the mobile telephone 11 that has acquired the user trustworthiness information then updates the user trustworthiness 352 stored in the non-contact IC card 146 and provides this to the authentication server 41 using the processing of step S181 of FIG. 26. Abe '171 at [0350] When the main control unit 131 of the mobile telephone 11 deletes the temporary commercial transaction information 391 using the acquired temporary commercial transaction information rewriting key 362 based on the instruction from the authentication server 41, the processing advances to step S184 of FIG. 26, and deletion completion notification is provided to the authentication server 41. Abe '171 at [0360] For example, as shown in FIG. 29, when a purchaser mobile telephone 11-3 constituting a mobile telephone used when purchasing merchandise transfers purchasing information 353 stored in a non-contact IC card 146-3 to a transfer destination mobile telephone 11-4, a transfer destination card identification number (i.e. card identification number 351-4) is overwritten (taken to be purchasing information 453) with a purchasing card identification number 353 (i.e. card identification number 351-3) contained in the purchasing information 353, and stored in a non-contact IC card 146-4 of the transfer destination mobile telephone 11-4 (arrow 463). Abe '171 at [0364]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	First, in step S231, the main control unit 131 of the purchaser mobile telephone 11-3 makes a request to the point-of-purchase server 21 via the network 10 for permission to transfer the purchasing information 353. Abe '171 at [0370] When it is determined that a request for the card identification number information of the transfer destination has been acquired, the main control unit 131 advances processing to step S235, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0371] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-4 is positioned within the communication range of the non-contact IC card 146-3, the CPU 161 of the non-contact IC card 146-3 detects the non-contact IC card 146-4 and notifies the main control unit 131 via antenna 170. Abe '171 at [0378] When it is determined that the updated purchasing information 453 and purchasing information rewriting key 361 have been acquired, the main control unit 131 advances processing to step S241 of FIG. 31, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0380] As described in the following, the transfer destination mobile telephone 11-4 provided with the purchasing information 453 and the purchasing information rewriting key 361 records the updated purchasing information 453 in the non-contact IC card 146-4 using the acquired purchasing information rewriting key 361. When recording is complete, the purchasing information rewriting key 361 is deleted, and completion of writing is provided to the purchaser mobile telephone 11-3. Abe '171 at [0395] In step S238 of FIG. 30, the purchaser mobile telephone 11-3 provides the requested card identification number information of the transfer destination to the point-of-purchase server 21.

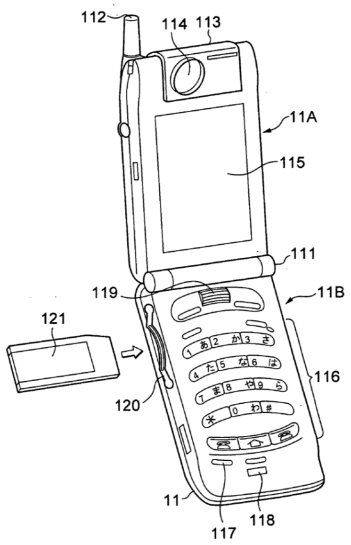
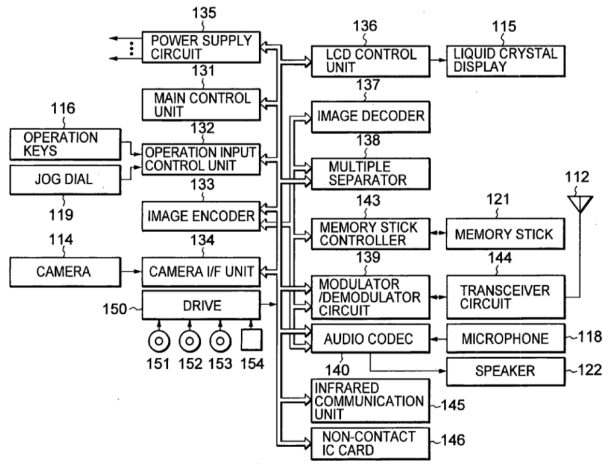
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0412]–[0413] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-3 is positioned within the communication range of the non-contact IC card 146-4, the CPU 161 of the non-contact IC card 146-4 detects the non-contact IC card 146-3 and notifies the main control unit 131 via the antenna 170. When it is determined that the purchaser mobile telephone 11-3 is within communication range based on information provided by the CPU 161, the main control unit 131 of the transfer destination mobile telephone 11-4 advances processing to step S293, and card identification number information containing the requested card identification number 351-4 is provided to the purchaser mobile telephone 11-3 using short-range wireless communication by the non-contact IC card 146-4. Abe '171 at [0446] When it is determined that notification of completion of writing has been acquired, the CPU 201 advances processing to step S364, controls the communication unit 224, provides the purchasing information rewriting key 361 to the purchaser mobile telephone 11, and makes a request for deletion of purchasing information for which commercial transaction completion is finished to the purchaser mobile telephone 11. Abe '171 at [0454] In the case in FIG. 42, as in the case in FIG. 18, when the non-contact IC card 146 is positioned with communication range of short-range wireless communication of the IC card reader/writer 275, the point-of-receipt server 31 the mobile telephone 11 is in the proximity of makes a request to (arrow 501) and acquires from (arrow 502) the mobile telephone 11 purchasing information 353 and the card identification number 351. Abe '171 at [0460] Namely, in step S381, the main control unit 131 of the mobile telephone 11 controls the non-contact IC card 146 so as to determine whether or not a request for card identification number information containing the purchasing information 353 and card identification number 351 has been acquired from the point-of-receipt server 31, and waits until it is determined that acquisition has taken place. Abe '171 at [0481]

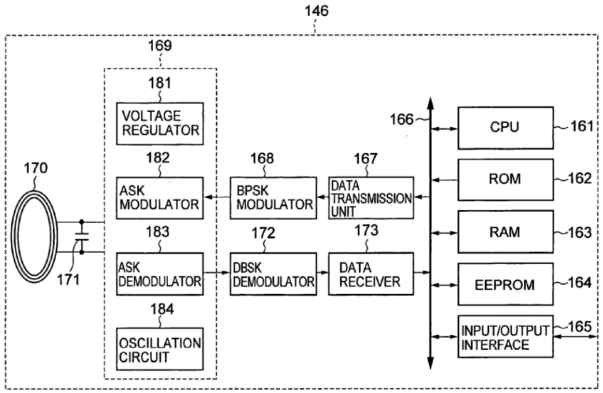
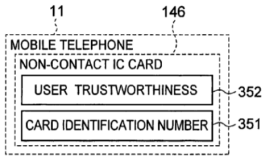
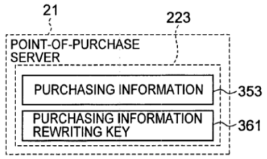
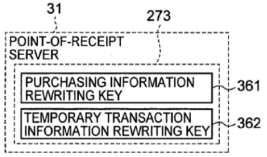
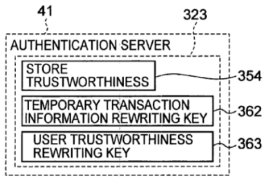
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	In FIG. 47, as with the case in FIG. 24, the mobile telephone 11 accesses the authentication server 41 (arrow 511), but in a point of difference with the case of FIG. 24, the authentication server 41 does not request temporary commercial transaction information, but does request (arrow 512) and acquire (arrow 513) user trustworthiness information. The authentication server 41 then updates the user trustworthiness 352 contained in the acquired user trustworthiness information based on the purchasing information 353 provided by the point-of-purchase server 21 and provides this to (arrow 514) and stores this in the mobile telephone 11. Abe '171 at [0484] First, in step S471, as in the case of step S171 of FIG. 25, the main control unit 131 of the mobile telephone 11 accesses the authentication server 41 via the network 10. Abe '171 at [0504] In the above, a description is given where the purchaser of the merchandise acquires purchasing information 353 using the mobile telephone 11, and authentication processing is then carried out using the acquired purchasing information 353 when receiving the merchandise. However, the device used by the purchase may be any mobile communication terminal device such as, for example, a PDA (Personal Digital Assistant) etc. *See also* 1[pre] above. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Abe '171 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Abe '171 at Fig. 36

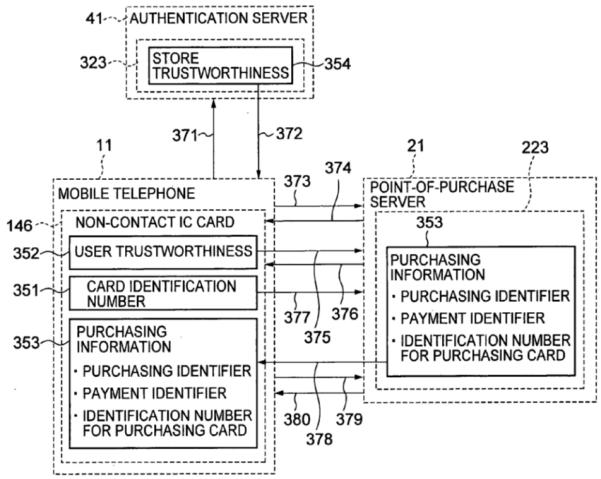
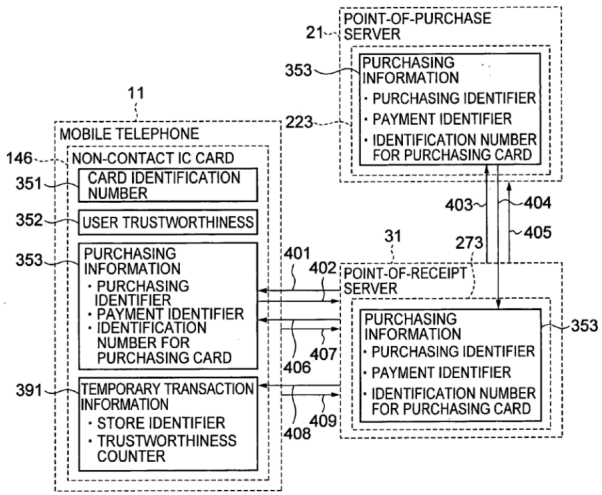
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 36  Abe '171 at [0147] Electronic money information is stored in the EEPROM 164. The user is then able to settle fees for purchased products and services etc. by utilizing this electronic money. The settlement history is also stored in an EEPROM 164. Abe '171 at claim 26 first acquiring means for acquiring information relating to a commercial transaction employed in user authentication from said information processing apparatus during product purchasing; Abe '171 at claim 27 first acquiring means for acquiring information relating to a commercial transaction employed in user authentication from said information processing apparatus during product purchasing; To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.

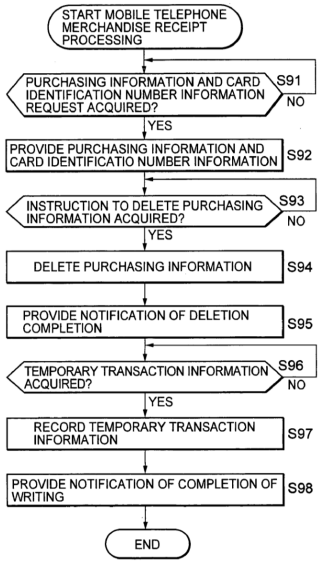
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Abe '171 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Abe '171 at Fig. 36 FIG. 36  Abe '171 at [0147] Electronic money information is stored in the EEPROM 164. The user is then able to settle fees for purchased products and services etc. by utilizing this electronic money. The settlement history is also stored in an EEPROM 164. Abe '171 at claim 26 first acquiring means for acquiring information relating to a commercial transaction employed in user authentication from said information processing apparatus during product purchasing; Abe '171 at claim 27 first acquiring means for acquiring information relating to a commercial transaction employed in user authentication from said information processing apparatus during product purchasing;

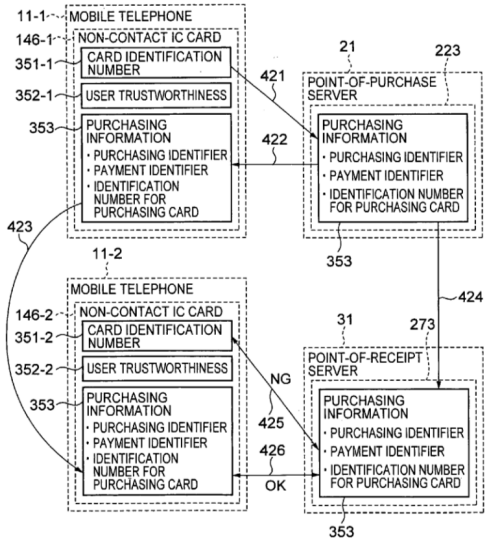
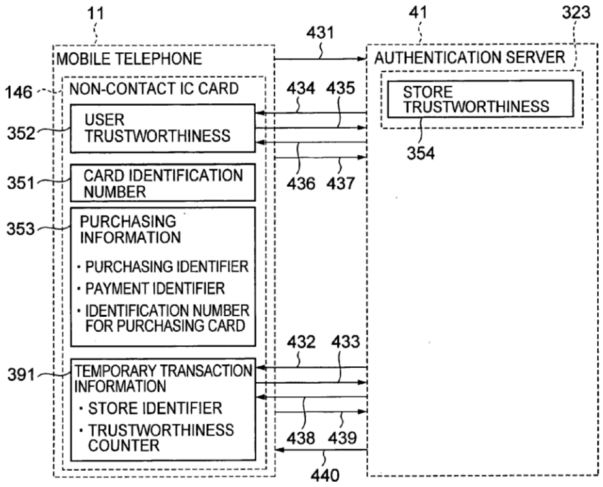
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Abe '171 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Abe '171 at Abstract The present invention relates to an information processing system, information communication terminal and method, information processing apparatus and method, recording medium, and program capable of enabling safer electronic commercial transactions in a straightforward manner. A point-of-purchase server 21 generates purchasing information using a card Identification number allotted to a non-contact IC-card of a mobile telephone 11. A point-of-receipt server 31 acquires this purchasing information and confirms the card identification number allotted to the non-contact IC card of the mobile telephone 11 and a purchasing card identification number. The authentication server 41 calculates user trustworthiness and store trustworthiness based on temporary commercial transaction information stored in the non-contact IC card of the mobile telephone 11. The calculated user trustworthiness and store trustworthiness is then reference by the mobile telephone 11 and point-of-purchase server 21 in the next commercial transaction. The present invention can be applied to electronic commercial transaction services. Abe '171 at Figure 2

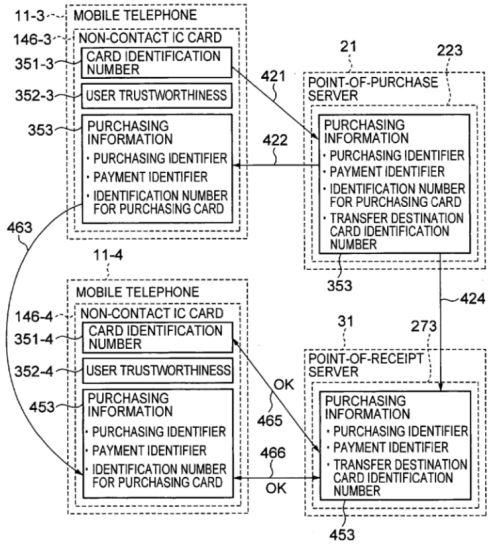
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 2  Abe '171 at Figure 4 FIG. 4  Abe '171 at Figure 5

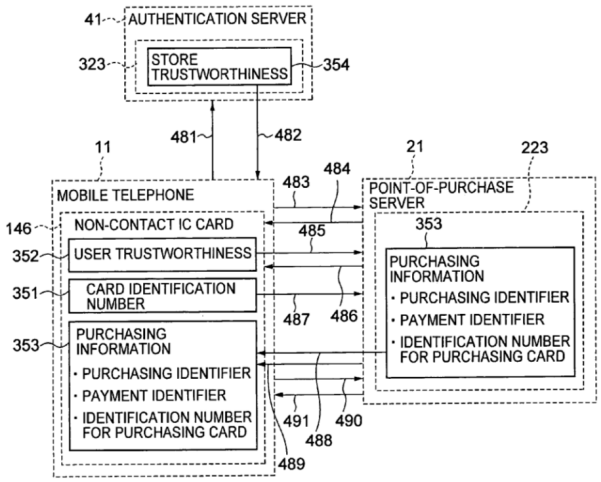
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 5  Abe '171 at Fig.11A–D FIG. 11A  FIG. 11B  FIG. 11C  FIG. 11D  Abe '171 at Fig. 12

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 12  Abe '171 at Fig. 18 FIG. 18  Abe '171 at Fig. 19

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 19  Abe '171 at Fig. 23

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 23  Abe '171 at Fig. 24 FIG. 24 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at Fig. 29 FIG. 29  Abe '171 at Fig. 36

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 36  Abe '171 at [0006] An information processing system of the present invention is characterized by an information communication terminal connected to a network, for holding information relating to a commercial transaction and an information processing apparatus connected to the network, for managing information relating to the commercial transaction, wherein the information communication terminal comprises first acquiring means for acquiring information relating to the commercial transaction from the information processing apparatus during merchandise purchasing, first storage means for storing information relating to the commercial transaction acquired by the first acquiring means, and first providing means for providing information relating to the commercial transaction stored by the first storage means to the information processing apparatus during receipt of merchandise, wherein the information processing apparatus comprises second providing means for providing information relating to the commercial transaction to the information communication terminal during merchandise sales, second storage means for storing information relating to the commercial transaction, second acquiring means for acquiring information relating to the commercial transaction from the information communication terminal during merchandise delivery, and authentication means for authenticating information relating to said commercial transaction acquired by the second acquiring means using information relating to the commercial transaction stored by the second storage means. Abe '171 at [0007]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	A second information processing system of the present invention is characterized by an information communication terminal connected to a network, for holding information relating to a commercial transaction, a first information processing apparatus connected to the network, for managing information relating to the commercial transaction, and a second information processing apparatus connected to the network, for managing information relating to trustworthiness of a first user constituting a user of the information communication terminal and information relating to trustworthiness of a second user constituting a user of the first information processing apparatus, wherein the information communication terminal comprises first storage means for storing information relating to trustworthiness of the first user, first providing means for providing information relating to trustworthiness of the first user stored by the first storage means to the first information processing apparatus, first acquiring means for acquiring information relating to trustworthiness of the second user from the second information processing apparatus, second acquiring means for acquiring information relating to the commercial transaction from the first information processing apparatus, first providing means for providing trustworthiness of the first user stored by the first storage means and information relating to the commercial transaction acquired by the second acquiring means to the second information processing apparatus, and third acquiring means for acquiring information relating to trustworthiness of the first user updated by the second information processing apparatus, wherein the first information processing apparatus comprises fourth acquiring means for acquiring information relating to trustworthiness of the first user from the information communication terminal, and second providing means for providing information relating to the commercial transaction to the information communication terminal, and the second information processing apparatus comprises second storage means for storing information relating to trustworthiness of the second user, second providing means for providing information relating to trustworthiness of the second user stored by the second storage means to the information communication terminal, fifth acquiring means for acquiring information relating to the first user from the information communication terminal and information relating to the commercial transaction, updating means for updating information relating to the first user acquired by the fifth acquiring means and information relating to trustworthiness of the second user stored by the second storage means based on information relating to the commercial transaction acquired by the fifth acquiring means, and third providing means for providing the information relating to trustworthiness of the first user updated by the updating means to the information communication terminal. Abe ’171 at [0037] FIG. 2 is a view showing an example configuration for the external appearance of the mobile telephone of FIG. 1.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0040] FIG. 5 is a block view showing a detailed example of a configuration for a non-contact IC card of FIG. 4. Abe '171 at [0041] FIG. 5 is a view showing an example of a specification for the non-contact IC card of FIG. 4. Abe '171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe '171 at [0110] A memory stick slot 120 for installing a freely detachable memory stick (registered trademark) 121 is provided at an upper part of the left side of the main body 11B. When the memo button 117 is pressed down, the mobile telephone 11 records speech of the person being called in the installed memory stick 121. The mobile telephone 11 records e-mail, simple homepages and images taken using the camera 114 in the installed memory stick 131 according to user operations. Abe '171 at [0112] Because the mobile telephone 11 is configured so as to be capable of being installed with this kind of memory stick 121, it is possible to share data with other electronic equipment via the memory stick 121. Abe '171 at [0113] It is possible to extend the functions of the mobile telephone 11 still further by incorporating a module (chip) for extending prescribed functions into the memory stick 121 and installing this in the memory stick slot 120.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0114] For example, as described in the following, by installing the memory stick 121 incorporating a non-contact IC (Integrated Circuit) card in the mobile telephone 11, it is possible to extend the functions so as to give the same electronic commercial transaction functions as for non-contact IC cards even when, for example, these modules are not built-into the mobile telephone 11. Abe '171 at [0116] A power supply circuit 135, operation input control unit 132, image encoder 133, camera interface (I/F) unit 134, LCD control unit 136, multiple separator 138, modulator/demodulator circuit 139, audio codec 140, infrared communication unit 145 and non-contact IC card 146 (in this example, a dedicated non-contact IC card (Felica chip (registered trademark)) is provided but it is also possible to provide non-contact IC card functions in the memory stick 121) are connected to a main control unit 131 for providing overall control of each part of the display unit 11A and body 11B via a main bus 141, and the image encoder 133, image decoder 137, multiple separator 138, a memory stick controller 143, the modulator/demodulator circuit 139, and the audio codec 140 are connected via a synchronous bus 142. Abe '171 at [0118] The main control unit 131 constituted by a CPU (Central Processing Unit), ROM (Read Only Memory) and RAM (Random Access Memory) etc. converts an audio signal collected by the microphone 118 into a digital audio signal using the audio codec 140 at the time of audio call mode. The digital audio data is subjected to spectrum diffusion processing by the modulator/demodulator circuit 139, subjected to digital/analog conversion processing and frequency conversion processing by a transceiver circuit 144, and is transmitted via the antenna 112. Abe '171 at [0134] The non-contact IC card 146 may then be brought close to another information processing apparatus having an IC card reader/writer so that when electromagnetic waves radiated from the IC card reader/writer are received, various information is provided to the IC card reader/writer in response to this. Abe '171 at [0137] The non-contact IC card 146 is comprised of, for example, an antenna (loop antenna) 170 and capacitor 171 shown in the drawing, and an IC storing other aspects of the configuration on one chip. The non-contact IC card 146 then communicates various types of data with an IC card reader/writer provided at

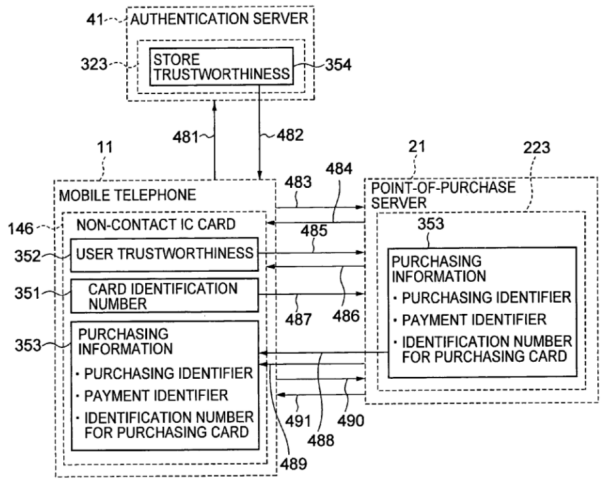
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	another information processing apparatus in a half-duplex manner by utilizing electromagnetic induction, and does not by any means have to be card-shaped. Further, “IC card” is a name given for convenience of description, and is intended to mean functions described above or described in the following. Further, for example, a Felica chip (registered trademark) may also be given as a device providing substantially the same functions as the non-contact IC card 146. Abe ’171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. Abe ’171 at [0178] The mobile telephone 11 shown in FIG. 11A holds information for a card identification number 351 and user trustworthiness 352 in the built-in non-contact IC card 146. Abe ’171 at [0221] In step S25, the main control unit 131 determines whether or not a request for this card identification number information has been acquired, and waits until it is determined that acquisition has taken place. When it is determined that a card identification number information request has been acquired, the main control unit 131 advances processing to step S26, the card identification number 351 is acquired from the non-contact IC card 146, and card identification number information containing this card identification number 351 is provided to the point-of-purchase server 21 via the network 10. This processing corresponds to the processing of arrow 377 of FIG. 12. Abe ’171 at [0244] In step S71 of FIG. 17, the CPU 201 controls the communication unit 224 so as to make a request for card identification number information of the non-contact IC card 146 built-into the mobile telephone 11. This processing corresponds to the processing of arrow 376 of FIG. 12. Abe ’171 at [0248] When purchasing/charging processing is complete, in step S74, the CPU 201 generates purchasing information relating to sale of merchandise on this occasion, and controls the communication unit 224 so that this generated purchasing information is provided to the mobile telephone 11 via the network 10 so as

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	to be stored in the non-contact IC card 146. This processing corresponds to the processing of arrow 378 of FIG. 12. Abe '171 at [0257] In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance by the point-of-purchase 20. The user then positions the mobile telephone 11 in the vicinity of the IC card reader/writer 275 of the point-of-receipt server 31 installed at the point of receipt 30, and positions the non-contact IC card 146 built-into the mobile telephone 11 in the vicinity of the IC card reader/writer 275. Abe '171 at [0266] The mobile telephone 11 then records the provided temporary commercial transaction information 391 in the non-contact IC card 146 using the acquired temporary commercial transaction information rewriting key 362. When recording is complete, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362, and provides the notification of completion of writing to the point-of-receipt server 31 (arrow 409) so as to complete processing relating to handing over of the merchandise. Abe '171 at [0271] When it is determined that a request for the purchasing information 353 and the card identification number information has been acquired, the main control unit 131 advances processing to step S92, controls the CPU 161 of the non-contact IC card 146, and provides card identification number information containing the requested purchasing information 353, and card identification number 351 to the point-of-receipt server 31. This processing corresponds to the processing of arrow 402 of FIG. 18. Abe '171 at [0273] In step S93, the main control unit 131 controls the CPU 161 of the non-contact IC card 146 so as to determine whether or not an instruction to delete the purchasing information rewriting key 361 from the point-of-receipt server 31 and the purchasing information has been acquired, and waits until it is determined that acquisition has taken place. Abe '171 at [0282]

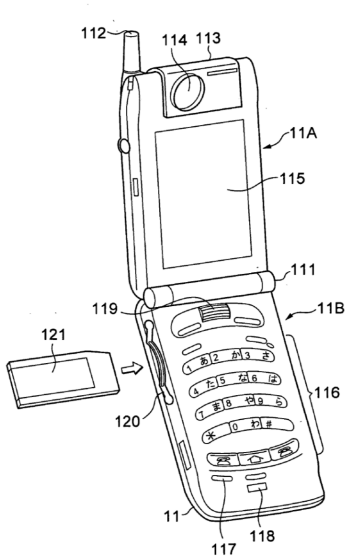
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0307] For example, as shown in FIG. 23, when a user of a mobile telephone 11-1 purchases merchandise from the point-of-purchase 20, the point-of-purchase server 21 generates purchasing information 353 (arrow 421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422). Abe '171 at [0319] The authentication server 41 that has accessed the mobile telephone 11 then, as described in the following, requests temporary commercial transaction information 391 stored in the non-contact IC card 146 of the mobile telephone 11. Abe '171 at [0347] The main control unit 131 of the mobile telephone 11 that has acquired the user trustworthiness information then updates the user trustworthiness 352 stored in the non-contact IC card 146 and provides this to the authentication server 41 using the processing of step S181 of FIG. 26. Abe '171 at [0360] For example, as shown in FIG. 29, when a purchaser mobile telephone 11-3 constituting a mobile telephone used when purchasing merchandise transfers purchasing information 353 stored in a non-contact IC card 146-3 to a transfer destination mobile telephone 11-4, a transfer destination card identification number (i.e. card identification number 351-4) is overwritten (taken to be purchasing information 453) with a purchasing card identification number 353 (i.e. card identification number 351-3) contained in the purchasing information 353, and stored in a non-contact IC card 146-4 of the transfer destination mobile telephone 11-4 (arrow 463). Abe '171 at [0370] When it is determined that a request for the card identification number information of the transfer destination has been acquired, the main control unit 131 advances processing to step S235, a

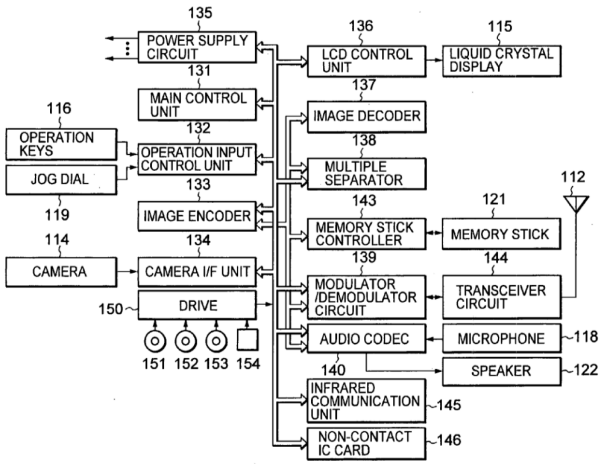
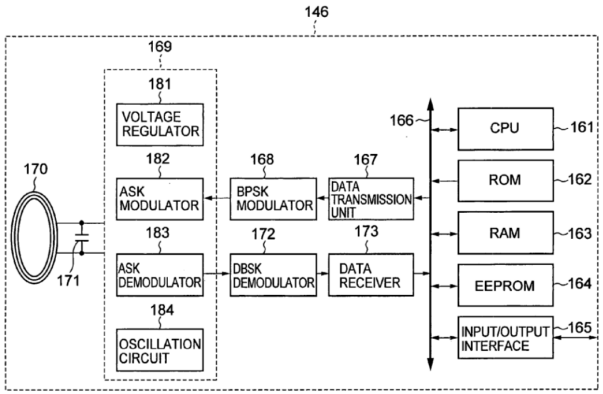
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0371] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-4 is positioned within the communication range of the non-contact IC card 146-3, the CPU 161 of the non-contact IC card 146-3 detects the non-contact IC card 146-4 and notifies the main control unit 131 via antenna 170. Abe '171 at [0378] When it is determined that the updated purchasing information 453 and purchasing information rewriting key 361 have been acquired, the main control unit 131 advances processing to step S241 of FIG. 31, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0380] As described in the following, the transfer destination mobile telephone 11-4 provided with the purchasing information 453 and the purchasing information rewriting key 361 records the updated purchasing information 453 in the non-contact IC card 146-4 using the acquired purchasing information rewriting key 361. When recording is complete, the purchasing information rewriting key 361 is deleted, and completion of writing is provided to the purchaser mobile telephone 11-3. Abe '171 at [0412]–[0413] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-3 is positioned within the communication range of the non-contact IC card 146-4, the CPU 161 of the non-contact IC card 146-4 detects the non-contact IC card 146-3 and notifies the main control unit 131 via the antenna 170. When it is determined that the purchaser mobile telephone 11-3 is within communication range based on information provided by the CPU 161, the main control unit 131 of the transfer destination mobile telephone 11-4 advances processing to step S293, and card identification number information containing the requested card identification number 351-4 is provided to the purchaser mobile telephone 11-3 using short-range wireless communication by the non-contact IC card 146-4.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0420] In the above, a description is given where the point-of-receipt server 31 of the point of receipt 30 holds the purchasing information rewriting key 361, with the purchasing information 353 stored in the non-contact IC card 146 being deleted after delivery of the merchandise. However, the present invention is by no means limited in this respect, and this electronic commercial transaction system may be simplified by not having the point-of-receipt server 31 delete the purchasing information. Abe '171 at [0454] In the case in FIG. 42, as in the case in FIG. 18, when the non-contact IC card 146 is positioned with communication range of short-range wireless communication of the IC card reader/writer 275, the point-of-receipt server 31 the mobile telephone 11 is in the proximity of makes a request to (arrow 501) and acquires from (arrow 502) the mobile telephone 11 purchasing information 353 and the card identification number 351. Abe '171 at [0460] Namely, in step S381, the main control unit 131 of the mobile telephone 11 controls the non-contact IC card 146 so as to determine whether or not a request for card identification number information containing the purchasing information 353 and card identification number 351 has been acquired from the point-of-receipt server 31, and waits until it is determined that acquisition has taken place. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Abe '171 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Abe '171 at Fig. 36

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 36  Abe '171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe '171 at [0093] The mobile telephone 11 is operated by the user so as to carry out wireless communication with the nearest base station 12, access the point-of-purchase server 21 via the network 10, and carry out merchandise purchasing processing. The mobile telephone 11 is operated by the user so as to access the authentication server 41 of the authentication service provider 40, trustworthiness of the point-of-purchase 20 is acquired, and this is provided to the user to enable a determination to be made as to whether or not to purchase the merchandise (product).

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Abe '171 discloses or renders obvious "[a] mobile device." For example: *See* above at 1[pre]. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Abe '171 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a]. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Abe '171 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Abe '171 at Abstract The present invention relates to an information processing system, information communication terminal and method, information processing apparatus and method, recording medium, and program capable of enabling safer electronic commercial transactions in a straightforward manner. A point-of-purchase server 21 generates purchasing information using a card Identification number allotted to a non-contact IC-card of a mobile telephone 11. A point-of-receipt server 31 acquires this purchasing information and confirms the card identification number allotted to the non-contact IC card of the mobile telephone 11 and a purchasing card identification number. The authentication server 41 calculates user trustworthiness and store trustworthiness based on temporary commercial transaction information stored in the non-contact IC card of the mobile telephone 11. The calculated user trustworthiness and store trustworthiness is then

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	reference by the mobile telephone 11 and point-of-purchase server 21 in the next commercial transaction. The present invention can be applied to electronic commercial transaction services. Abe '171 at Figure 2 FIG. 2  Abe '171 at Figure 4

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 4  Abe '171 at Figure 5 FIG. 5  Abe '171 at Fig.11A–D

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")

FIG. 11A

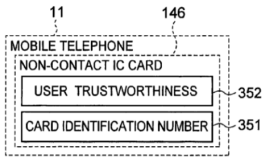


FIG. 11B

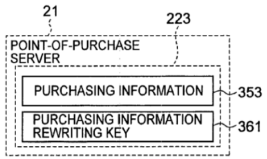


FIG. 11C

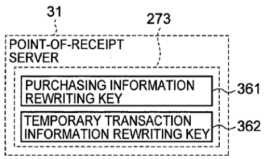
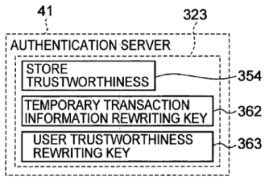
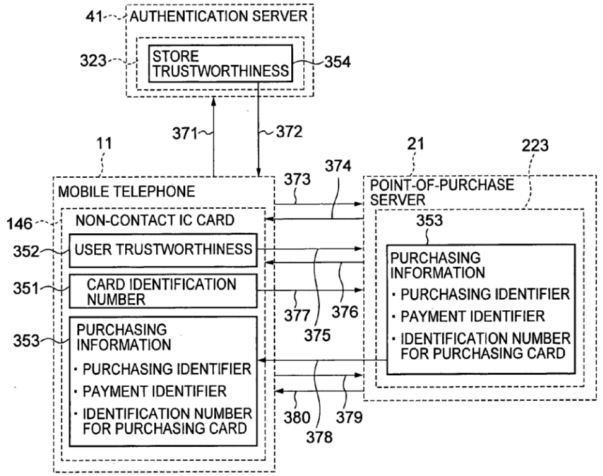


FIG. 11D

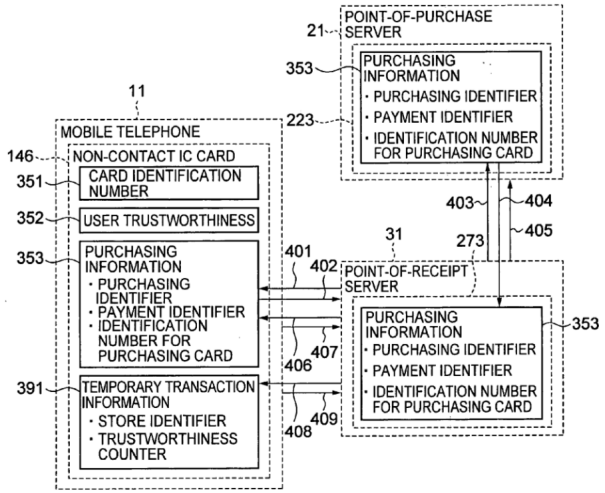
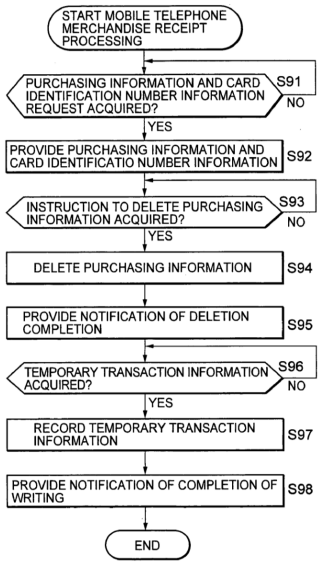


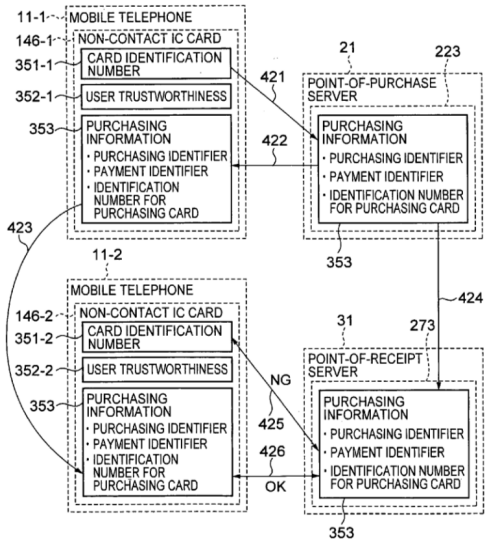
Abe '171 at Fig. 12

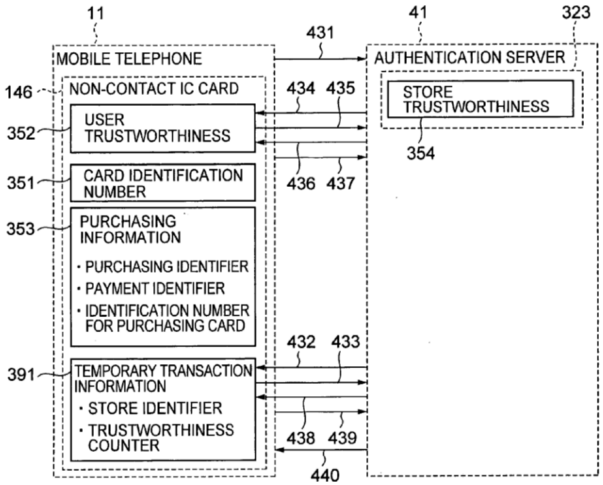
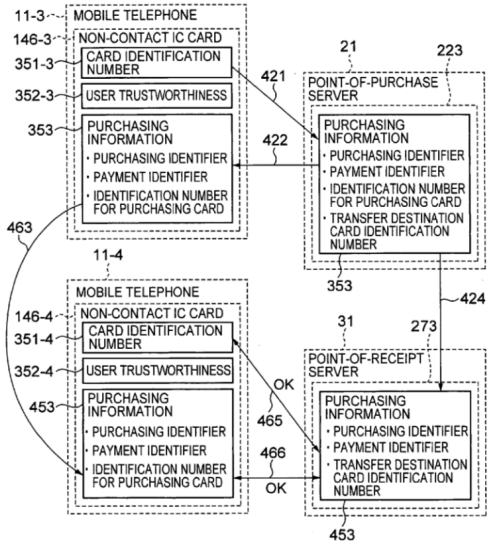
FIG. 12

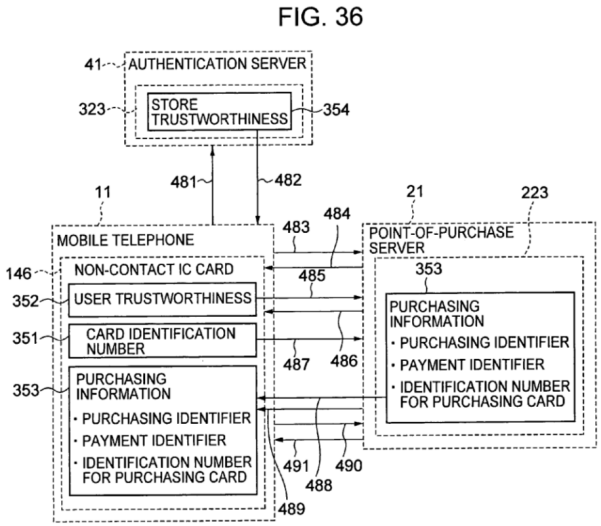


Abe '171 at Fig. 18

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 18  Abe '171 at Fig. 19 FIG. 19 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at Fig. 23 FIG. 23  Abe '171 at Fig. 24

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 24  Abe '171 at Fig. 29 FIG. 29 

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at Fig. 36  Abe '171 at [0037] FIG. 2 is a view showing an example configuration for the external appearance of the mobile telephone of FIG. 1. Abe '171 at [0040] FIG. 5 is a block view showing a detailed example of a configuration for a non-contact IC card of FIG. 4. Abe '171 at [0041] FIG. 5 is a view showing an example of a specification for the non-contact IC card of FIG. 4. Abe '171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe '171 at [0093] The mobile telephone 11 is operated by the user so as to carry out wireless communication with the nearest base station 12, access the point-of-purchase server 21 via the network 10, and carry out merchandise purchasing processing. The mobile telephone 11 is operated by the user so as to access the authentication server 41 of the authentication service provider 40, trustworthiness of the point-of-purchase 20 is acquired, and this is provided to the user to enable a determination to be made as to whether or not to purchase the merchandise (product). Abe '171 at [0110] A memory stick slot 120 for installing a freely detachable memory stick (registered trademark) 121 is provided at an upper part of the left side of the main body 11B. When the memo button 117 is pressed down, the mobile telephone 11 records speech of the person being called in the installed memory stick 121. The mobile telephone 11 records e-mail, simple homepages and images taken using the camera 114 in the installed memory stick 131 according to user operations. Abe '171 at [0113] It is possible to extend the functions of the mobile telephone 11 still further by incorporating a module (chip) for extending prescribed functions into the memory stick 121 and installing this in the memory stick slot 120. Abe '171 at [0114] For example, as described in the following, by installing the memory stick 121 incorporating a non-contact IC (Integrated Circuit) card in the mobile telephone 11, it is possible to extend the functions so as to give the same electronic commercial transaction functions as for non-contact IC cards even when, for example, these modules are not built-into the mobile telephone 11. Abe '171 at [0116] A power supply circuit 135, operation input control unit 132, image encoder 133, camera interface (I/F) unit 134, LCD control unit 136, multiple separator 138, modulator/demodulator circuit 139, audio codec 140, infrared communication unit 145 and non-contact IC card 146 (in this example, a dedicated non-

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	contact IC card (Felica chip (registered trademark)) is provided but it is also possible to provide non-contact IC card functions in the memory stick 121) are connected to a main control unit 131 for providing overall control of each part of the display unit 11A and body 11B via a main bus 141, and the image encoder 133, image decoder 137, multiple separator 138, a memory stick controller 143, the modulator/demodulator circuit 139, and the audio codec 140 are connected via a synchronous bus 142. Abe ’171 at [0134] The non-contact IC card 146 may then be brought close to another information processing apparatus having an IC card reader/writer so that when electromagnetic waves radiated from the IC card reader/writer are received, various information is provided to the IC card reader/writer in response to this. Abe ’171 at [0137] The non-contact IC card 146 is comprised of, for example, an antenna (loop antenna) 170 and capacitor 171 shown in the drawing, and an IC storing other aspects of the configuration on one chip. The non-contact IC card 146 then communicates various types of data with an IC card reader/writer provided at another information processing apparatus in a half-duplex manner by utilizing electromagnetic induction, and does not by any means have to be card-shaped. Further, “IC card” is a name given for convenience of description, and is intended to mean functions described above or described in the following. Further, for example, a Felica chip (registered trademark) may also be given as a device providing substantially the same functions as the non-contact IC card 146. Abe ’171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. Abe ’171 at [0178] The mobile telephone 11 shown in FIG. 11A holds information for a card identification number 351 and user trustworthiness 352 in the built-in non-contact IC card 146. Abe ’171 at [0221] In step S25, the main control unit 131 determines whether or not a request for this card identification number information has been acquired, and waits until it is determined that acquisition has taken place. When it is determined that a card identification number information request has been acquired, the main

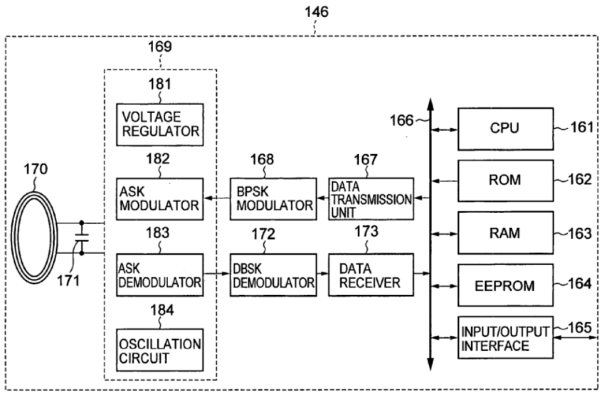
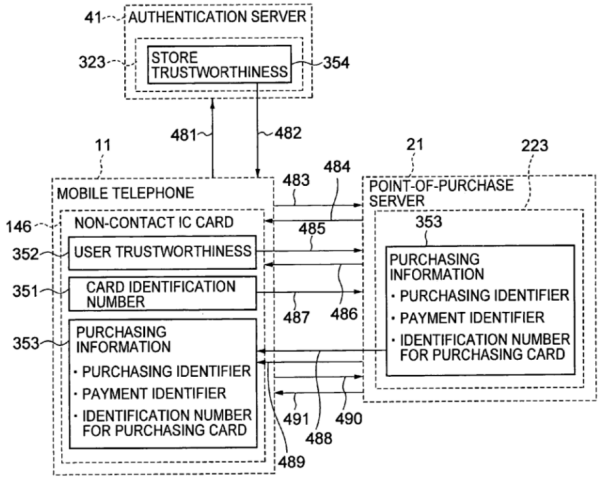
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	control unit 131 advances processing to step S26, the card identification number 351 is acquired from the non-contact IC card 146, and card identification number information containing this card identification number 351 is provided to the point-of-purchase server 21 via the network 10. This processing corresponds to the processing of arrow 377 of FIG. 12. Abe '171 at [0244] In step S71 of FIG. 17, the CPU 201 controls the communication unit 224 so as to make a request for card identification number information of the non-contact IC card 146 built-into the mobile telephone 11. This processing corresponds to the processing of arrow 376 of FIG. 12. Abe '171 at [0248] When purchasing/charging processing is complete, in step S74, the CPU 201 generates purchasing information relating to sale of merchandise on this occasion, and controls the communication unit 224 so that this generated purchasing information is provided to the mobile telephone 11 via the network 10 so as to be stored in the non-contact IC card 146. This processing corresponds to the processing of arrow 378 of FIG. 12. Abe '171 at [0257] In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance by the point-of-purchase 20. The user then positions the mobile telephone 11 in the vicinity of the IC card reader/writer 275 of the point-of-receipt server 31 installed at the point of receipt 30, and positions the non-contact IC card 146 built-into the mobile telephone 11 in the vicinity of the IC card reader/writer 275. Abe '171 at [0266] The mobile telephone 11 then records the provided temporary commercial transaction information 391 in the non-contact IC card 146 using the acquired temporary commercial transaction information rewriting key 362. When recording is complete, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362, and provides the notification of completion of writing to the point-of-receipt server 31 (arrow 409) so as to complete processing relating to handing over of the merchandise. Abe '171 at [0271]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	When it is determined that a request for the purchasing information 353 and the card identification number information has been acquired, the main control unit 131 advances processing to step S92, controls the CPU 161 of the non-contact IC card 146, and provides card identification number information containing the requested purchasing information 353, and card identification number 351 to the point-of-receipt server 31. This processing corresponds to the processing of arrow 402 of FIG. 18. Abe '171 at [0273] In step S93, the main control unit 131 controls the CPU 161 of the non-contact IC card 146 so as to determine whether or not an instruction to delete the purchasing information rewriting key 361 from the point-of-receipt server 31 and the purchasing information has been acquired, and waits until it is determined that acquisition has taken place. Abe '171 at [0282] When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0307] For example, as shown in FIG. 23, when a user of a mobile telephone 11-1 purchases merchandise from the point-of-purchase 20, the point-of-purchase server 21 generates purchasing information 353 (arrow 421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422). Abe '171 at [0319] The authentication server 41 that has accessed the mobile telephone 11 then, as described in the following, requests temporary commercial transaction information 391 stored in the non-contact IC card 146 of the mobile telephone 11. Abe '171 at [0347] The main control unit 131 of the mobile telephone 11 that has acquired the user trustworthiness information then updates the user trustworthiness 352 stored in the non-contact IC card 146 and provides this to the authentication server 41 using the processing of step S181 of FIG. 26.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0360] For example, as shown in FIG. 29, when a purchaser mobile telephone 11-3 constituting a mobile telephone used when purchasing merchandise transfers purchasing information 353 stored in a non-contact IC card 146-3 to a transfer destination mobile telephone 11-4, a transfer destination card identification number (i.e. card identification number 351-4) is overwritten (taken to be purchasing information 453) with a purchasing card identification number 353 (i.e. card identification number 351-3) contained in the purchasing information 353, and stored in a non-contact IC card 146-4 of the transfer destination mobile telephone 11-4 (arrow 463). Abe '171 at [0370] When it is determined that a request for the card identification number information of the transfer destination has been acquired, the main control unit 131 advances processing to step S235, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0378] When it is determined that the updated purchasing information 453 and purchasing information rewriting key 361 have been acquired, the main control unit 131 advances processing to step S241 of FIG. 31, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0380] As described in the following, the transfer destination mobile telephone 11-4 provided with the purchasing information 453 and the purchasing information rewriting key 361 records the updated purchasing information 453 in the non-contact IC card 146-4 using the acquired purchasing information rewriting key 361. When recording is complete, the purchasing information rewriting key 361 is deleted, and completion of writing is provided to the purchaser mobile telephone 11-3. Abe '171 at [0412]–[0413] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-3 is positioned within the communication range of the

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	non-contact IC card 146-4, the CPU 161 of the non-contact IC card 146-4 detects the non-contact IC card 146-3 and notifies the main control unit 131 via the antenna 170. When it is determined that the purchaser mobile telephone 11-3 is within communication range based on information provided by the CPU 161, the main control unit 131 of the transfer destination mobile telephone 11-4 advances processing to step S293, and card identification number information containing the requested card identification number 351-4 is provided to the purchaser mobile telephone 11-3 using short-range wireless communication by the non-contact IC card 146-4. Abe '171 at [0420] In the above, a description is given where the point-of-receipt server 31 of the point of receipt 30 holds the purchasing information rewriting key 361, with the purchasing information 353 stored in the non-contact IC card 146 being deleted after delivery of the merchandise. However, the present invention is by no means limited in this respect, and this electronic commercial transaction system may be simplified by not having the point-of-receipt server 31 delete the purchasing information. Abe '171 at [0454] In the case in FIG. 42, as in the case in FIG. 18, when the non-contact IC card 146 is positioned with communication range of short-range wireless communication of the IC card reader/writer 275, the point-of-receipt server 31 the mobile telephone 11 is in the proximity of makes a request to (arrow 501) and acquires from (arrow 502) the mobile telephone 11 purchasing information 353 and the card identification number 351. Abe '171 at [0460] Namely, in step S381, the main control unit 131 of the mobile telephone 11 controls the non-contact IC card 146 so as to determine whether or not a request for card identification number information containing the purchasing information 353 and card identification number 351 has been acquired from the point-of-receipt server 31, and waits until it is determined that acquisition has taken place. *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Patent Owner's Ex. 2020
Page 091

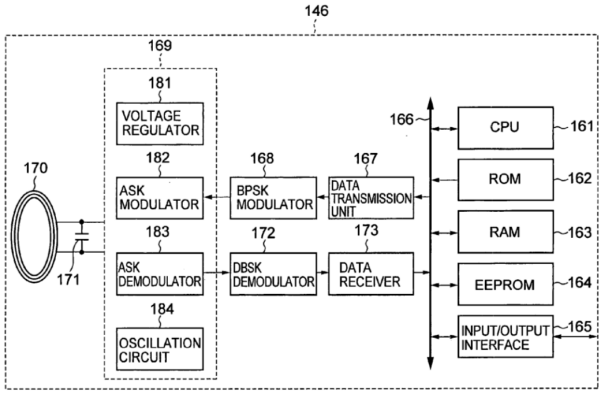
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Abe '171 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Abe '171 at Figure 5 FIG. 5  Abe '171 at Fig. 36 FIG. 36  Abe '171 at [0009]

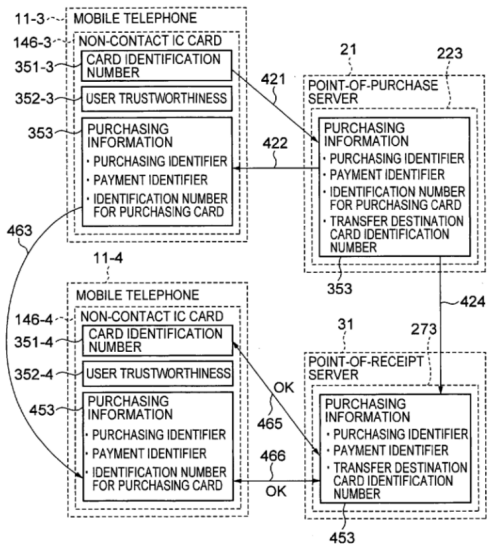
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	The information communication device is further characterized by wireless communication means for carrying out short-range wireless communication via electromagnetic radiation with the first information processing apparatus in close proximity. The first providing means is then capable of providing information relating to the commercial transaction to the first information processing apparatus using short-range wireless communication by the wireless communication means. Abe ’171 at [0030] The first information processing system of the present invention is provided with an information communication terminal connected to a network, for holding information relating to a commercial transaction and an information processing apparatus connected to the network, for managing information relating to the commercial transaction. At the information communication terminal, information relating to the commercial transaction is acquired from the information processing apparatus during merchandise purchasing. Acquired information relating to the commercial transaction is then stored. Information relating to the stored commercial transaction is then provided to the information processing apparatus during receipt of the merchandise. At the information processing apparatus, information relating to the commercial transaction is provided to the information communication terminal during merchandise sales and stored. Information relating to the commercial transaction is then acquired from the information communication terminal during merchandise delivery. Information relating to the acquired commercial transaction is then authenticated using information relating to the stored commercial transaction. Abe ’171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe ’171 at [0101] The display unit 11A has an antenna 112 for transmitting and receiving signals that is capable of being pulled out or stored provided at an upper part of a left end. The mobile telephone 11 transmits and

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112. Abe ’171 at [0118] The main control unit 131 constituted by a CPU (Central Processing Unit), ROM (Read Only Memory) and RAM (Random Access Memory) etc. converts an audio signal collected by the microphone 118 into a digital audio signal using the audio codec 140 at the time of audio call mode. The digital audio data is subjected to spectrum diffusion processing by the modulator/demodulator circuit 139, subjected to digital/analog conversion processing and frequency conversion processing by a transceiver circuit 144, and is transmitted via the antenna 112. Abe ’171 at [0134] The non-contact IC card 146 may then be brought close to another information processing apparatus having an IC card reader/writer so that when electromagnetic waves radiated from the IC card reader/writer are received, various information is provided to the IC card reader/writer in response to this. Abe ’171 at [0137] The non-contact IC card 146 is comprised of, for example, an antenna (loop antenna) 170 and capacitor 171 shown in the drawing, and an IC storing other aspects of the configuration on one chip. The non-contact IC card 146 then communicates various types of data with an IC card reader/writer provided at another information processing apparatus in a half-duplex manner by utilizing electromagnetic induction, and does not by any means have to be card-shaped. Further, “IC card” is a name given for convenience of description, and is intended to mean functions described above or described in the following. Further, for example, a Felica chip (registered trademark) may also be given as a device providing substantially the same functions as the non-contact IC card 146. Abe ’171 at [0140] At the interface 169, an alternating magnetic field excited at the antenna 170 is rectified by the ASK demodulator 183, and this is stabilized at a voltage regulator 181 and supplied to each part as a direct current power source. The electric power of electromagnetic waves radiated from the IC card reader/writer is regulated to as to generate an electric field covering the required electric power at the non-contact IC card as described in the following. Abe ’171 at [0153]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. Abe '171 at [0169]–[0170] When response data from the non-contact IC card 146 is supplied from the demodulation unit 294, the SPU 306 subjects this data to, for example, BPSK demodulation (decoding of Manchester code) etc., and provides the acquired data to the CPU 301. Further, when a command sent to the non-contact IC card 146 is provided via the bus 305, the SPU 306 subjects this command to BPSK modulation (encoding to Manchester code), and the acquired data is outputted to the modulator 292. The modulator 292 ASK modulates a carrier wave of a prescribed frequency (for example, 13.56 MHz) supplied by an oscillating circuit (OSC) 293 based on data supplied by the SPU 306, and outputs the generated modulated wave from an antenna 295 as electromagnetic radiation. On the other hand, the demodulator 294 demodulates a modulated wave (ASK modulated wave) acquired via the antenna 295 and outputs the demodulated data to the SPU 296. Abe '171 at [0282] When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0370] When it is determined that a request for the card identification number information of the transfer destination has been acquired, the main control unit 131 advances processing to step S235, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. Abe '171 at [0371] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-4 is positioned within the communication range of the non-

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	contact IC card 146-3, the CPU 161 of the non-contact IC card 146-3 detects the non-contact IC card 146-4 and notifies the main control unit 131 via antenna 170. Abe '171 at [0378] When it is determined that the updated purchasing information 453 and purchasing information rewriting key 361 have been acquired, the main control unit 131 advances processing to step S241 of FIG. 31, a determination is made as to whether or not the transfer destination mobile telephone 11-4 is within communication range of short-range wireless communication by the non-contact IC card 146-3, and determination that this is the case is awaited. *See also* 1[c] and claim 5 above. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	Abe '171 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: *See* above at [1d]. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Abe '171 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Abe '171 at Abstract The present invention relates to an information processing system, information communication terminal and method, information processing apparatus and method, recording medium, and program capable of enabling safer electronic commercial transactions in a straightforward manner. A point-of-purchase server 21 generates purchasing information using a card Identification number allotted to a non-contact IC-card of a mobile telephone 11. A point-of-receipt server 31 acquires this purchasing information and confirms the card identification number allotted to the non-contact IC card of the mobile telephone 11 and a purchasing card identification number. The authentication server 41 calculates user trustworthiness and store trustworthiness based on temporary commercial transaction information stored in the non-contact IC

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	card of the mobile telephone 11. The calculated user trustworthiness and store trustworthiness is then reference by the mobile telephone 11 and point-of-purchase server 21 in the next commercial transaction. The present invention can be applied to electronic commercial transaction services. Abe '171 at Figure 5 FIG. 5  Abe '171 at Fig. 29

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 29  Abe '171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10. Abe '171 at [0093] The mobile telephone 11 is operated by the user so as to carry out wireless communication with the nearest base station 12, access the point-of-purchase server 21 via the network 10, and carry out merchandise purchasing processing. The mobile telephone 11 is operated by the user so as to access the authentication server 41 of the authentication service provider 40, trustworthiness of the point-of-purchase

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	20 is acquired, and this is provided to the user to enable a determination to be made as to whether or not to purchase the merchandise (product). Abe '171 at [0137] The non-contact IC card 146 is comprised of, for example, an antenna (loop antenna) 170 and capacitor 171 shown in the drawing, and an IC storing other aspects of the configuration on one chip. The non-contact IC card 146 then communicates various types of data with an IC card reader/writer provided at another information processing apparatus in a half-duplex manner by utilizing electromagnetic induction, and does not by any means have to be card-shaped. Further, "IC card" is a name given for convenience of description, and is intended to mean functions described above or described in the following. Further, for example, a Felica chip (registered trademark) may also be given as a device providing substantially the same functions as the non-contact IC card 146. Abe '171 at [0163] An input/output interface 270 is connected at the bus 260, and an input unit 271 comprised of a keyboard and mouse etc., an output unit 272 comprised of a display consisting of a CRT or LCD etc. and a speaker etc., a storage unit 273 comprised of a hard disc etc., a communication unit 274 comprised of a modem or terminal adapter etc., and an IC card reader/writer 275 for carrying out wireless communication with a non-contact IC card in the vicinity are connected to the input/output interface 270. Abe '171 at [0197] The point-of-purchase server 21 that has acquired the user trustworthiness 352 and confirmed that the user of the mobile telephone 11 is trustworthy then makes a request to the mobile telephone 11 for the card identification number 351 allotted to the non-contact IC card 146 (arrow 376). The mobile telephone 11 then provides the card identification number 351 in response to this request. Abe '171 at [0257] In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance by the point-of-purchase 20. The user then positions the mobile telephone 11 in the vicinity of the IC card reader/writer 275 of the point-of-receipt server 31 installed at the point of receipt 30, and positions the non-contact IC card 146 built-into the mobile telephone 11 in the vicinity of the IC card reader/writer 275.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0258] When the non-contact IC card 146 is positioned within communication range, the point-of-receipt server 31 acquires purchasing information 353 and card identification number information (card identification number 351) stored in the non-contact IC card 146 of the mobile telephone 11 via the IC reader/writer 275 (arrow 401 and arrow 402). Abe '171 at [0266] The mobile telephone 11 then records the provided temporary commercial transaction information 391 in the non-contact IC card 146 using the acquired temporary commercial transaction information rewriting key 362. When recording is complete, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362, and provides the notification of completion of writing to the point-of-receipt server 31 (arrow 409) so as to complete processing relating to handing over of the merchandise. Abe '171 at [0282] When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe '171 at [0395] In step S238 of FIG. 30, the purchaser mobile telephone 11-3 provides the requested card identification number information of the transfer destination to the point-of-purchase server 21. *See also* claim 8 above. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

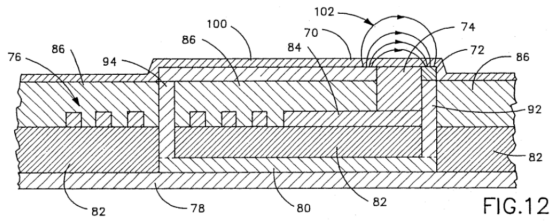
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Abe '171 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example: *See* above at claim 3. To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	To the extent this limitation is not disclosed by Abe '171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe '171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

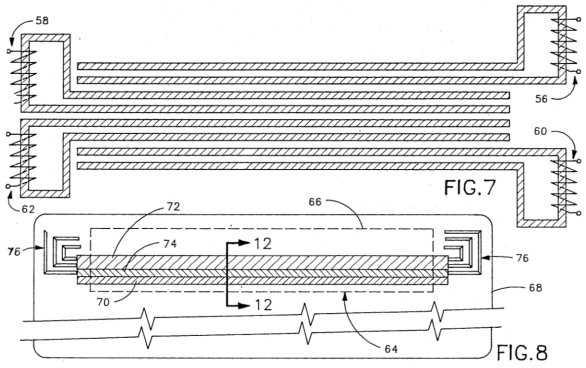
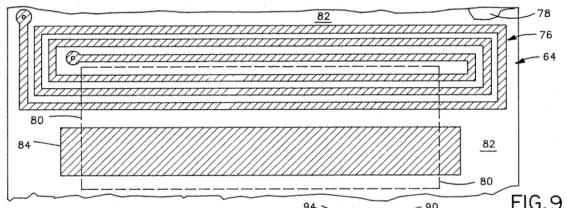
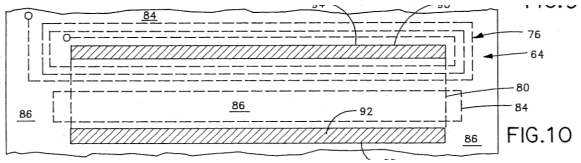
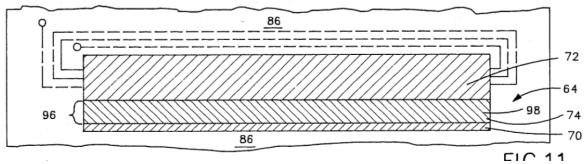
Patent Owner's Ex. 2020
Page 101

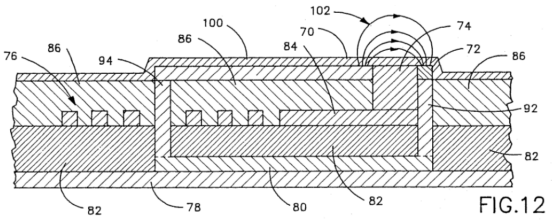
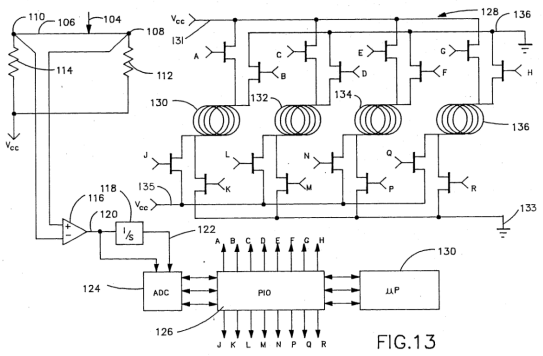
As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Burkhardt '283 and (b) under 35 U.S.C. § 103(a) as obvious over Burkhardt '283 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to US4791283A ("Burkhardt '283")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Burkhardt '283 discloses or renders obvious "[a] mobile device." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figure 12

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 FIG.12 Burkhardt '283 at 1:8–10 The present invention pertains generally to magnetic recording and more specifically to a device for emulating a prerecorded magnetic stripe on a transaction card. Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe. To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Burkhardt '283 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at Figs. 7+8  FIG.7 FIG.8 Burkhardt '283 at Figure 9  FIG. 9 Burkhardt '283 at Figure 10  FIG.10 Burkhardt '283 at Figure 11  FIG. 11

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at Figure 12  FIG.12 Burkhardt '283 at Fig. 13  FIG.13 Burkhardt '283 at 1:8–10 The present invention pertains generally to magnetic recording and more specifically to a device for emulating a prerecorded magnetic stripe on a transaction card. Burkhardt '283 at 1:51–65 U.S. Pat. No. 4,354,099 issued to Rayment et al. discloses an identifier device which interacts with a reader to identify the device. The reader generates a current on drive coil A which interacts with detector coil B to induce a current in drive coil C. The magnetic field which is generated by drive coil C in the identifier is detected by detector coil D in the sensor. Detector coils and drive coils B and C in the identifier are laid out in an array, such as illustrated in FIG. 5. Depending upon which of these coils are interconnected, a specific set of drive coils C are activated to specifically identify the identifier. The

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	United Kingdom Patent Application No. GB2079017A discloses the same invention as disclosed in U.S. Pat. No. 4,354,099, which is the equivalent of the United Kingdom Patent Application. Burkhardt '283 at 1:66–2:10 U.S. Pat. No. 4,253,017 issued to Whitehead on Feb. 24, 1981 discloses a mganetically coded identification card which has a multiplicity of magnetic core spots 20 that can be alternatively recorded in opposite directions. A number of the magnetic core spots are permanently recorded while other spots can be changed to indicate variable information, such as the last port of entry, or egress, and the last use of the card. Data recorded on the magnetic spots may be erased and replaced with new data. Recording is accomplished by energizing coils on horseshoe magnets in the required manner to magnetize the spots to record the variable information. Burkhardt '283 at 2:21–27 Each of the Springer patents referenced above discloses circular magnetic generators for generating magnetic vectors having a spherical geometry which is well defined for the purpose of magnetic image storage with high resolution. The Springer patents disclose various plating techniques for forming the concentric magnetic structures. Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator. Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe.

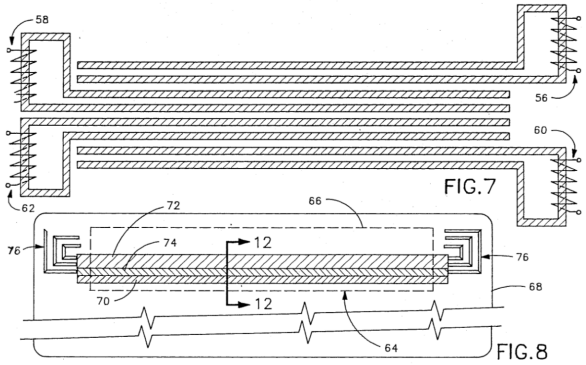
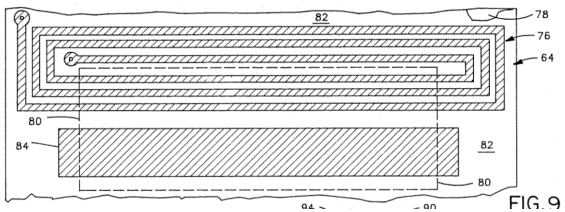
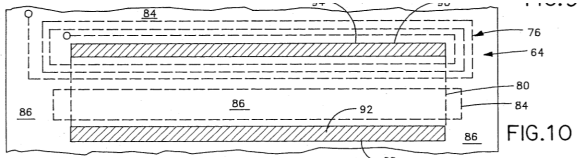
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:9–13 FIG. 13 is a schematic diagram of the device of the present invention for detecting the speed of movement of the card through the card reader and the quadrature driving circuit for applying electrical current to the magnetic field generators. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits.

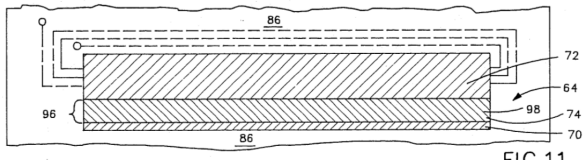
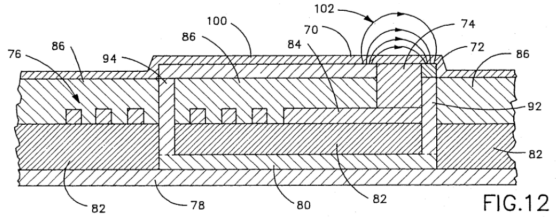
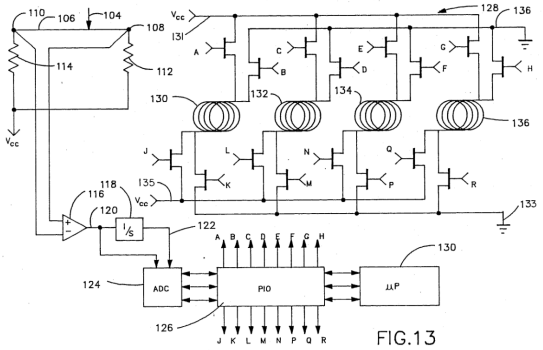
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 6:15–22 FIG. 7 is a schematic plan view illustrating the manner in which four magnetic field generators 56, 58, 60, 62 may be disposed on the card to form four separate magnetic stripes which emulate four prerecorded stripes on a conventional transaction card. Each separate magnetic generator has a separate drive coil for sequentially generating magnetic data on each of the magnetic field generator. Burkhardt '283 at 6:23–31 FIG. 8 is a schematic plan view of the manner in which an alternative magnetic field generator 64 is disposed in the magnetic stripe area 66 of a standard credit card 68. The magnetic field generator 64, illustrated in FIG. 8, comprises a three dimensional structure having pole pieces 70, 72 which are separated by a diamagnetic material 74. Spiral coil 76 is wrapped around the magnetic stand portion which is coupled to magnetic pole portion 72, as disclosed above. Burkhardt '283 at 6:32–51 FIG. 9 is a schematic plan view illustrating the initial steps of forming the magnetic field generator structure 64 of the second embodiment of the present invention. A flexible nonconductive nonpermeable substrate 78 is provided which can form one of the plastic laminate layers of the transaction card of the present invention. A layer of highly permeable material is then applied to the substrate 78 and etched to form a magnetic bottom pole piece 80. Alternatively, the permeable metal can be applied by masking techniques to form the bottom pole piece 80 in the desired configuration. A filler layer 82 of nonconductive, nonpermeable material is then applied over the bottom pole piece 80 and plastic substrate 78 to form a substantially flat surface. A layer of copper or other conductive material is then applied over the filler layer 82 and etched to form a spiral coil 76 and back plane 84. Again, these layers can be applied by any desired process including the use of sputtering, masking techniques, lamination techniques, electro-less and electro-plating, etc. Burkhardt '283 at 6:52–66 FIG. 10 illustrates the next step in forming the magnetic field generator 64 of the second embodiment of the present invention. A second filler layer 86 is applied over the back plane 84, conductive coil 76 and first filler layer 82. The filler layer 84 is then etched to form wells 88, 90 which are aligned directly over the end portions of bottom pole piece 80. A highly permeable material is then placed in wells 88, 90 to form a magnetically conductive stand portions 92, 94, respectively. A magnetic material can comprise a nickel iron material which is powdered and set in a binder which is chemically cured or heat set.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Alternatively, any other desired means of filling wells 88, 90 can be used to form the magnetic stands 92, 94. The magnetic stand 92, 94 must necessarily have magnetic continuity with bottom pole piece 80. Burkhardt '283 at 6:67–7:13 FIG. 11 illustrates the next step in forming the magnetic field generator 64 of the second embodiment of the present invention. A permeable material is applied over the second filler layer 86 and etched to reveal top pole pieces 70, 72. The gap 96 between pole pieces 70, 72 is then etched down to the copper plane 84 through filler layer 86. The well formed by etching the gap portion 96 and filler layer 86 is thn filled with a conductive material 98 to form diamagnetic break 74 between pole pieces 70 and 72. Of necessity, the material forming the magnetic break 74 is in continuous electrical contact with the copper back plane 84. The electrical contact is low in resistance and without break or interruption. A final top protective layer is then applied over the entire structure. Burkhardt '283 at 7:14–29 FIG. 12 is a cross-sectional view of the device as illustrated in FIG. 8. FIG. 12 illustrates the flexible substrate 78, bottom pole piece 80 deposited on the upper surface of flexible substrate 78, filler layer 82 which is applied over the bottom pole piece 80 and flexible substrate 78, the conductive coil 76 and diamagnetic break plane 84 deposited on the upper surface of first filler layer 82, second filler layer 86, magnetic pole stands 92, 94 which are magnetically coupled to bottom pole piece 80, upper pole pieces 70, 72, diamagnetic break 74 and top protective layer 100. As is illustrated in FIG. 12, diamagnetic break 74 prevents the direct passage of magnetic field lines from pole piece 70 to pole piece 72. Magnetic field lines 102 couple pole pieces 70, 72 by protruding vertically from the card for easy coupling with a magnetic read head. Burkhardt '283 at 8:13–36 Quadrature driving circuit 128 is driven by the various contacts A through R which are enabled by the parallel input/output unit 126. Upon application of enable current from contacts A and K, a flux pattern in a first predetermined direction will be generated on coil 130 as a result of current flowing from the voltage source V_{cc} 131 to ground potential 133. Upon application of enable current to connectors B and J, a reverse current is applied through coil 130 to produce a magnetic field in an opposite direction since current flows from V_{cc} 135 to ground potential 136. Coils 130, 132, 134, and 136 are the same coils fabrication earlier as item 76 (FIG. 10) or items 28, 48 (FIG. 4). The other quadrature driving circuits operate in essentially the same manner. For example, if the A-K connection were to indicate a logic one and the B-J connection were to indicate a logic zero, the C-M, E-P, G-R connections would indicate logics ones while the L-D, N-F and Q-H connections would indicate logics zero. In this manner, the four

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	coils 130, 132, 134 and 136 are capable of transmitting data by generating magnetic fields in opposite directions in response to the quadrature driving circuit and thereby simultaneously produce data on four separate magnetic field generators. Burkhardt '283 at 8:37–54 The present invention therefore provides magnetic field generators which are capable of emulating prerecorded magnetic data on a conventional prerecorded magnetic stripe of a transaction card without the necessity of precisely locating the card in a precise predetermined location. The present invention is capable of detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transferred from the microprocessor to the magnetic field generator within the scanning time of the card across the read head of the card reader. Diamagnetic material is used between pole pieces to generate magnetic field lines which extend vertically from the card to thereby increase the field strength adjacent the magnetic field generator outside of the card. Additionally, the card of the present invention can be used with the large number of conventional card readers presently in use with only minor modification. Burkhardt '283 at 9:2–6 1. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader as said card is moved through said card reader, comprising: Burkhardt '283 at 9:9–14 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:5–9 6. A method of transferring data from a transaction card to a card reader as said card is moved through said card reader by emulating a magnetic stripe disposed on a predetermined area on said card comprising the steps of: Burkhardt '283 at 10:12–18 applying said sequentially generated data to a magnetic field generator to sequentially generate magnetic fields representative of said data simultaneously across substantially the entire portion of said

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	predetermined area, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:25–28 A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 at 10:31–36 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:57–60 8. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 at 10:63–68 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a memory to hold transaction data; and	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Burkhardt '283 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figs. 7+8  FIG.7 FIG.8 Burkhardt '283 at Figure 9  FIG. 9 Burkhardt '283 at Figure 10  FIG.10

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at Figure 11  Burkhardt '283 at Figure 12  FIG.12 Burkhardt '283 at Fig. 13  FIG.13 Burkhardt '283 at 1:51–65 U.S. Pat. No. 4,354,099 issued to Rayment et al. discloses an identifier device which interacts with a reader to identify the device. The reader generates a current on drive coil A which interacts with detector coil B to induce a current in drive coil C. The magnetic field which is generated by drive coil C in the identifier is detected by detector coil D in the sensor. Detector coils and drive coils B and C in the

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	identifier are laid out in an array, such as illustrated in FIG. 5. Depending upon which of these coils are interconnected, a specific set of drive coils C are activated to specifically identify the identifier. The United Kingdom Patent Application No. GB2079017A discloses the same invention as disclosed in U.S. Pat. No. 4,354,099, which is the equivalent of the United Kingdom Patent Application. Burkhardt '283 at 1:66–2:10 U.S. Pat. No. 4,253,017 issued to Whitehead on Feb. 24, 1981 discloses a mganetically coded identification card which has a multiplicity of magnetic core spots 20 that can be alternatively recorded in opposite directions. A number of the magnetic core spots are permanently recorded while other spots can be changed to indicate variable information, such as the last port of entry, or egress, and the last use of the card. Data recorded on the magnetic spots may be erased and replaced with new data. Recording is accomplished by energizing coils on horseshoe magnets in the required manner to magnetize the spots to record the variable information. Burkhardt '283 at 2:21–27 Each of the Springer patents referenced above discloses circular magnetic generators for generating magnetic vectors having a spherical geometry which is well defined for the purpose of magnetic image storage with high resolution. The Springer patents disclose various plating techniques for forming the concentric magnetic structures. Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator. Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion

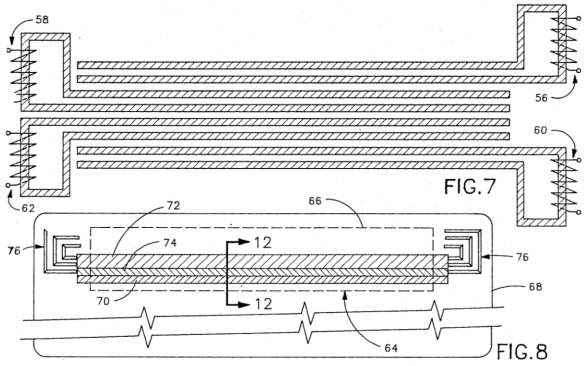
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe. Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:9–13 FIG. 13 is a schematic diagram of the device of the present invention for detecting the speed of movement of the card through the card reader and the quadrature driving circuit for applying electrical current to the magnetic field generators. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits. Burkhardt '283 at 6:15–22 FIG. 7 is a schematic plan view illustrating the manner in which four magnetic field generators 56, 58, 60, 62 may be disposed on the card to form four separate magnetic stripes which emulate four prerecorded stripes on a conventional transaction card. Each separate magnetic generator has a separate drive coil for sequentially generating magnetic data on each of the magnetic field generator. Burkhardt '283 at 6:23–31 FIG. 8 is a schematic plan view of the manner in which an alternative magnetic field generator 64 is disposed in the magnetic stripe area 66 of a standard credit card 68. The magnetic field generator 64, illustrated in FIG. 8, comprises a three dimensional structure having pole pieces 70, 72 which are separated by a diamagnetic material 74. Spiral coil 76 is wrapped around the magnetic stand portion which is coupled to magnetic pole portion 72, as disclosed above. Burkhardt '283 at 6:32–51 FIG. 9 is a schematic plan view illustrating the initial steps of forming the magnetic field generator structure 64 of the second embodiment of the present invention. A flexible nonconductive nonpermeable substrate 78 is provided which can form one of the plastic laminate layers of the transaction card of the present invention. A layer of highly permeable material is then applied to the substrate 78 and etched to form a magnetic bottom pole piece 80. Alternatively, the permeable metal can be applied by masking techniques to form the bottom pole piece 80 in the desired configuration. A filler layer 82 of nonconductive, nonpermeable material is then applied over the bottom pole piece 80 and plastic substrate 78 to form a substantially flat surface. A layer of copper or other conductive material is then applied over the filler layer 82 and etched to form a spiral coil 76 and back plane 84. Again, these layers can be applied by any desired process including the use of sputtering, masking techniques, lamination techniques, electro-less and electro-plating, etc. Burkhardt '283 at 6:52–66 FIG. 10 illustrates the next step in forming the magnetic field generator 64 of the second embodiment of the present invention. A second filler layer 86 is applied over the back plane 84, conductive coil 76 and first filler layer 82. The filler layer 84 is then etched to form wells 88, 90 which are aligned directly over the end portions of bottom pole piece 80. A highly permeable material is then placed in wells 88, 90 to form a magnetically conductive stand portions 92, 94, respectively. A magnetic material can comprise a

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	nickel iron material which is powdered and set in a binder which is chemically cured or heat set. Alternatively, any other desired means of filling wells 88, 90 can be used to form the magnetic stands 92, 94. The magnetic stand 92, 94 must necessarily have magnetic continuity with bottom pole piece 80. Burkhardt '283 at 6:67–7:13 FIG. 11 illustrates the next step in forming the magnetic field generator 64 of the second embodiment of the present invention. A permeable material is applied over the second filler layer 86 and etched to reveal top pole pieces 70, 72. The gap 96 between pole pieces 70, 72 is then etched down to the copper plane 84 through filler layer 86. The well formed by etching the gap portion 96 and filler layer 86 is thn filled with a conductive material 98 to form diamagnetic break 74 between pole pieces 70 and 72. Of necessity, the material forming the magnetic break 74 is in continuous electrical contact with the copper back plane 84. The electrical contact is low in resistance and without break or interruption. A final top protective layer is then applied over the entire structure. Burkhardt '283 at 7:14–29 FIG. 12 is a cross-sectional view of the device as illustrated in FIG. 8. FIG. 12 illustrates the flexible substrate 78, bottom pole piece 80 deposited on the upper surface of flexible substrate 78, filler layer 82 which is applied over the bottom pole piece 80 and flexible substrate 78, the conductive coil 76 and diamagnetic break plane 84 deposited on the upper surface of first filler layer 82, second filler layer 86, magnetic pole stands 92, 94 which are magnetically coupled to bottom pole piece 80, upper pole pieces 70, 72, diamagnetic break 74 and top protective layer 100. As is illustrated in FIG. 12, diamagnetic break 74 prevents the direct passage of magnetic field lines from pole piece 70 to pole piece 72. Magnetic field lines 102 couple pole pieces 70, 72 by protruding vertically from the card for easy coupling with a magnetic read head. Burkhardt '283 at 7:62–8:12 Both the difference voltage signal 120, which is proportional to position of the card in the card reader, and differentiated difference voltage signal 122, which is proportional to velocity of movement of the card, are applied to analog to digital converter 124. Analog to digital converter 124 includes an integral multiplexer. The digital signal output of the analog to digital converter 124 is applied to a parallel input/output unit 126. The analog to digital converter 124 applies the digital signal, indicative of position and velocity of the card, to a parallel input/output unit 126 which controls the application of power to various contacts A through R in the quadrature driver circuit 128. Microprocessor 130 receives the digitized information indicating the position and velocity of the card and determines a rate at which data is

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	to be produced to ensure that all the data is generated and applied to the magnetic field generators within the scanning time of the card across the read head of the card reader. Burkhardt '283 at 8:13–36 Quadrature driving circuit 128 is driven by the various contacts A through R which are enabled by the parallel input/output unit 126. Upon application of enable current from contacts A and K, a flux pattern in a first predetermined direction will be generated on coil 130 as a result of current flowing from the voltage source V_{cc} 131 to ground potential 133. Upon application of enable current to connectors B and J, a reverse current is applied through coil 130 to produce a magnetic field in an opposite direction since current flows from V_{cc} 135 to ground potential 136. Coils 130, 132, 134, and 136 are the same coils fabrication earlier as item 76 (FIG. 10) or items 28, 48 (FIG. 4). The other quadrature driving circuits operate in essentially the same manner. For example, if the A-K connection were to indicate a logic one and the B-J connection were to indicate a logic zero, the C-M, E-P, G-R connections would indicate logics ones while the L-D, N-F and Q-H connections would indicate logics zero. In this manner, the four coils 130, 132, 134 and 136 are capable of transmitting data by generating magnetic fields in opposite directions in response to the quadrature driving circuit and thereby simultaneously produce data on four separate magnetic field generators. Burkhardt '283 at 8:37–54 The present invention therefore provides magnetic field generators which are capable of emulating prerecorded magnetic data on a conventional prerecorded magnetic stripe of a transaction card without the necessity of precisely locating the card in a precise predetermined location. The present invention is capable of detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transferred from the microprocessor to the magnetic field generator within the scanning time of the card across the read head of the card reader. Diamagnetic material is used between pole pieces to generate magnetic field lines which extend vertically from the card to thereby increase the field strength adjacent the magnetic field generator outside of the card. Additionally, the card of the present invention can be used with the large number of conventional card readers presently in use with only minor modification. Burkhardt '283 at 9:2–6 1. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader as said card is moved through said card reader, comprising:

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 10:5–9 6. A method of transferring data from a transaction card to a card reader as said card is moved through said card reader by emulating a magnetic stripe disposed on a predetermined area on said card comprising the steps of: Burkhardt '283 at 10:12–18 applying said sequentially generated data to a magnetic field generator to sequentially generate magnetic fields representative of said data simultaneously across substantially the entire portion of said predetermined area, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:25–28 A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 at 10:31–36 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:57–60 8. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 at 10:63–68 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	*See* 1[pre] above.

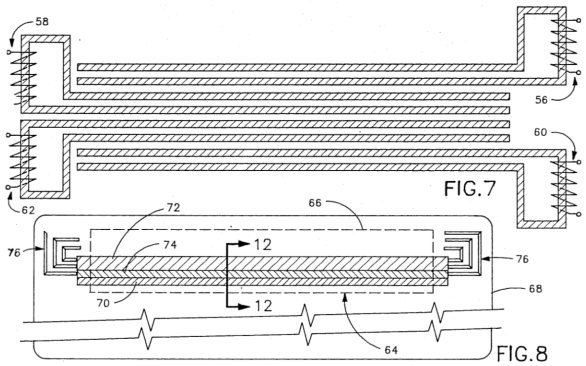
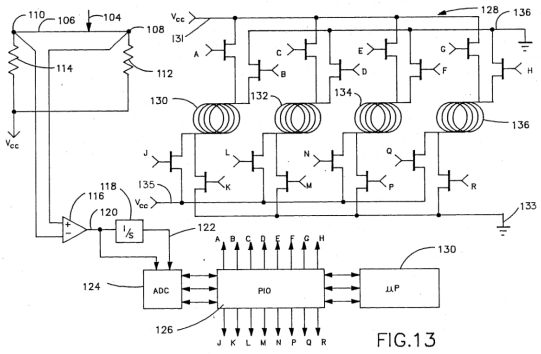
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Burkhardt '283 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figs. 7+8  FIG.7 FIG.8 Burkhardt '283 at 1:8–10 The present invention pertains generally to magnetic recording and more specifically to a device for emulating a prerecorded magnetic stripe on a transaction card.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 1:51–65 U.S. Pat. No. 4,354,099 issued to Rayment et al. discloses an identifier device which interacts with a reader to identify the device. The reader generates a current on drive coil A which interacts with detector coil B to induce a current in drive coil C. The magnetic field which is generated by drive coil C in the identifier is detected by detector coil D in the sensor. Detector coils and drive coils B and C in the identifier are laid out in an array, such as illustrated in FIG. 5. Depending upon which of these coils are interconnected, a specific set of drive coils C are activated to specifically identify the identifier. The United Kingdom Patent Application No. GB2079017A discloses the same invention as disclosed in U.S. Pat. No. 4,354,099, which is the equivalent of the United Kingdom Patent Application. Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator. Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe. Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits. Burkhardt '283 at 6:15–22 FIG. 7 is a schematic plan view illustrating the manner in which four magnetic field generators 56, 58, 60, 62 may be disposed on the card to form four separate magnetic stripes which emulate four prerecorded stripes on a conventional transaction card. Each separate magnetic generator has a separate drive coil for sequentially generating magnetic data on each of the magnetic field generator. Burkhardt '283 at 8:37–54 The present invention therefore provides magnetic field generators which are capable of emulating prerecorded magnetic data on a conventional prerecorded magnetic stripe of a transaction card without the necessity of precisely locating the card in a precise predetermined location. The present invention is capable of detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transferred from the microprocessor to the magnetic field generator within the scanning time of the card across the read head of the card reader. Diamagnetic material is used between pole pieces

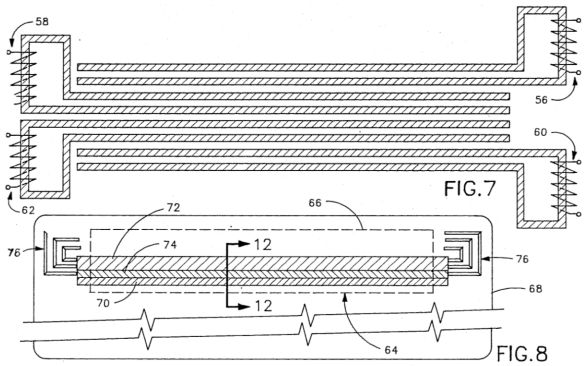
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	to generate magnetic field lines which extend vertically from the card to thereby increase the field strength adjacent the magnetic field generator outside of the card. Additionally, the card of the present invention can be used with the large number of conventional card readers presently in use with only minor modification. Burkhardt '283 at 9:2–6 1. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader as said card is moved through said card reader, comprising: Burkhardt '283 at 9:9–14 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:5–9 6. A method of transferring data from a transaction card to a card reader as said card is moved through said card reader by emulating a magnetic stripe disposed on a predetermined area on said card comprising the steps of: Burkhardt '283 at 10:12–18 applying said sequentially generated data to a magnetic field generator to sequentially generate magnetic fields representative of said data simultaneously across substantially the entire portion of said predetermined area, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:31–36 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:57–60 8. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising:

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Burkhardt '283 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figs. 7+8

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 FIG.7 FIG.8 Burkhardt '283 at Fig. 13  FIG.13 Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe. Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to

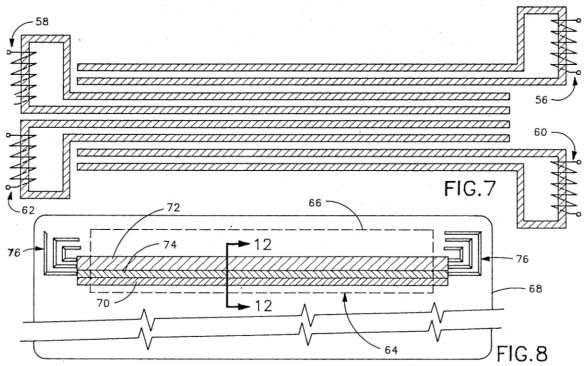
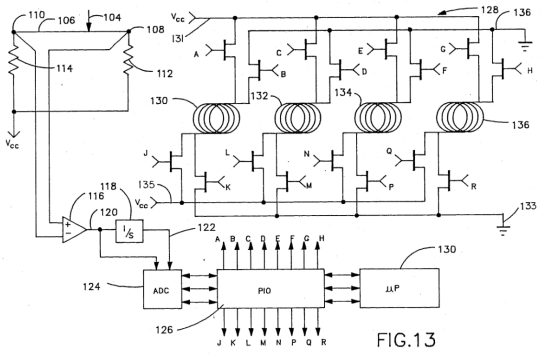
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits. Burkhardt '283 at 10:37–45 said magnetic field generator means further comprising nonconductive, permeable structure means disposed in substantially a single plane on said card, said nonconductive permeable structure means having pole portions which are separated by a gap which extends substantially along the entire length which said prerecorded magnetic stripe would otherwise extend, and a loop portion coupled to said pole portions; To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Burkhardt '283 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figs. 7+8

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 FIG.7 FIG.8 Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator. Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe. Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:9–13 FIG. 13 is a schematic diagram of the device of the present invention for detecting the speed of movement of the card through the card reader and the quadrature driving circuit for applying electrical current to the magnetic field generators. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits. Burkhardt '283 at 6:15–22 FIG. 7 is a schematic plan view illustrating the manner in which four magnetic field generators 56, 58, 60, 62 may be disposed on the card to form four separate magnetic stripes which emulate four prerecorded stripes on a conventional transaction card. Each separate magnetic generator has a separate drive coil for sequentially generating magnetic data on each of the magnetic field generator. Burkhardt '283 at 8:37–54

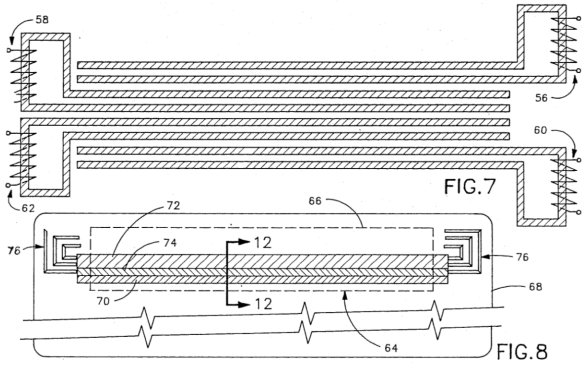
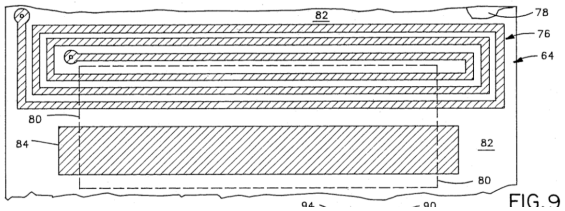
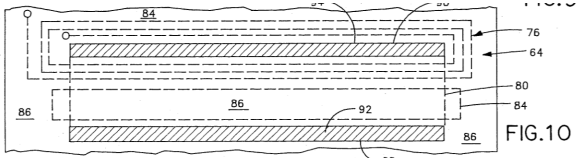
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	The present invention therefore provides magnetic field generators which are capable of emulating prerecorded magnetic data on a conventional prerecorded magnetic stripe of a transaction card without the necessity of precisely locating the card in a precise predetermined location. The present invention is capable of detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transferred from the microprocessor to the magnetic field generator within the scanning time of the card across the read head of the card reader. Diamagnetic material is used between pole pieces to generate magnetic field lines which extend vertically from the card to thereby increase the field strength adjacent the magnetic field generator outside of the card. Additionally, the card of the present invention can be used with the large number of conventional card readers presently in use with only minor modification. Burkhardt '283 at 9:2–6 1. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader as said card is moved through said card reader, comprising: Burkhardt '283 at 10:5–9 6. A method of transferring data from a transaction card to a card reader as said card is moved through said card reader by emulating a magnetic stripe disposed on a predetermined area on said card comprising the steps of: Burkhardt '283 at 10:12–18 applying said sequentially generated data to a magnetic field generator to sequentially generate magnetic fields representative of said data simultaneously across substantially the entire portion of said predetermined area, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:25–28 A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 at 10:57–60 8. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising:

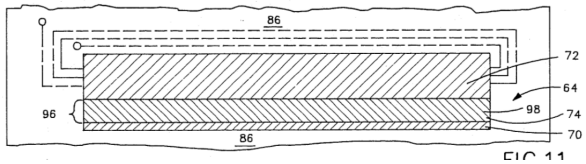
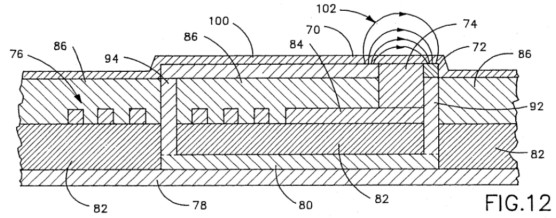
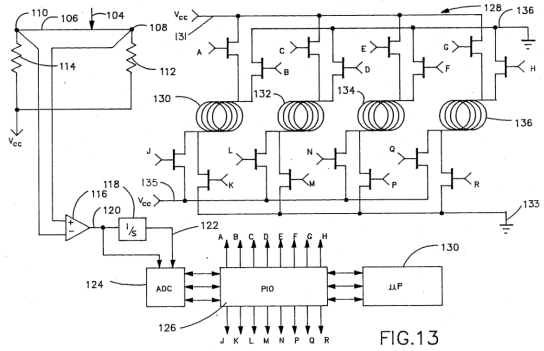
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Burkhardt '283 discloses or renders obvious "[a] mobile device." For example: *See* above at 1[pre]. To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Burkhardt '283 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a]. To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Burkhardt '283 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Burkhardt '283 at Abstract > A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figs. 7+8

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 FIG.7 FIG.8 Burkhardt '283 at Fig. 13  FIG.13 Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe. Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits. Burkhardt '283 at 8:37–54 The present invention therefore provides magnetic field generators which are capable of emulating prerecorded magnetic data on a conventional prerecorded magnetic stripe of a transaction card without the necessity of precisely locating the card in a precise predetermined location. The present invention is capable of detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transferred from the microprocessor to the magnetic field generator within the scanning time of the card across the read head of the card reader. Diamagnetic material is used between pole pieces to generate magnetic field lines which extend vertically from the card to thereby increase the field strength adjacent the magnetic field generator outside of the card. Additionally, the card of the present invention can be used with the large number of conventional card readers presently in use with only minor modification. Burkhardt '283 at 10:37–45 said magnetic field generator means further comprising nonconductive, permeable structure means disposed in substantially a single plane on said card, said nonconductive permeable structure means having pole portions which are separated by a gap which extends substantially along the entire length which said prerecorded magnetic stripe would otherwise extend, and a loop portion coupled to said pole portions; *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Burkhardt '283 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figs. 7+8  FIG.7 FIG.8 Burkhardt '283 at Figure 9  FIG.9 Burkhardt '283 at Figure 10  FIG.10 Burkhardt '283 at Figure 11

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 Burkhardt '283 at Figure 12  FIG.12 Burkhardt '283 at Fig. 13  FIG.13 Burkhardt '283 at 1:51–65 U.S. Pat. No. 4,354,099 issued to Rayment et al. discloses an identifier device which interacts with a reader to identify the device. The reader generates a current on drive coil A which interacts with detector coil B to induce a current in drive coil C. The magnetic field which is generated by drive coil C in the identifier is detected by detector coil D in the sensor. Detector coils and drive coils B and C in the identifier are laid out in an array, such as illustrated in FIG. 5. Depending upon which of these coils are interconnected, a specific set of drive coils C are activated to specifically identify the identifier. The

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	United Kingdom Patent Application No. GB2079017A discloses the same invention as disclosed in U.S. Pat. No. 4,354,099, which is the equivalent of the United Kingdom Patent Application. Burkhardt '283 at 1:66–2:10 U.S. Pat. No. 4,253,017 issued to Whitehead on Feb. 24, 1981 discloses a mganetically coded identification card which has a multiplicity of magnetic core spots 20 that can be alternatively recorded in opposite directions. A number of the magnetic core spots are permanently recorded while other spots can be changed to indicate variable information, such as the last port of entry, or egress, and the last use of the card. Data recorded on the magnetic spots may be erased and replaced with new data. Recording is accomplished by energizing coils on horseshoe magnets in the required manner to magnetize the spots to record the variable information. Burkhardt '283 at 2:21–27 Each of the Springer patents referenced above discloses circular magnetic generators for generating magnetic vectors having a spherical geometry which is well defined for the purpose of magnetic image storage with high resolution. The Springer patents disclose various plating techniques for forming the concentric magnetic structures. Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator. Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe.

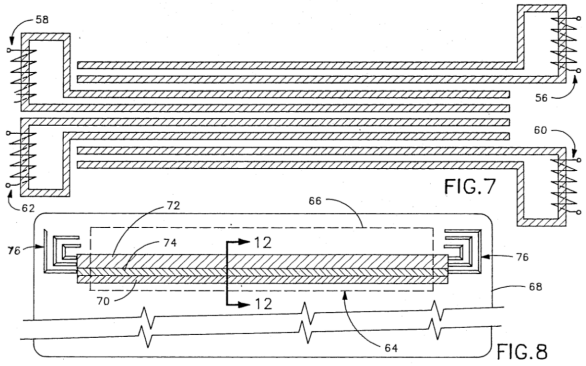
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:9–13 FIG. 13 is a schematic diagram of the device of the present invention for detecting the speed of movement of the card through the card reader and the quadrature driving circuit for applying electrical current to the magnetic field generators. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 6:15–22 FIG. 7 is a schematic plan view illustrating the manner in which four magnetic field generators 56, 58, 60, 62 may be disposed on the card to form four separate magnetic stripes which emulate four prerecorded stripes on a conventional transaction card. Each separate magnetic generator has a separate drive coil for sequentially generating magnetic data on each of the magnetic field generator. Burkhardt '283 at 6:23–31 FIG. 8 is a schematic plan view of the manner in which an alternative magnetic field generator 64 is disposed in the magnetic stripe area 66 of a standard credit card 68. The magnetic field generator 64, illustrated in FIG. 8, comprises a three dimensional structure having pole pieces 70, 72 which are separated by a diamagnetic material 74. Spiral coil 76 is wrapped around the magnetic stand portion which is coupled to magnetic pole portion 72, as disclosed above. Burkhardt '283 at 6:32–51 FIG. 9 is a schematic plan view illustrating the initial steps of forming the magnetic field generator structure 64 of the second embodiment of the present invention. A flexible nonconductive nonpermeable substrate 78 is provided which can form one of the plastic laminate layers of the transaction card of the present invention. A layer of highly permeable material is then applied to the substrate 78 and etched to form a magnetic bottom pole piece 80. Alternatively, the permeable metal can be applied by masking techniques to form the bottom pole piece 80 in the desired configuration. A filler layer 82 of nonconductive, nonpermeable material is then applied over the bottom pole piece 80 and plastic substrate 78 to form a substantially flat surface. A layer of copper or other conductive material is then applied over the filler layer 82 and etched to form a spiral coil 76 and back plane 84. Again, these layers can be applied by any desired process including the use of sputtering, masking techniques, lamination techniques, electro-less and electro-plating, etc. Burkhardt '283 at 6:52–66 FIG. 10 illustrates the next step in forming the magnetic field generator 64 of the second embodiment of the present invention. A second filler layer 86 is applied over the back plane 84, conductive coil 76 and first filler layer 82. The filler layer 84 is then etched to form wells 88, 90 which are aligned directly over the end portions of bottom pole piece 80. A highly permeable material is then placed in wells 88, 90 to form a magnetically conductive stand portions 92, 94, respectively. A magnetic material can comprise a nickel iron material which is powdered and set in a binder which is chemically cured or heat set.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Alternatively, any other desired means of filling wells 88, 90 can be used to form the magnetic stands 92, 94. The magnetic stand 92, 94 must necessarily have magnetic continuity with bottom pole piece 80. Burkhardt '283 at 6:67–7:13 FIG. 11 illustrates the next step in forming the magnetic field generator 64 of the second embodiment of the present invention. A permeable material is applied over the second filler layer 86 and etched to reveal top pole pieces 70, 72. The gap 96 between pole pieces 70, 72 is then etched down to the copper plane 84 through filler layer 86. The well formed by etching the gap portion 96 and filler layer 86 is thn filled with a conductive material 98 to form diamagnetic break 74 between pole pieces 70 and 72. Of necessity, the material forming the magnetic break 74 is in continuous electrical contact with the copper back plane 84. The electrical contact is low in resistance and without break or interruption. A final top protective layer is then applied over the entire structure. Burkhardt '283 at 7:14–29 FIG. 12 is a cross-sectional view of the device as illustrated in FIG. 8. FIG. 12 illustrates the flexible substrate 78, bottom pole piece 80 deposited on the upper surface of flexible substrate 78, filler layer 82 which is applied over the bottom pole piece 80 and flexible substrate 78, the conductive coil 76 and diamagnetic break plane 84 deposited on the upper surface of first filler layer 82, second filler layer 86, magnetic pole stands 92, 94 which are magnetically coupled to bottom pole piece 80, upper pole pieces 70, 72, diamagnetic break 74 and top protective layer 100. As is illustrated in FIG. 12, diamagnetic break 74 prevents the direct passage of magnetic field lines from pole piece 70 to pole piece 72. Magnetic field lines 102 couple pole pieces 70, 72 by protruding vertically from the card for easy coupling with a magnetic read head. Burkhardt '283 at 7:62–8:12 Both the difference voltage signal 120, which is proportional to position of the card in the card reader, and differentiated difference voltage signal 122, which is proportional to velocity of movement of the card, are applied to analog to digital converter 124. Analog to digital converter 124 includes an integral multiplexer. The digital signal output of the analog to digital converter 124 is applied to a parallel input/output unit 126. The analog to digital converter 124 applies the digital signal, indicative of position and velocity of the card, to a parallel input/output unit 126 which controls the application of power to various contacts A through R in the quadrature driver circuit 128. Microprocessor 130 receives the digitized information indicating the position and velocity of the card and determines a rate at which data is to be produced to ensure that all the data is generated and applied to the magnetic field generators within the scanning time of the card across the read head of the card reader.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 8:13–36 Quadrature driving circuit 128 is driven by the various contacts A through R which are enabled by the parallel input/output unit 126. Upon application of enable current from contacts A and K, a flux pattern in a first predetermined direction will be generated on coil 130 as a result of current flowing from the voltage source V_{cc} 131 to ground potential 133. Upon application of enable current to connectors B and J, a reverse current is applied through coil 130 to produce a magnetic field in an opposite direction since current flows from V_{cc} 135 to ground potential 136. Coils 130, 132, 134, and 136 are the same coils fabrication earlier as item 76 (FIG. 10) or items 28, 48 (FIG. 4). The other quadrature driving circuits operate in essentially the same manner. For example, if the A-K connection were to indicate a logic one and the B-J connection were to indicate a logic zero, the C-M, E-P, G-R connections would indicate logics ones while the L-D, N-F and Q-H connections would indicate logics zero. In this manner, the four coils 130, 132, 134 and 136 are capable of transmitting data by generating magnetic fields in opposite directions in response to the quadrature driving circuit and thereby simultaneously produce data on four separate magnetic field generators. Burkhardt '283 at 8:37–54 The present invention therefore provides magnetic field generators which are capable of emulating prerecorded magnetic data on a conventional prerecorded magnetic stripe of a transaction card without the necessity of precisely locating the card in a precise predetermined location. The present invention is capable of detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transferred from the microprocessor to the magnetic field generator within the scanning time of the card across the read head of the card reader. Diamagnetic material is used between pole pieces to generate magnetic field lines which extend vertically from the card to thereby increase the field strength adjacent the magnetic field generator outside of the card. Additionally, the card of the present invention can be used with the large number of conventional card readers presently in use with only minor modification. Burkhardt '283 at 9:2–6 1. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader as said card is moved through said card reader, comprising: Burkhardt '283 at 10:5–9

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	6. A method of transferring data from a transaction card to a card reader as said card is moved through said card reader by emulating a magnetic stripe disposed on a predetermined area on said card comprising the steps of: Burkhardt '283 at 10:12–18 applying said sequentially generated data to a magnetic field generator to sequentially generate magnetic fields representative of said data simultaneously across substantially the entire portion of said predetermined area, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:25–28 A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 at 10:31–36 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; Burkhardt '283 at 10:57–60 8. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 at 10:63–68 magnetic field generator means for sequentially generating magnetic fields across substantially the entire portion of said predetermined area in response to said data, said magnetic fields having a field strength substantially equivalent to prerecorded data on said magnetic stripe; *See also* 1[c] and claim 5 above. To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	*See* 1[pre] above.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Burkhardt '283 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Burkhardt '283 at Abstract A device and method for transferring data from a microprocessor located in a transaction card through a card reader by emulating a prerecorded magnetic stripe on a conventional transaction car such as a credit or debit card. Data is sequentially produced by the microprocessor within the card and applied to a magnetic field generator which produces magnetic fields that emulate prerecorded data on a conventional magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transmitted from the microprocessor to the magnetic field generators within the scanning time of the card across read head of the card reader. Burkhardt '283 at Figs. 7+8  FIG.7 FIG.8 Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the prior art by providing a magnetic field generator which is elongated to produce a magnetic field across substantially the entire length of a conventional prerecorded magnetic stripe. The microprocessor of the present invention

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device for detecting the speed at which the card is moving through the card reader to control the rate at which data is transmitted to the magnetic field generator. Burkhardt '283 at 3:19–29 The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising sequentially generating data to be read by the card reader; a magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded data on the magnetic stripe. Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded magnetic stripe in both field strength and the rate at which data is read from the card. The card need not be precisely located within the card reader to provide a proper connection for transferring data. Rather, the present invention can be located anywhere within the card reader and need not even be moved to transmit data at the proper rate. Additionally, the present invention is simple and easy to manufacture and does not require a complex array of magnetic field generators or complex multiplexing techniques. Rather, the data is sequentially fed to the elongated magnetic field generator which sequentially generates data bits across the entire length of the magnetic stripe to allow detection at any location of the read head of the card reader on the magnetic stripe independently of the speed of movement of the card through the card reader. Burkhardt '283 at 3:64–66 FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:17–35 FIG. 1 is a schematic view of the back side of a credit card 10 illustrating a magnetic stripe area 12 which normally contains four separate magnetic stripes containing prerecorded information, such as account number and other identifying information pertaining to the transaction card 10. The present invention uses magnetic field generators which extend along substantially the entire length of the magnetic stripe 12 so

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration date 18. During the process of lamination of the various layers of the credit card 10 of the present invention, edge connectors 20, 22 are provided along the edge of the credit card 10 to provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits. Burkhardt '283 at 8:37–54 The present invention therefore provides magnetic field generators which are capable of emulating prerecorded magnetic data on a conventional prerecorded magnetic stripe of a transaction card without the necessity of precisely locating the card in a precise predetermined location. The present invention is capable of detecting the position and speed of movement of the card through the card reader to ensure that all of the data is transferred from the microprocessor to the magnetic field generator within the scanning time of the card across the read head of the card reader. Diamagnetic material is used between pole pieces to generate magnetic field lines which extend vertically from the card to thereby increase the field strength adjacent the magnetic field generator outside of the card. Additionally, the card of the present invention can be used with the large number of conventional card readers presently in use with only minor modification. *See also* claim 8 above. To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Burkhardt '283 discloses or renders obvious "[t]he mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: *See* above at claim 2.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

Patent Owner's Ex. 2020
Page 146

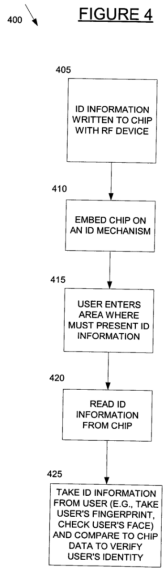
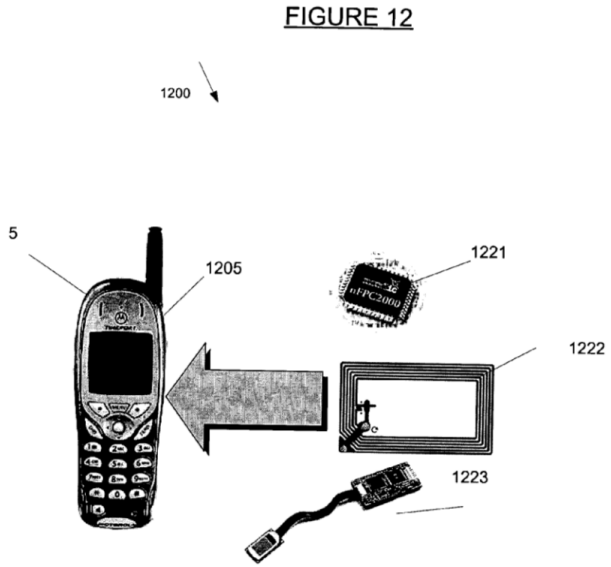
DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,202,156

EXHIBIT E3: US20040066273A1 ("Cortina '273")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Cortina '273 and (b) under 35 U.S.C. § 103(a) as obvious over Cortina '273 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to US20040066273A1 ("Cortina '273")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Cortina '273 discloses or renders obvious "[a] mobile device." For example: Cortina '273 at Fig. 4

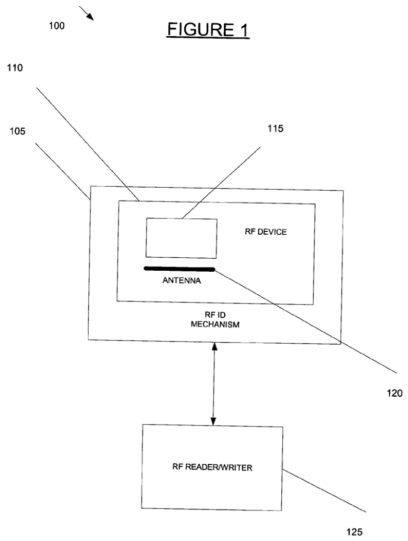
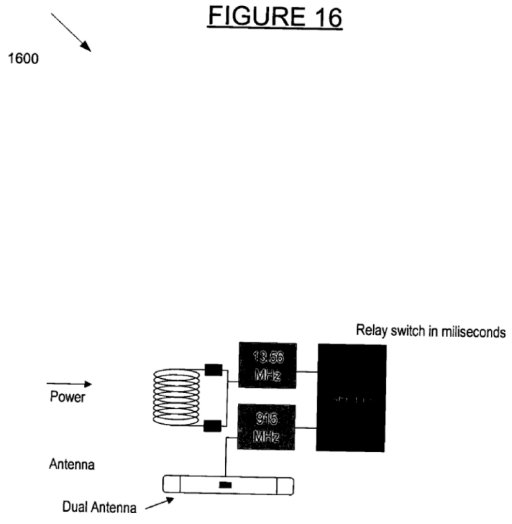
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	 Cortina '273 at Figure 12 

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at [0006] An RF Communications Device (e.g., Cellular Telephone) and Method of Use. Cortina ’273 at [0026] Numerous features of RF identification mechanism are utilized in one embodiment of the present invention. In this embodiment, the RF device is embedded in the RF identification mechanism. One example of an RF identification mechanism is a card, and the description below refers to the identification mechanism as a card in several examples. However, those experienced in the art will recognize that multiple other embodiments of the identification mechanism are possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA). Cortina ’273 at [0096] FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina ’273 at [0097] In 405, the identification information (e.g., fingerprint, picture) is written to a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415, a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity. Cortina ’273 at [0130] One embodiment of the RF communication device creates a communication through a network to a point of sale (“POS”). This is performed, for example, by a wireless RF device that stores a person's identification information, and can thus become a person's identification “document.” This is discussed in the context of an RF cellular telephone, but those experienced in the art will recognize that any communication device, including but not limited to a personal digital assistant or a pager, can be used. Cortina ’273 at [0131] As a user with an RF cellular telephone approaches a POS with an RF reader/writer, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone. The user is then asked to enter authentication information (e.g., a fingerprint). If the user wishes to complete a

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	transaction, the user enters the authentication information. An exchange of information via the RF reader/writer and the RF cellular telephone results in verification that the authentication information matches the RF cellular telephone information. Cortina '273 at [0132] The present invention, referred to in one embodiment as a RF cellular telephone, creates a communication through a network of cells to a point of sale (POS). This is performed by combining Global System for Mobile Communication (GSM) technology with a wireless RF device that can store a person's identification information, including an electronic or biometric "signature" (e.g., fingerprint, facial, iris, or other recognition feature). GSM technology includes a compact chip located on the back of the telephone. The compact chip has an operating system. The GSM telephones identify the telephones to a network carrier to avoid, for example, telephone cloning. Cortina '273 at [0133] The RF cellular telephone can thus become a person's identification document (e.g., passport, boarding pass) and/or credit card or other card (e.g., mileage cards). Multiple types of information can be carried and stored on the RF cellular telephone. The following uses are examples of how the RF cellular telephone can be used: an RF cellular telephone can be used as a substitute for credit cards, transforming the cellular telephone into the media of commercial transactions and transform telephony into the identification media for commercial establishments or authorities; an RF cellular telephone can be a personal identification or a Portable Data File (PDF); an RF cellular telephone can be integrated with a Global Positioning System (GPS) receiver; an RF cellular telephone can be integrated with hand held devices to provide Internet access, and access to business and personal information (e.g., email); and an RF cellular telephone could be a boarding pass (e.g., e-ticket) and/or could track a user going through security with authentication by fingerprint at a gate or other local area. Those experienced in the art will recognize that there are multiple other examples and uses of the RF cellular telephone. Cortina '273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210. Cortina '273 at [0139] The RF cellular telephone 1205 can include the following: a fingerprint identifier 1221 (e.g., an Application Specific Integrated Circuit (ASIC) chip, which is a chip that is designed specifically to run

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	fingerprint matching software on an operating system); and an RF device 1222 (with an antenna in the chip) to store identification information. In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223. As mentioned earlier, this could either be included on the RF cellular telephone, or on a fingerprint digital scanning device at the point of contact. Cortina '273 at [0202] FIG. 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a "one-to-many" hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card. Cortina '273 at claim 3 a radio frequency device comprising a radio frequency antenna embedded on a chip; an item incorporating the radio frequency device; and a radio frequency reader to read information from the radio frequency device. Cortina '273 at claim 4 4. A method of verifying registration information of an item, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto the item; Cortina '273 at claim 9 9. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; an identification mechanism incorporating the radio frequency device; and Cortina '273 at claim 10

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	10. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto an identification mechanism; Cortina '273 at claim 15 15. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; a communication device incorporating the radio frequency device; and Cortina '273 at claim 16 16. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto a communications device; Cortina '273 at claim 19 19. The system of claim 15 wherein the communications device comprises: a cellular phone; a personal digital assistant; a pager; a personal communications device To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Cortina '273 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Cortina '273 at Abstract The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader. Cortina '273 at Fig. 1

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	 Cortina '273 at Figure 16 

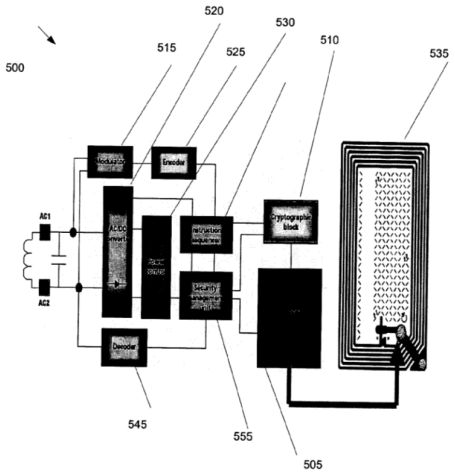
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0003] The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader/writer. The system and method can be used in numerous embodiments, including, but not limited to: Cortina '273 at [0012] FIGS. 1, 2 and 4 illustrate the general invention, according to one embodiment of the present invention. Cortina '273 at [0015] IGS. 12-14 illustrate the RF communications device and method of use, in an embodiment of the present invention. Cortina '273 at [0020] FIG. 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120. Cortina '273 at [0022] FIG. 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF device allows electronic identification via the reading of data stored in the chip in a contactless mode. Cortina '273 at [0096] FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina '273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210.

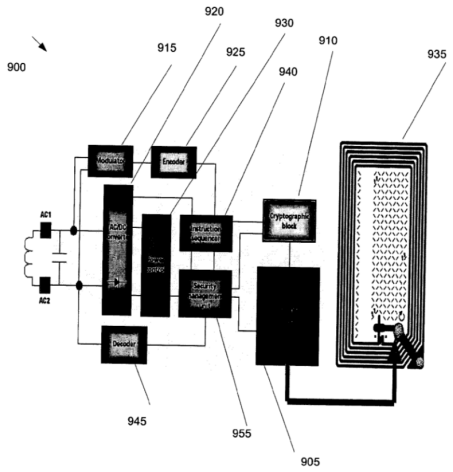
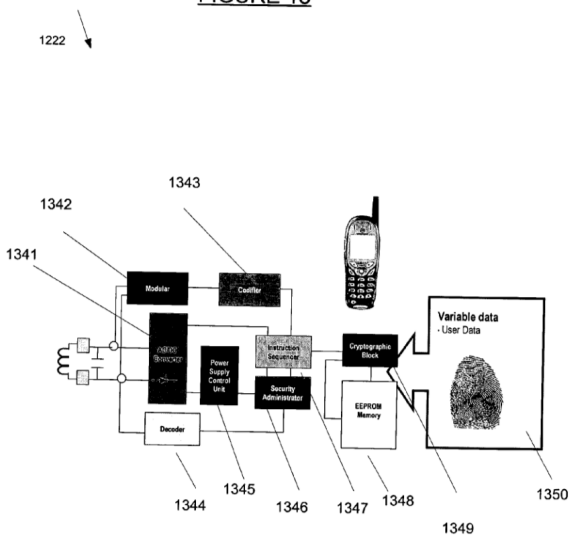
Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at [0140] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in FIG. 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements aren't met, a user cannot access the memory of the chip. The chip includes an AC-DC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from a antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 1347 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device. Cortina ’273 at [0143] FIG. 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone.

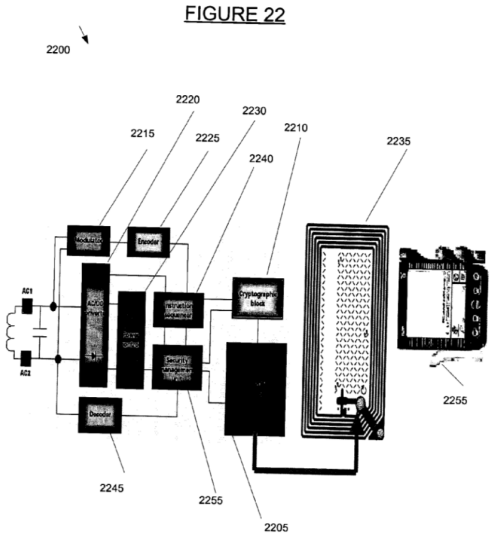
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0144] According to FIG. 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF reader/writer connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information). Cortina '273 at [0165] RF Identification Mechanism, RF Device, and RF reader/writer. One embodiment of the present invention comprises: an RF identification mechanism (e.g., an RF laser card), RF decals containing an Chip (e.g., a 2K bit chip or data memory circuit) with contactless read/write capabilities and an integrated RF antenna (e.g., a 13.56 MHz RF antenna); and an RF reader/writer. Cortina '273 at [0166] Multiple Chip Background Information. Often multiple frequencies are used. This takes advantage of the best electromagnetic and electrostatic characteristics of certain frequencies, one for long range reading and the second for field penetration (e.g., rain). Multiple frequence can be created using a dual modulator that can switch in milliseconds from one frequency to another. (See FIG. 16.) Cortina '273 at [0178] In 1825, at the point of entry or other appropriate place, RF antennas automatically read the RF decals as the vehicle approaches the custom's station and displays the data. A display screen on a computer (e.g., PC, PDA) in the customs area displays a reading of each RF decal as they pass within X number of feet of the antennas. The computer validates each RF decal by providing identification information (e.g., driver's photo, fingerprint, other data input at point of origin.) In 1830, the driver presents his RF laser card to a custom's officials at the point of entry (or other appropriate place) for validation and shipment verification. In 1835, the customs agent clears the shipping components for entry/exit and inputs this approval information to the RF card and RF decal. If the vehicle requires additional customs inspections, the customs agent will assign the next inspection station information to the driver's RF card and RF decals. Cortina '273 at [0199] The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz. The chip contains unique identifying data for persons or items subject to scrutiny, and can be read by nearby security or other control personnel with handheld or

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	stationary RF reader/writer or RF reader/writer devices for real time validation. Furthermore, the RF device is manufactured with light diffraction and other high security print features that eliminate document forgery and enable instant visual verification of authenticity. The RF device also includes an integrated AFIS digital fingerprint capability. The present invention can also use other unique identifying characteristics associated with additional elements of the air transport industry, including cargo, flight services, maintenance, and aircraft parts. Cortina '273 at [0202] FIG. 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a "one-to-many" hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card. Cortina '273 at claim 1 a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina '273 at claim 3 a radio frequency device comprising a radio frequency antenna embedded on a chip; an item incorporating the radio frequency device; and a radio frequency reader to read information from the radio frequency device. Cortina '273 at claim 4 4. A method of verifying registration information of an item, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto the item; Cortina '273 at claim 9

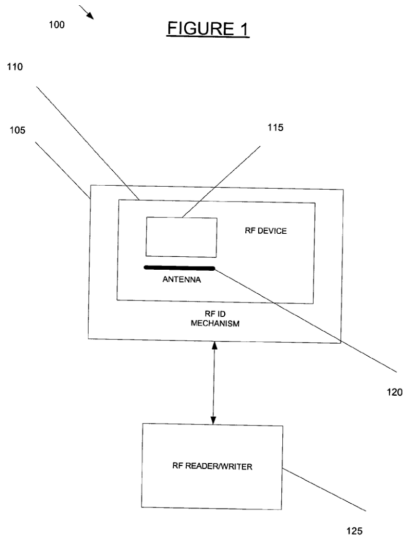
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	9. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; an identification mechanism incorporating the radio frequency device; and Cortina '273 at claim 10 10. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto an identification mechanism; Cortina '273 at claim 15 15. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; a communication device incorporating the radio frequency device; and Cortina '273 at claim 16 16. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto a communications device; Cortina '273 at claim 20 20. A system of verifying border crossing control information, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina '273 at claim 21 21. A method of verifying border crossing control information, comprising: storing identification information on a chip with a radio frequency antenna; Cortina '273 at claim 42 a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in radio frequency identification type integrated circuit and a communication antenna connected to the radio frequency identification type; and To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

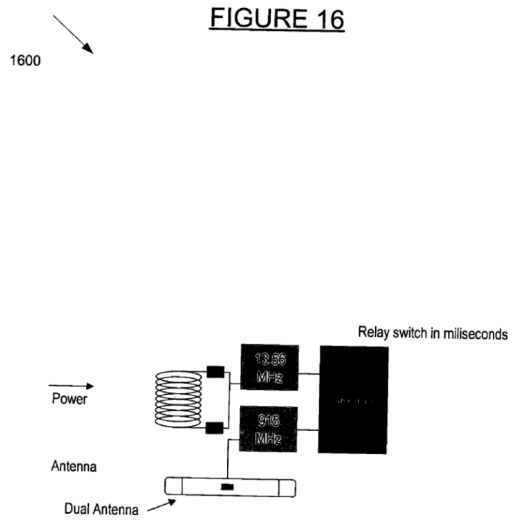
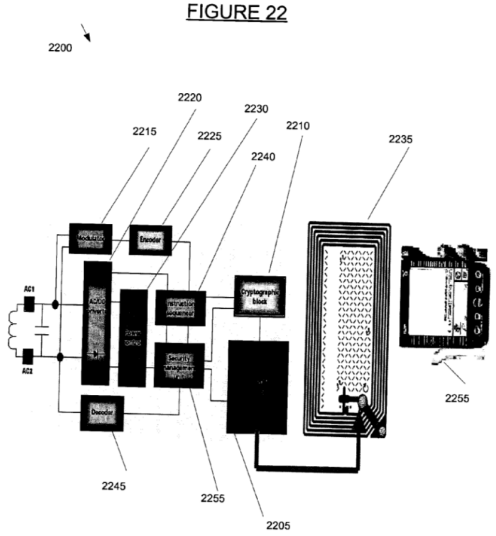
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
[1b] a memory to hold transaction data; and	Cortina '273 discloses or renders obvious "a memory to hold transaction data." For example: Cortina '273 at Figure 5 FIGURE 5  Cortina '273 at Figure 9

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIGURE 9  Cortina '273 at Figure 13 FIGURE 13 

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at Fig. 22  Cortina ’273 at [0102] FIG. 5 illustrates an RF registered item 500, according to one embodiment of the present invention. The registered item 500 includes the following components: A modulator 515 is a device that receives baseband signals from a antenna. An AC/DC converter 520 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 525 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 545 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 550 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 530 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 555 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 510 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 505 stores data. Information can be read and written from or to this device. Cortina ’273 at [0123]

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIG. 9 illustrates an RF registered item 900, according to one embodiment of the present invention. The registered item 900 includes the following components, as described earlier: a modulator 915, an AC/DC converter 920, an encoder 925, a power control 930, an instruction sequencer 940, a cryptographic block 910, a decoder 945, a security management unit 955, a memory 905, and an antenna 935. Cortina '273 at [0140] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in FIG. 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements aren't met, a user cannot access the memory of the chip. The chip includes an AC-DC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from a antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 1347 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Cortina '273 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Cortina '273 at Abstract The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader.

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at Fig. 1  Cortina ’273 at Figure 16

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIGURE 16  Cortina '273 at Fig. 22 FIGURE 22 

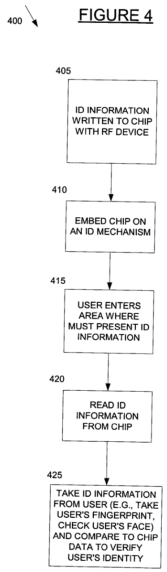
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0003] The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader/writer. The system and method can be used in numerous embodiments, including, but not limited to: Cortina '273 at [0012] FIGS. 1, 2 and 4 illustrate the general invention, according to one embodiment of the present invention. Cortina '273 at [0015] IGS. 12-14 illustrate the RF communications device and method of use, in an embodiment of the present invention. Cortina '273 at [0020] FIG. 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120. Cortina '273 at [0022] FIG. 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF device allows electronic identification via the reading of data stored in the chip in a contactless mode. Cortina '273 at [0096] FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina '273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210.

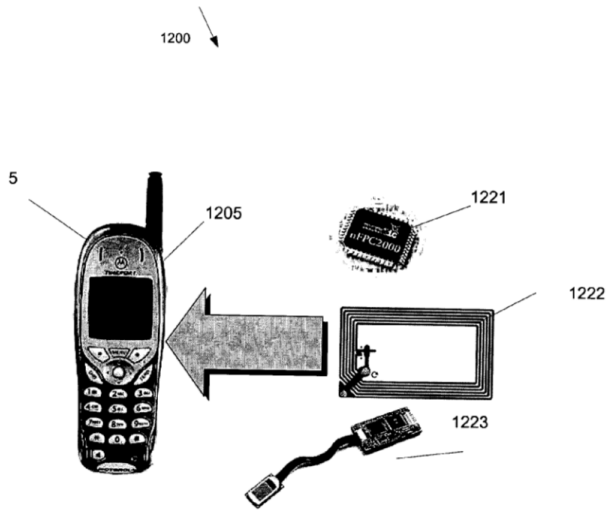
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0140] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in FIG. 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements aren't met, a user cannot access the memory of the chip. The chip includes an AC-DC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from a antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 1347 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device. Cortina '273 at [0141] In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel milage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security. Cortina '273 at [0143] FIG. 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone. Cortina '273 at [0144] According to FIG. 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF reader/writer connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information). Cortina '273 at [0165] RF Identification Mechanism, RF Device, and RF reader/writer. One embodiment of the present invention comprises: an RF identification mechanism (e.g., an RF laser card), RF decals containing an Chip (e.g., a 2K bit chip or data memory circuit) with contactless read/write capabilities and an integrated RF antenna (e.g., a 13.56 MHz RF antenna); and an RF reader/writer. Cortina '273 at [0166] Multiple Chip Background Information. Often multiple frequencies are used. This takes advantage of the best electromagnetic and electrostatic characteristics of certain frequencies, one for long range reading and the second for field penetration (e.g., rain). Multiple frequence can be created using a dual modulator that can switch in milliseconds from one frequency to another. (See FIG. 16.) Cortina '273 at [0178] In 1825, at the point of entry or other appropriate place, RF antennas automatically read the RF decals as the vehicle approaches the custom's station and displays the data. A display screen on a computer (e.g., PC, PDA) in the customs area displays a reading of each RF decal as they pass within X number of feet of the antennas. The computer validates each RF decal by providing identification information (e.g., driver's photo, fingerprint, other data input at point of origin.) In 1830, the driver presents his RF laser card to a custom's officials at the point of entry (or other appropriate place) for validation and shipment verification. In 1835, the customs agent clears the shipping components for entry/exit and inputs this approval information to the RF card and RF decal. If the vehicle requires additional customs inspections,

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	the customs agent will assign the next inspection station information to the driver's RF card and RF decals. Cortina ’273 at [0199] The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz. The chip contains unique identifying data for persons or items subject to scrutiny, and can be read by nearby security or other control personnel with handheld or stationary RF reader/writer or RF reader/writer devices for real time validation. Furthermore, the RF device is manufactured with light diffraction and other high security print features that eliminate document forgery and enable instant visual verification of authenticity. The RF device also includes an integrated AFIS digital fingerprint capability. The present invention can also use other unique identifying characteristics associated with additional elements of the air transport industry, including cargo, flight services, maintenance, and aircraft parts. Cortina ’273 at [0202] FIG. 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a “one-to-many” hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card. Cortina ’273 at claim 1 a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina ’273 at claim 3 a radio frequency device comprising a radio frequency antenna embedded on a chip; an item incorporating the radio frequency device; and a radio frequency reader to read information from the radio frequency device.

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at claim 4 4. A method of verifying registration information of an item, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto the item; Cortina '273 at claim 9 9. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; an identification mechanism incorporating the radio frequency device; and Cortina '273 at claim 10 10. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto an identification mechanism; Cortina '273 at claim 15 15. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; a communication device incorporating the radio frequency device; and Cortina '273 at claim 16 16. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto a communications device; Cortina '273 at claim 20 20. A system of verifying border crossing control information, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina '273 at claim 21 21. A method of verifying border crossing control information, comprising: storing identification information on a chip with a radio frequency antenna; Cortina '273 at claim 42

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in radio frequency identification type integrated circuit and a communication antenna connected to the radio frequency identification type; and To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	Cortina '273 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: Cortina '273 at Fig. 4  Cortina '273 at Figure 12

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIGURE 12  Cortina '273 at [0006] An RF Communications Device (e.g., Cellular Telephone) and Method of Use. Cortina '273 at [0026] Numerous features of RF identification mechanism are utilized in one embodiment of the present invention. In this embodiment, the RF device is embedded in the RF identification mechanism. One example of an RF identification mechanism is a card, and the description below refers to the identification mechanism as a card in several examples. However, those experienced in the art will recognize that multiple other embodiments of the identification mechanism are possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA). Cortina '273 at [0096] FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina '273 at [0097] In 405, the identification information (e.g., fingerprint, picture) is written to a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415,

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity. Cortina ’273 at [0130] One embodiment of the RF communication device creates a communication through a network to a point of sale (“POS”). This is performed, for example, by a wireless RF device that stores a person's identification information, and can thus become a person's identification “document.” This is discussed in the context of an RF cellular telephone, but those experienced in the art will recognize that any communication device, including but not limited to a personal digital assistant or a pager, can be used. Cortina ’273 at [0131] As a user with an RF cellular telephone approaches a POS with an RF reader/writer, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone. The user is then asked to enter authentication information (e.g., a fingerprint). If the user wishes to complete a transaction, the user enters the authentication information. An exchange of information via the RF reader/writer and the RF cellular telephone results in verification that the authentication information matches the RF cellular telephone information. Cortina ’273 at [0132] The present invention, referred to in one embodiment as a RF cellular telephone, creates a communication through a network of cells to a point of sale (POS). This is performed by combining Global System for Mobile Communication (GSM) technology with a wireless RF device that can store a person's identification information, including an electronic or biometric “signature” (e.g., fingerprint, facial, iris, or other recognition feature). GSM technology includes a compact chip located on the back of the telephone. The compact chip has an operating system. The GSM telephones identify the telephones to a network carrier to avoid, for example, telephone cloning. Cortina ’273 at [0133] The RF cellular telephone can thus become a person's identification document (e.g., passport, boarding pass) and/or credit card or other card (e.g., mileage cards). Multiple types of information can be carried and stored on the RF cellular telephone. The following uses are examples of how the RF cellular telephone can be used: an RF cellular telephone can be used as a substitute for credit cards, transforming the cellular telephone into the media of commercial transactions and transform telephony into the

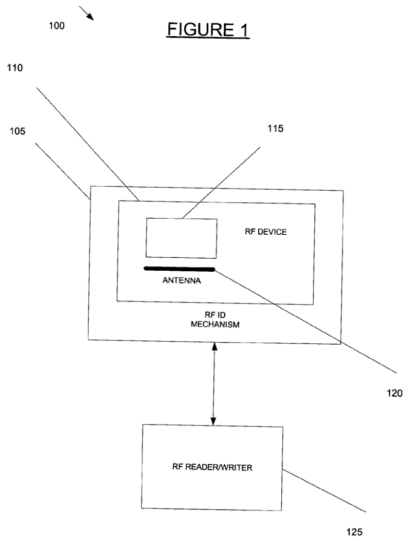
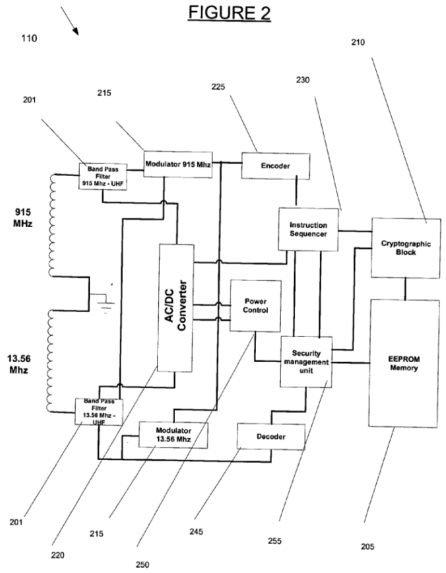
Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	identification media for commercial establishments or authorities; an RF cellular telephone can be a personal identification or a Portable Data File (PDF); an RF cellular telephone can be integrated with a Global Positioning System (GPS) receiver; an RF cellular telephone can be integrated with hand held devices to provide Internet access, and access to business and personal information (e.g., email); and an RF cellular telephone could be a boarding pass (e.g., e-ticket) and/or could track a user going through security with authentication by fingerprint at a gate or other local area. Those experienced in the art will recognize that there are multiple other examples and uses of the RF cellular telephone. Cortina ’273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210. Cortina ’273 at [0139] The RF cellular telephone 1205 can include the following: a fingerprint identifier 1221 (e.g., an Application Specific Integrated Circuit (ASIC) chip, which is a chip that is designed specifically to run fingerprint matching software on an operating system); and an RF device 1222 (with an antenna in the chip) to store identification information. In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223. As mentioned earlier, this could either be included on the RF cellular telephone, or on a fingerprint digital scanning device at the point of contact. Cortina ’273 at [0202] FIG. 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a “one-to-many” hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card.

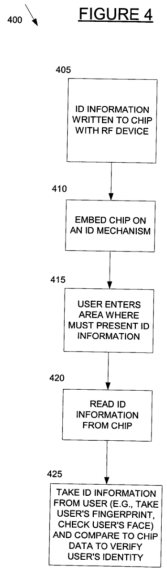
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at claim 3 a radio frequency device comprising a radio frequency antenna embedded on a chip; an item incorporating the radio frequency device; and a radio frequency reader to read information from the radio frequency device. Cortina '273 at claim 4 4. A method of verifying registration information of an item, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto the item; Cortina '273 at claim 9 9. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; an identification mechanism incorporating the radio frequency device; and Cortina '273 at claim 10 10. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto an identification mechanism; Cortina '273 at claim 15 15. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; a communication device incorporating the radio frequency device; and Cortina '273 at claim 16 16. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto a communications device; Cortina '273 at claim 19 19. The system of claim 15 wherein the communications device comprises: a cellular phone; a personal digital assistant;

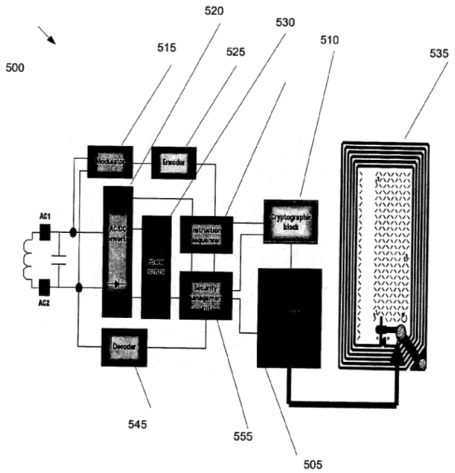
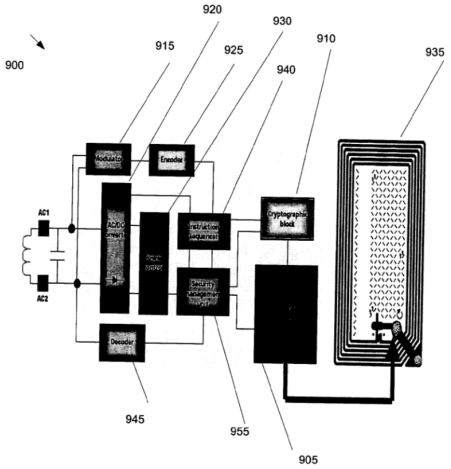
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	a pager; a personal communications device *See also* 1[pre] above. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Cortina '273 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Cortina '273 at [0141] In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel milage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security. Cortina '273 at [0143] FIG. 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will

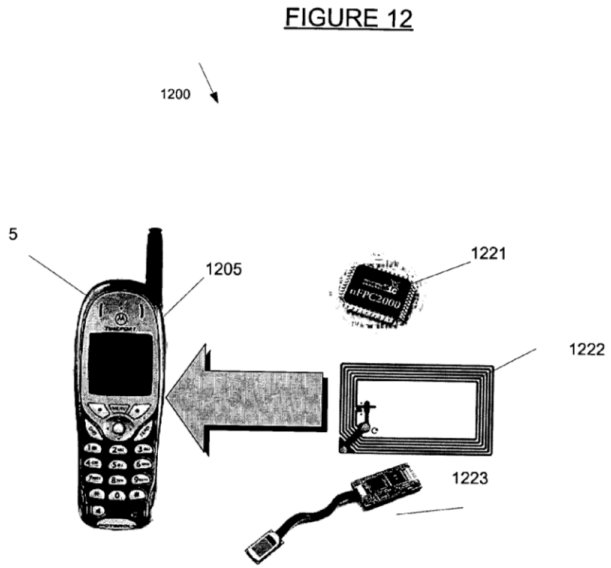
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone. Cortina '273 at [0144] According to FIG. 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF reader/writer connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information). To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Cortina '273 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Cortina '273 at [0141] In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel milage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security. Cortina '273 at [0143] FIG. 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on

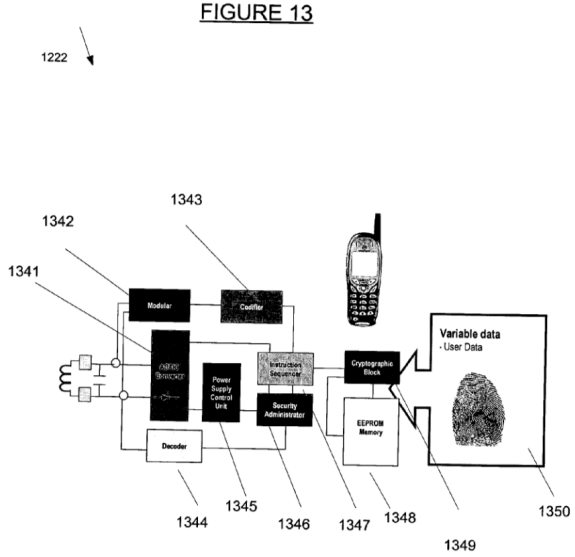
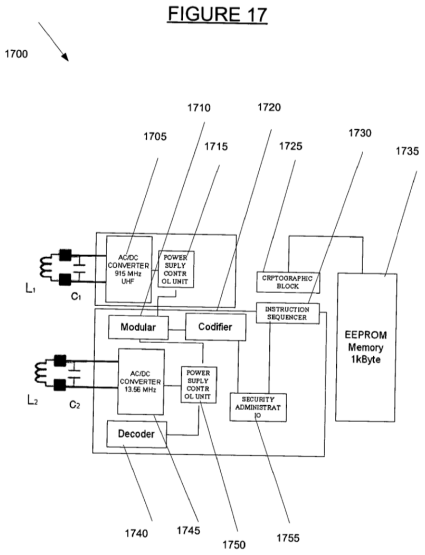
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone. Cortina '273 at [0144] According to FIG. 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF reader/writer connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information). To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Cortina '273 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Cortina '273 at Fig. 1

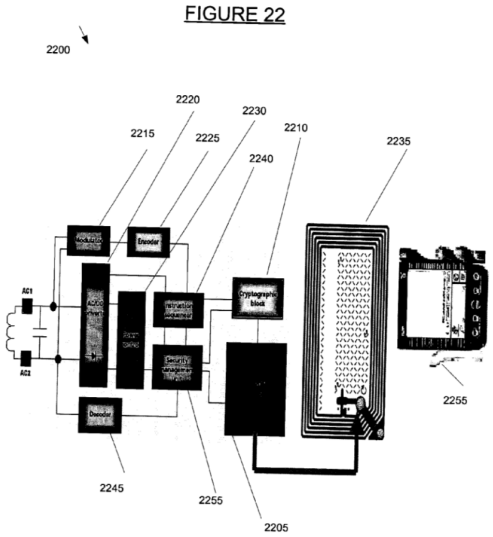
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	 Cortina '273 at Fig. 2 

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at Fig. 4  Cortina ’273 at Figure 5

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIGURE 5  Cortina '273 at Figure 9 FIGURE 9 

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at Figure 12  Cortina ’273 at Figure 13

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	FIGURE 13  Cortina ’273 at Fig. 17 FIGURE 17 

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at Fig. 22  Cortina '273 at [0020] FIG. 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120. Cortina '273 at [0022] FIG. 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF device allows electronic identification via the reading of data stored in the chip in a contactless mode. Cortina '273 at [0023] FIG. 5 illustrates a dual frequency RF device 110, according to one embodiment of the present invention. Those experienced in the art will see that a one frequency or multiple (more than two) frequency RF device can also be used. The RF device includes the following components: A modulator 215 is a device that receives baseband signals from a antenna. An AC/DC converter 220 is a device that receives an

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	alternating current (AC) and converts it to direct current (DC). An encoder 225 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 245 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 250 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 230 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 255 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 210 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 205 stores data. Information can be read and written from or to this device. Cortina '273 at [0026] Numerous features of RF identification mechanism are utilized in one embodiment of the present invention. In this embodiment, the RF device is embedded in the RF identification mechanism. One example of an RF identification mechanism is a card, and the description below refers to the identification mechanism as a card in several examples. However, those experienced in the art will recognize that multiple other embodiments of the identification mechanism are possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA). Cortina '273 at [0096] FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina '273 at [0097] In 405, the identification information (e.g., fingerprint, picture) is written to a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415, a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity. Cortina '273 at [0102] FIG. 5 illustrates an RF registered item 500, according to one embodiment of the present invention. The registered item 500 includes the following components: A modulator 515 is a device that receives baseband signals from a antenna. An AC/DC converter 520 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 525 is a device for encoding information received

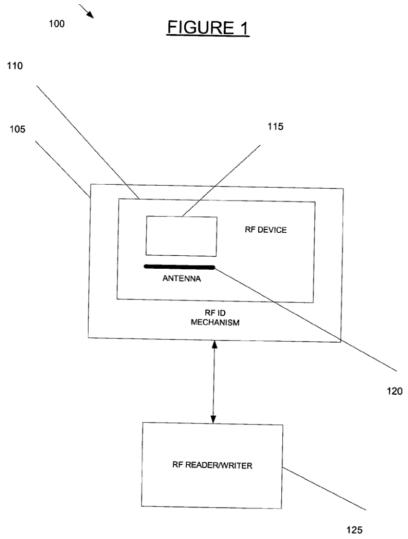
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	so that it may be utilized by another device or protocol. A decoder 545 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 550 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 530 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 555 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 510 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 505 stores data. Information can be read and written from or to this device. Cortina '273 at [0123] FIG. 9 illustrates an RF registered item 900, according to one embodiment of the present invention. The registered item 900 includes the following components, as described earlier: a modulator 915, an AC/DC converter 920, an encoder 925, a power control 930, an instruction sequencer 940, a cryptographic block 910, a decoder 945, a security management unit 955, a memory 905, and an antenna 935. Cortina '273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210. Cortina '273 at [0139] The RF cellular telephone 1205 can include the following: a fingerprint identifier 1221 (e.g., an Application Specific Integrated Circuit (ASIC) chip, which is a chip that is designed specifically to run fingerprint matching software on an operating system); and an RF device 1222 (with an antenna in the chip) to store identification information. In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223. As mentioned earlier, this could either be included on the RF cellular telephone, or on a fingerprint digital scanning device at the point of contact. Cortina '273 at [0140] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in FIG. 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements aren't met, a user cannot access the memory of the chip. The chip includes an AC-DC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information

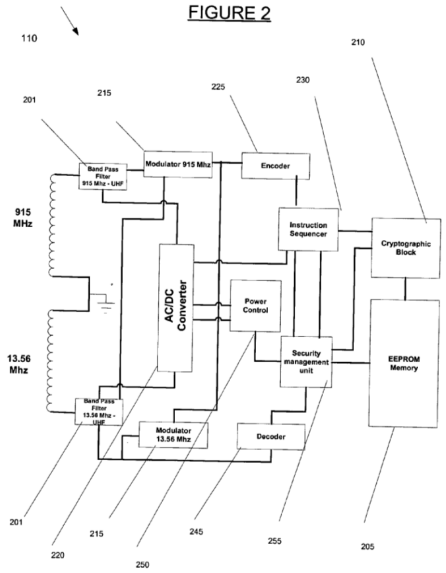
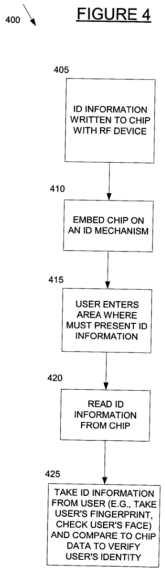
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from a antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 1347 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device. Cortina '273 at [0174] FIG. 17 illustrates an overview of the chip, according to one embodiment of the present invention. As described in detail above, the chip includes: an AC/DC converter (915 MHz) 1705 and accompanying power supply control unit 1715; a modular 1710; a codifier 1720; an AC/DC converter (13.56 MHz) 1745 and accompanying power supply control unit 1750; a decoder 1740; a security administrator 1755; an instruction sequencer 1730; a cryptographic block 1725, and memory 1735. Cortina '273 at [0199] The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz. The chip contains unique identifying data for persons or items subject to scrutiny, and can be read by nearby security or other control personnel with handheld or stationary RF reader/writer or RF reader/writer devices for real time validation. Furthermore, the RF device is manufactured with light diffraction and other high security print features that eliminate document forgery and enable instant visual verification of authenticity. The RF device also includes an integrated AFIS digital fingerprint capability. The present invention can also use other unique identifying characteristics associated with additional elements of the air transport industry, including cargo, flight services, maintenance, and aircraft parts. Cortina '273 at [0200] As described above, the chip has a memory 2205 (e.g., 2 k), an option hardware wired cryptographic block 2210 (with 4 exchange encrypted keys with up to 256 bits), a modulator 2215, a converter 2220, an encoder 2225, a power control 2230, an instruction sequencer 2260, a decoder 2245, a security management unit 2255, an memory 2205.

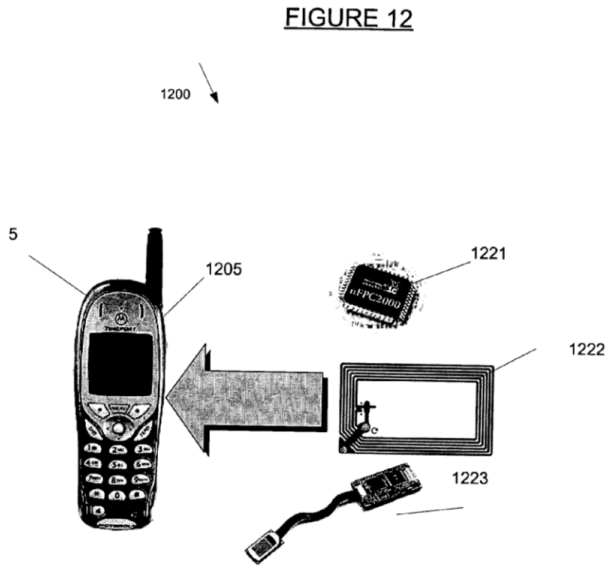
Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at [0202] FIG. 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a “one-to-many” hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card. Cortina ’273 at claim 1 a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina ’273 at claim 3 a radio frequency device comprising a radio frequency antenna embedded on a chip; an item incorporating the radio frequency device; and a radio frequency reader to read information from the radio frequency device. Cortina ’273 at claim 4 4. A method of verifying registration information of an item, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto the item; Cortina ’273 at claim 9 9. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; an identification mechanism incorporating the radio frequency device; and Cortina ’273 at claim 10 10. A method of verifying identification information of an individual, comprising:

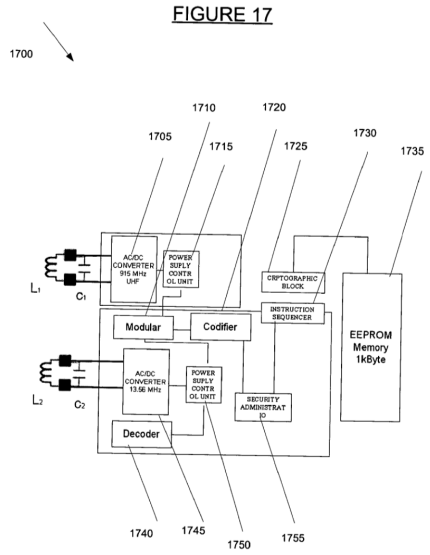
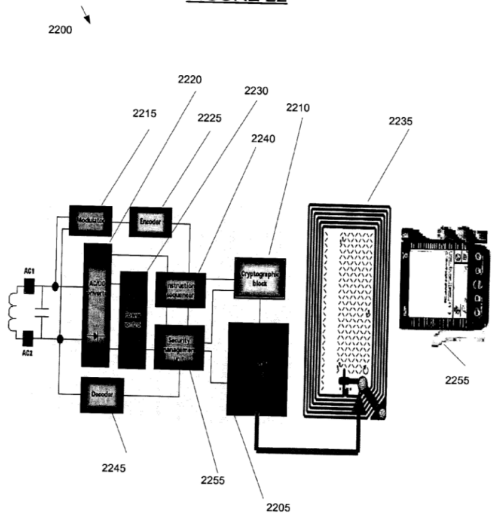
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto an identification mechanism; Cortina '273 at claim 15 15. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; a communication device incorporating the radio frequency device; and Cortina '273 at claim 16 16. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto a communications device; Cortina '273 at claim 20 20. A system of verifying border crossing control information, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina '273 at claim 21 21. A method of verifying border crossing control information, comprising: storing identification information on a chip with a radio frequency antenna; Cortina '273 at claim 41 41. The method of claim 35, wherein the chip is an integrated circuit. Cortina '273 at claim 42 a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in radio frequency identification type integrated circuit and a communication antenna connected to the radio frequency identification type; and To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Cortina '273 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Cortina '273 at [0143] FIG. 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Cortina '273 discloses or renders obvious "[a] mobile device." For example: *See* above at 1[pre]. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Cortina '273 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example:

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	See above at [1a]. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Cortina '273 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Cortina '273 at Fig. 1  Cortina '273 at Fig. 2

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIGURE 2  Cortina '273 at Fig. 4 FIGURE 4 

Claim Element	Exemplary Citations to US20040066273A1 (“Cortina ’273”)
	Cortina ’273 at Figure 12  Cortina ’273 at Fig. 17

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIGURE 17  Cortina '273 at Fig. 22 FIGURE 22 

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0020] FIG. 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120. Cortina '273 at [0022] FIG. 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF device allows electronic identification via the reading of data stored in the chip in a contactless mode. Cortina '273 at [0023] FIG. 5 illustrates a dual frequency RF device 110, according to one embodiment of the present invention. Those experienced in the art will see that a one frequency or multiple (more than two) frequency RF device can also be used. The RF device includes the following components: A modulator 215 is a device that receives baseband signals from a antenna. An AC/DC converter 220 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 225 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 245 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 250 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 230 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 255 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 210 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 205 stores data. Information can be read and written from or to this device. Cortina '273 at [0026] Numerous features of RF identification mechanism are utilized in one embodiment of the present invention. In this embodiment, the RF device is embedded in the RF identification mechanism. One example of an RF identification mechanism is a card, and the description below refers to the identification mechanism as a card in several examples. However, those experienced in the art will recognize that multiple other embodiments of the identification mechanism are possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA).

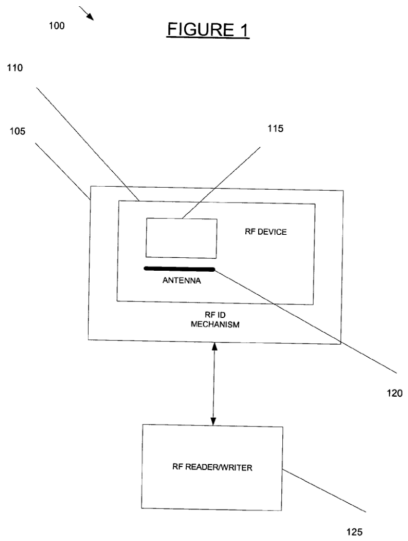
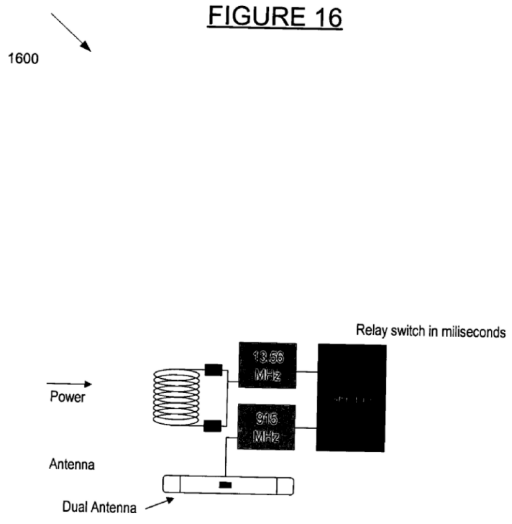
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0096] FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina '273 at [0097] In 405, the identification information (e.g., fingerprint, picture) is written to a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415, a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity. Cortina '273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210. Cortina '273 at [0139] The RF cellular telephone 1205 can include the following: a fingerprint identifier 1221 (e.g., an Application Specific Integrated Circuit (ASIC) chip, which is a chip that is designed specifically to run fingerprint matching software on an operating system); and an RF device 1222 (with an antenna in the chip) to store identification information. In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223. As mentioned earlier, this could either be included on the RF cellular telephone, or on a fingerprint digital scanning device at the point of contact. Cortina '273 at [0140] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in FIG. 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements aren't met, a user cannot access the memory of the chip. The chip includes an AC-DC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from a antenna. An AC/DC converter 1341 is a device that receives

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 1347 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device. Cortina '273 at [0141] In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel milage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security. Cortina '273 at [0174] FIG. 17 illustrates an overview of the chip, according to one embodiment of the present invention. As described in detail above, the chip includes: an AC/DC converter (915 MHz) 1705 and accompanying power supply control unit 1715; a modular 1710; a codifier 1720; an AC/DC converter (13.56 MHz) 1745 and accompanying power supply control unit 1750; a decoder 1740; a security administrator 1755; an instruction sequencer 1730; a cryptographic block 1725, and memory 1735. Cortina '273 at [0178] In 1825, at the point of entry or other appropriate place, RF antennas automatically read the RF decals as the vehicle approaches the custom's station and displays the data. A display screen on a computer (e.g., PC, PDA) in the customs area displays a reading of each RF decal as they pass within X number of feet of the antennas. The computer validates each RF decal by providing identification information (e.g., driver's photo, fingerprint, other data input at point of origin.) In 1830, the driver presents his RF laser card to a custom's officials at the point of entry (or other appropriate place) for validation and shipment verification. In 1835, the customs agent clears the shipping components for entry/exit and inputs this approval information to the RF card and RF decal. If the vehicle requires additional customs inspections, the customs agent will assign the next inspection station information to the driver's RF card and RF decals.

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0199] The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz. The chip contains unique identifying data for persons or items subject to scrutiny, and can be read by nearby security or other control personnel with handheld or stationary RF reader/writer or RF reader/writer devices for real time validation. Furthermore, the RF device is manufactured with light diffraction and other high security print features that eliminate document forgery and enable instant visual verification of authenticity. The RF device also includes an integrated AFIS digital fingerprint capability. The present invention can also use other unique identifying characteristics associated with additional elements of the air transport industry, including cargo, flight services, maintenance, and aircraft parts. Cortina '273 at [0200] As described above, the chip has a memory 2205 (e.g., 2 k), an option hardware wired cryptographic block 2210 (with 4 exchange encrypted keys with up to 256 bits), a modulator 2215, a converter 2220, an encoder 2225, a power control 2230, an instruction sequencer 2260, a decoder 2245, a security management unit 2255, an memory 2205. Cortina '273 at [0202] FIG. 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a "one-to-many" hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card. Cortina '273 at claim 1 a radio frequency device comprising a radio frequency antenna embedded on a chip;

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at claim 3 a radio frequency device comprising a radio frequency antenna embedded on a chip; an item incorporating the radio frequency device; and a radio frequency reader to read information from the radio frequency device. Cortina '273 at claim 4 4. A method of verifying registration information of an item, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto the item; Cortina '273 at claim 9 9. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; an identification mechanism incorporating the radio frequency device; and Cortina '273 at claim 10 10. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto an identification mechanism; Cortina '273 at claim 15 15. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; a communication device incorporating the radio frequency device; and Cortina '273 at claim 16 16. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto a communications device; Cortina '273 at claim 20 20. A system of verifying border crossing control information, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip;

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at claim 21 21. A method of verifying border crossing control information, comprising: storing identification information on a chip with a radio frequency antenna; Cortina '273 at claim 41 41. The method of claim 35, wherein the chip is an integrated circuit. Cortina '273 at claim 42 a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in radio frequency identification type integrated circuit and a communication antenna connected to the radio frequency identification type; and *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Cortina '273 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Cortina '273 at Abstract The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader. Cortina '273 at Fig. 1

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	 Cortina '273 at Figure 16 

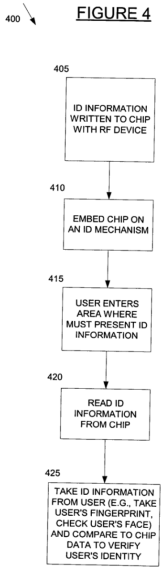
Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0003] The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader/writer. The system and method can be used in numerous embodiments, including, but not limited to: Cortina '273 at [0012] FIGS. 1, 2 and 4 illustrate the general invention, according to one embodiment of the present invention. Cortina '273 at [0015] IGS. 12-14 illustrate the RF communications device and method of use, in an embodiment of the present invention. Cortina '273 at [0020] FIG. 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120. Cortina '273 at [0022] FIG. 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF device allows electronic identification via the reading of data stored in the chip in a contactless mode. Cortina '273 at [0096] FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina '273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210.

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0140] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in FIG. 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements aren't met, a user cannot access the memory of the chip. The chip includes an AC-DC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from a antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 1347 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device. Cortina '273 at [0143] FIG. 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone.

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	Cortina '273 at [0144] According to FIG. 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF reader/writer connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information). Cortina '273 at [0165] RF Identification Mechanism, RF Device, and RF reader/writer. One embodiment of the present invention comprises: an RF identification mechanism (e.g., an RF laser card), RF decals containing an Chip (e.g., a 2K bit chip or data memory circuit) with contactless read/write capabilities and an integrated RF antenna (e.g., a 13.56 MHz RF antenna); and an RF reader/writer. Cortina '273 at [0166] Multiple Chip Background Information. Often multiple frequencies are used. This takes advantage of the best electromagnetic and electrostatic characteristics of certain frequencies, one for long range reading and the second for field penetration (e.g., rain). Multiple frequence can be created using a dual modulator that can switch in milliseconds from one frequency to another. (See FIG. 16.) Cortina '273 at [0178] In 1825, at the point of entry or other appropriate place, RF antennas automatically read the RF decals as the vehicle approaches the custom's station and displays the data. A display screen on a computer (e.g., PC, PDA) in the customs area displays a reading of each RF decal as they pass within X number of feet of the antennas. The computer validates each RF decal by providing identification information (e.g., driver's photo, fingerprint, other data input at point of origin.) In 1830, the driver presents his RF laser card to a custom's officials at the point of entry (or other appropriate place) for validation and shipment verification. In 1835, the customs agent clears the shipping components for entry/exit and inputs this approval information to the RF card and RF decal. If the vehicle requires additional customs inspections, the customs agent will assign the next inspection station information to the driver's RF card and RF decals. Cortina '273 at [0199] The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz. The chip contains unique identifying data for persons or items subject to scrutiny, and can be read by nearby security or other control personnel with handheld or

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	stationary RF reader/writer or RF reader/writer devices for real time validation. Furthermore, the RF device is manufactured with light diffraction and other high security print features that eliminate document forgery and enable instant visual verification of authenticity. The RF device also includes an integrated AFIS digital fingerprint capability. The present invention can also use other unique identifying characteristics associated with additional elements of the air transport industry, including cargo, flight services, maintenance, and aircraft parts. Cortina '273 at [0202] FIG. 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a "one-to-many" hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card. Cortina '273 at claim 1 a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina '273 at claim 3 a radio frequency device comprising a radio frequency antenna embedded on a chip; an item incorporating the radio frequency device; and a radio frequency reader to read information from the radio frequency device. Cortina '273 at claim 4 4. A method of verifying registration information of an item, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto the item; Cortina '273 at claim 9

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	9. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; an identification mechanism incorporating the radio frequency device; and Cortina '273 at claim 10 10. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto an identification mechanism; Cortina '273 at claim 15 15. A system of verifying identification information of an individual, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; a communication device incorporating the radio frequency device; and Cortina '273 at claim 16 16. A method of verifying identification information of an individual, comprising: storing first identification information on a chip with a radio frequency antenna; incorporating the chip onto a communications device; Cortina '273 at claim 20 20. A system of verifying border crossing control information, comprising; a radio frequency device comprising a radio frequency antenna embedded on a chip; Cortina '273 at claim 21 21. A method of verifying border crossing control information, comprising: storing identification information on a chip with a radio frequency antenna; Cortina '273 at claim 42 a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in radio frequency identification type integrated circuit and a communication antenna connected to the radio frequency identification type; and *See also* 1[c] and claim 5 above.

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	Cortina '273 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: *See* above at [1d]. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Cortina '273 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Cortina '273 at Fig. 4  Cortina '273 at [0096]

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	FIG. 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention. Cortina '273 at [0097] In 405, the identification information (e.g., fingerprint, picture) is written to a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415, a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity. Cortina '273 at [0137] FIG. 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210. Cortina '273 at [0141] In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel milage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security. Cortina '273 at [0143] FIG. 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate

Claim Element	Exemplary Citations to US20040066273A1 ("Cortina '273")
	embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone. Cortina '273 at [0178] In 1825, at the point of entry or other appropriate place, RF antennas automatically read the RF decals as the vehicle approaches the custom's station and displays the data. A display screen on a computer (e.g., PC, PDA) in the customs area displays a reading of each RF decal as they pass within X number of feet of the antennas. The computer validates each RF decal by providing identification information (e.g., driver's photo, fingerprint, other data input at point of origin.) In 1830, the driver presents his RF laser card to a custom's officials at the point of entry (or other appropriate place) for validation and shipment verification. In 1835, the customs agent clears the shipping components for entry/exit and inputs this approval information to the RF card and RF decal. If the vehicle requires additional customs inspections, the customs agent will assign the next inspection station information to the driver's RF card and RF decals. *See also* claim 8 above. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Cortina '273 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example: *See* above at claim 3. To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	To the extent this limitation is not disclosed by Cortina '273, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Cortina '273, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

Patent Owner's Ex. 2020
Page 209

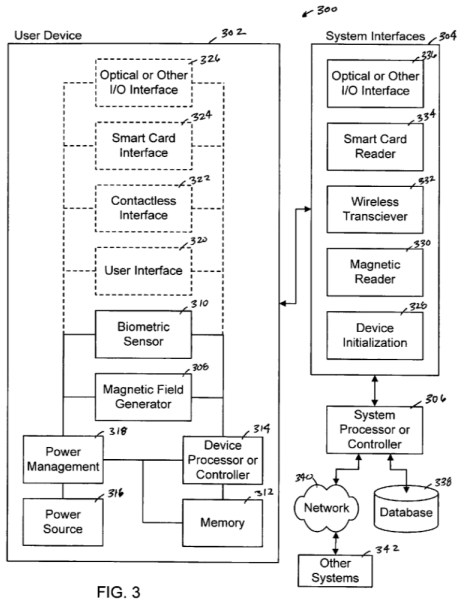
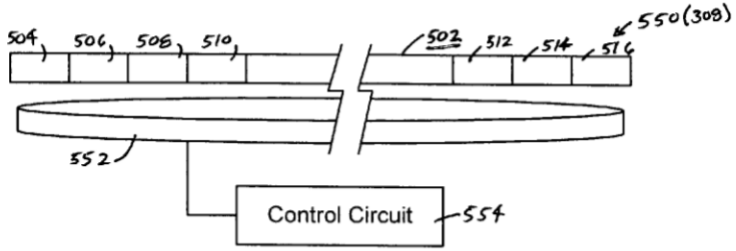
EXHIBIT E4: US20040133787A1 ("Doughty '787")

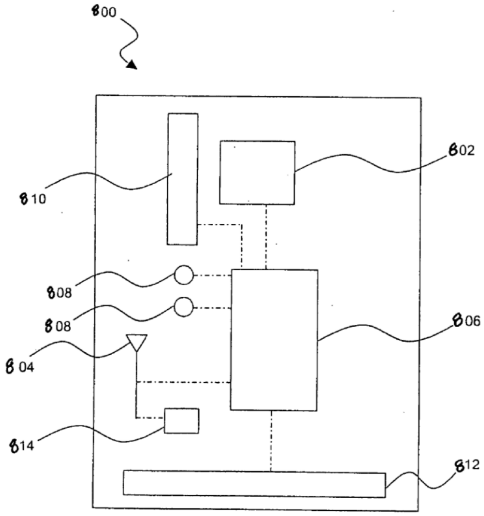
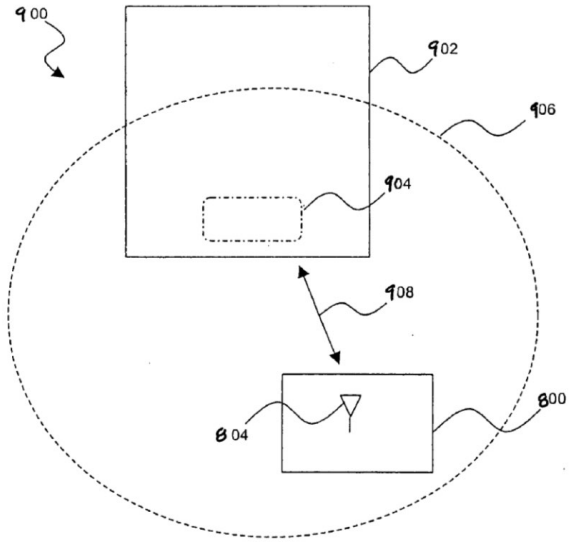
As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Doughty '787 and (b) under 35 U.S.C. § 103(a) as obvious over Doughty '787 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

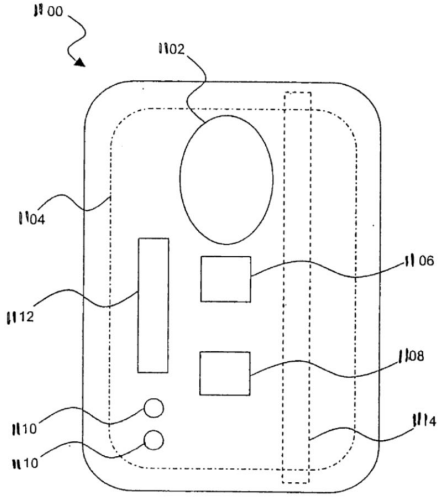
Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to US20040133787A1 ("Doughty '787")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Doughty '787 discloses or renders obvious "[a] mobile device." For example: Doughty '787 at [0046] The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	(PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc. Doughty '787 at claim 24 24. The apparatus as recited in claim 1, wherein the substrate is integrated into a personal communication device selected from a group consisting of a personal data assistant, a telecommunications device, a pager, a computer and an electronic mail transceiver. Doughty '787 at claim 86 86. The system as recited in claim 60, wherein the substrate is integrated into a personal communication device selected from a group consisting of a personal data assistant, a telecommunications device, a pager, a computer and an electronic mail transceiver. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Doughty '787 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Doughty '787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at Fig. 3

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 3 Doughty '787 at Fig. 5B  FIG. 5B Doughty '787 at Figure 8

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 Fig. 8 Doughty '787 at Figure 9  Fig. 9

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at Figure 11  Fig. 11 Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0011] The present invention also provides a method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The method includes the steps of receiving authentication data from the biometric sensor, determining whether the authentication data is valid for one of the users, and activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments. Doughty '787 at [0012] In addition, the present invention provides a system having one or more user devices, one or more system interfaces operable to communicate with the user device and a system processor communicably coupled to the one or more system interfaces. Each user device includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory. The device processor is operable to process biometric information received from the biometric sensor to verify that a

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. The user device also includes a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor. Doughty '787 at [0020] FIG. 5B depicts a block diagram of a programmable magnetic stripe using a single induction coil for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention; Doughty '787 at [0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention; Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0040]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified. Doughty '787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0050]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Referring now to FIG. 5A, a block diagram of a programmable magnetic stripe 500 (308 FIG. 3) using multiple inductive coils 518-530 in accordance with one embodiment of the present invention is shown. The programmable magnetic stripe 500 (308 FIG. 3) includes a magnetic stripe 502, multiple inductive coils 518-530 and a control circuit 532. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The individual inductive coils 518-530 are mounted immediately beneath each of the binary magnetic data cells 504-516. Each inductive coil 518-530 is electrically connected to the control circuit 532, which may be integrated into the device processor 314 (FIG. 3). When a positive or negative current is applied to each inductive coil 518-530, it changes the polarity of the magnetized particles in the binary magnetic data cell 504-516 of the data track in the magnetic stripe 502 immediately above it, thereby creating a spatially varying binary code or magnetic signal in the magnetic stripe 502 material that can be read by standard magnetic card readers when such binary code is applied in accordance with ISO standards. Doughty '787 at [0051] Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader. The data rate is determined based on the minimum and maximum swipe speeds that standard readers can accommodate. In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502. Doughty '787 at [0051]–[0052] Note that the individual data cells 504-516 are normally empty of data. There are several ways in which the card can be activated so that the data transfer can be started. For example, the card can be initially activated by the authorized user using an on-card "enable button", such as a low-power capacitance sensor, that can be built into the ring of the biometrics sensor 302 (FIG. 3) and used to "wake up" the card when the user is ready to authenticate himself/herself and begin using the card. Authentication of the card user is time stamped for use in determining the length of time to allow transmission of the emulated data. In addition, the magnetic reader 330 (FIG. 3) may have a start sentinel that signals a detector on the card to alert the card that it is in the presence of the card reader 330 (FIG. 3). Once the card is alerted that it is being swiped through the reader 330 (FIG. 3), it begins transmission of the emulated time-varying data from the device processor to the inductive coils 552, thereby generating an exact emulation and transmission to the reader 330 (FIG. 3) of the data that would have been produced by swiping the card through the reader 330 (FIG. 3) with spatially varying data included in the individual data cells 504-516. All such transmission of emulated card data is contingent upon valid biometric authentication of the card user, followed by detection of the card that it is in the presence of the reader head and the reader 330 (FIG. 3) has recognized the start sentinel on the card so that the reader 330 (FIG. 3) is ready to accept the stream of emulated data provided by the device processor. The transmission of data from the device processor 314 (FIG. 3) is suspended once the initial reading of data by the magnetic card reader 330 (FIG. 3) has been completed. This action prevents skimming of card information after the basic transaction has been completed. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320

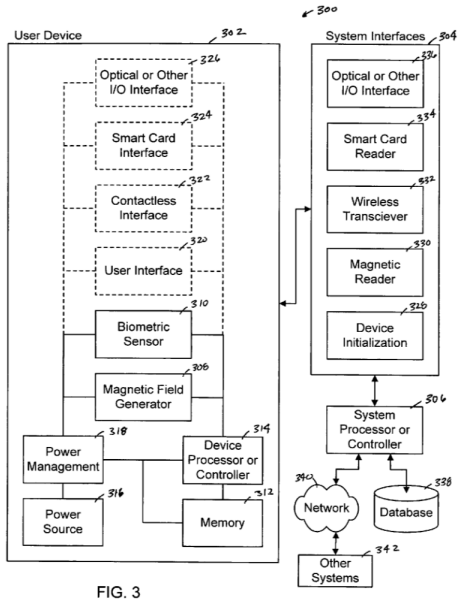
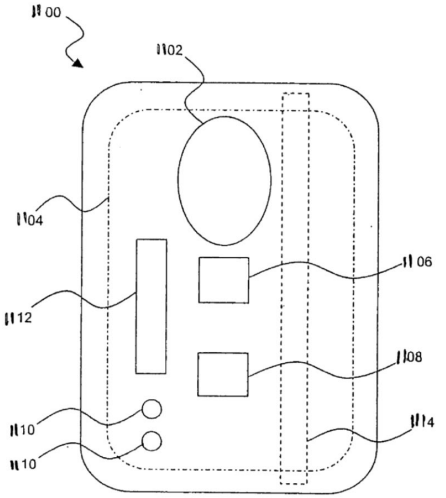
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at [0055] If, however, the authentication data is valid, as determined in decision block 718, the information associated with the authenticated user is accessed in block 720 and provided to the device outputs in block 722. The information can be a simple approval or denial of the transaction, or private information of the user that is required to enable or complete the transaction. As previously described in reference to FIG. 3, the device outputs may include a magnetic field generator 308 (programmable magnetic stripe), a contactless interface 322, a smart card interface 324, or an optical or other I/O interface 326. Using the magnetic field generator 308 for example, this step would involve activating the magnetic field generator 308 and generating a magnetic signal corresponding to the information associated with the authenticated user. In addition, the authentication step (block 716), the information access step (block 720) or the information output step (block 722) may also display information to the user, allow the user to select the information to enable the transaction or allow the user to select the device output or interface to be used. Once the transaction is complete, as determined in decision block 724, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. If, however, the transaction is not complete, as determined in decision block 724 and the process has not timed out, as determined in decision block 726, the process continues to wait for the transaction to be completed. If the process has timed out, as determined in decision block 726, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. The process can be set to interrupt the transaction and deny it if the process times out (e.g., the

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	magnetic field generator has been active for a specified period of time) or the biometric sensor no longer detects the authorized user. Note that this method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments, all of which are performed on the card/device. Doughty '787 at [0055]–[0056] Referring now to FIG. 8, one embodiment of an exemplary device 800 for effecting secure physical and commercial transactions in a contactless manner using biometrics is shown. As will be described later in greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media component 812, and a RF power conversion and power management unit 814. A number of inter-component communications paths 816 provide connections between various components of the device 800. Doughty '787 at [0057] The RF antenna 804 may perform multiple functions. For example, it may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The antenna 804 may be a single antenna capable of performing both functions or may comprise multiple antennae, with one antenna for capturing RF energy from the RF field and another antenna for supporting the two-way communication with the reader/writer device. The communications may include, for example, authenticated identification of a person operating the device 800, various purchases and financial transactions, air ticket booking and airport security check points, and other interactions between the device 800 and the reader/writer device. These communications may be secured using mechanisms such as data encryption. It is understood that other communications components, such as audio or optical components, may replace or supplement the antenna 804. In addition, the antenna 804 may be operable to function with wavelengths other than RF. Doughty '787 at [0061] Referring now to FIG. 9, the device is illustrated in an exemplary environment 900 that enables contactless interaction with a reader/writer device 902. To achieve this contactless interaction, the device 800 is shown with the antenna 804, as described in reference to FIG. 8. The device 902 uses one or more antennae 903 to communicate with device 800, as well as emanate a RF field 906 with the purpose of supplying power to compatible devices, such as device 800. In operation, a two-way communication link 908 may be established between the reader/writer device 902 and the device 800.

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at [0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the device 1100 includes several components, such as a fingerprint sensor 1102, a RF antenna 1104, a first controller 1106, a second controller 1108, function selector buttons 1110, an electro-luminescent display 1112 and a magnetic strip 1114. In the present example, the first controller 1106 is an application specific integrated circuit (“ASIC”) chip and the second controller is a smart card chip, although it is understood that the functionality of both controllers may be provided by a single controller. Doughty ’787 at [0077] Referring again to FIG. 11, the RF antenna 1104, which may include one or more antennae, may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The RF energy which is captured is converted to electrical energy and accumulated within the device 1100. In some embodiments of the device 1100, a rechargeable battery may power the electronic components when no RF energy field is present. Such a battery may be charged via a RF energy field or alternative charging means Doughty ’787 at claim 1 a magnetic field generator disposed within the substrate that is normally inactive; Doughty ’787 at claim 1 a processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified; and Doughty ’787 at claim 2 2. The apparatus as recited in claim 1, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty ’787 at claim 4

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a spatially varying or time-varying magnetic signal via the one or more induction coils and the magnetic stripe. Doughty '787 at claim 31 31. A method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor, the method comprising the steps of: receiving authentication data from the biometric sensor; determining whether the authentication data is valid for one of the users; and activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid. Doughty '787 at claim 38 38. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 42 42. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 53 53. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 57 57. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 64 64. The system as recited in claim 60, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a memory to hold transaction data; and	Doughty '787 discloses or renders obvious "a memory to hold transaction data." For example: Doughty '787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at Fig. 3

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 3 Doughty '787 at Figure 11  Fig. 11

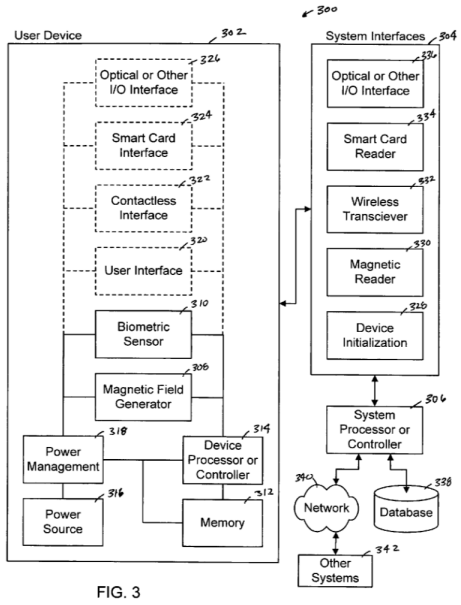
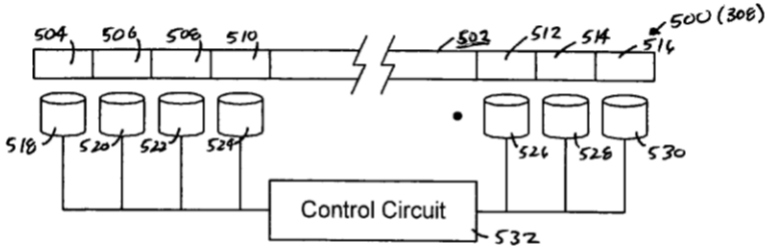
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0040]

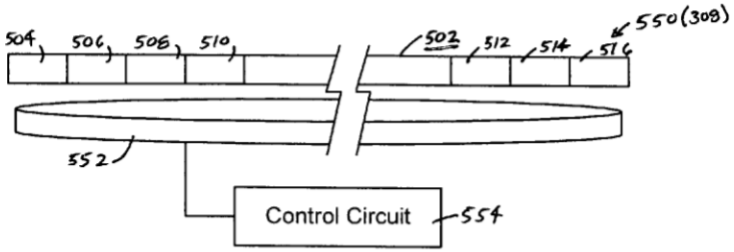
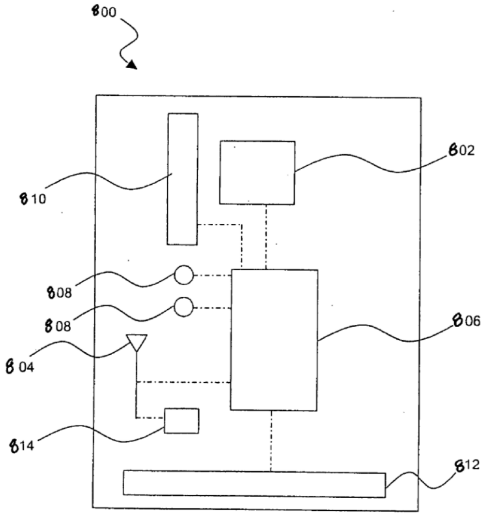
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified. Doughty '787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0046]

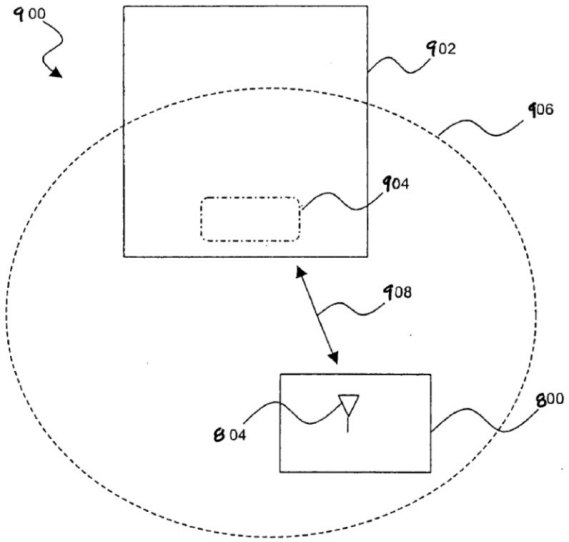
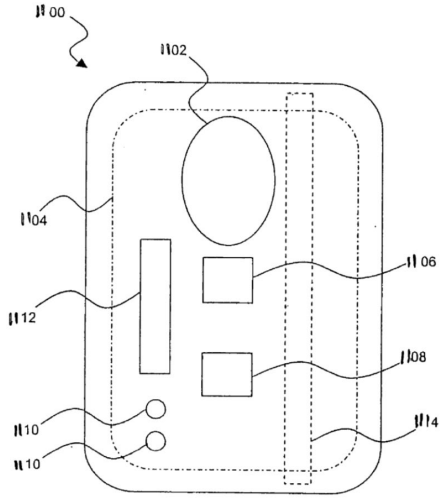
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc. Doughty ’787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty ’787 at [0065] The ASIC 1106 is a custom integrated circuit chip developed for use in the device 1100. The ASIC 1106 includes Random Access Memory (“RAM”) which may be used for temporarily storing a current fingerprint analog detected by the fingerprint sensor 1102 and for temporarily storing intermediate results of processing calculations (e.g., fingerprint comparisons, etc.). The ASIC 1106 may also include non-volatile memory (e.g., Flash memory or EEPROM) to store and retrieve one or more fingerprint template analogs that are used for comparison against the current fingerprint analog.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an "electronic purse" functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty '787 at claim 1 a memory disposed within the substrate; Doughty '787 at claim 1 a processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified; and Doughty '787 at claim 26 26. The apparatus as recited in claim 1, wherein the processor and the memory are integrated into a single integrated circuit. Doughty '787 at claim 60 60. A system comprising: one or more user devices, each user device comprising a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate, a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified, and a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor; one or more system interfaces operable to communicate with the user device; and a system processor communicably coupled to the one or more system interfaces. Doughty '787 at claim 88 88. The system as recited in claim 60, wherein the device processor and the memory are integrated into a single integrated circuit. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Doughty '787 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Doughty '787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at Fig. 3

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 3 Doughty '787 at Fig. 5A  FIG. 5A Doughty '787 at Fig. 5B

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 5B Doughty '787 at Figure 8  Fig. 8 Doughty '787 at Figure 9

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 Fig. 9 Doughty '787 at Figure 11  Fig. 11

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0011]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	The present invention also provides a method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The method includes the steps of receiving authentication data from the biometric sensor, determining whether the authentication data is valid for one of the users, and activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments. Doughty '787 at [0012] In addition, the present invention provides a system having one or more user devices, one or more system interfaces operable to communicate with the user device and a system processor communicably coupled to the one or more system interfaces. Each user device includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory. The device processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. The user device also includes a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor. Doughty '787 at [0020] FIG. 5B depicts a block diagram of a programmable magnetic stripe using a single induction coil for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention; Doughty '787 at [0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention; Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0040] Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified. Doughty '787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0045] The device 302 may also include a user interface 320 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The user interface 320 may include a touch pad, one or more buttons, a display, a voice sensor or other known user interfaces. The device 302 may also include a contactless interface 322 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The contactless interface 322 may include an antenna for wireless communication, an optical transceiver or other known contactless communication methods. In addition, device 302 may also include a smart card interface 324 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Moreover, device 302 may include an optical or other type of input/output (VO) interface 326 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318).

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0050] Referring now to FIG. 5A, a block diagram of a programmable magnetic stripe 500 (308 FIG. 3) using multiple inductive coils 518-530 in accordance with one embodiment of the present invention is shown. The programmable magnetic stripe 500 (308 FIG. 3) includes a magnetic stripe 502, multiple inductive coils 518-530 and a control circuit 532. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The individual inductive coils 518-530 are mounted immediately beneath each of the binary magnetic data cells 504-516. Each inductive coil 518-530 is electrically connected to the control circuit 532, which may be integrated into the device processor 314 (FIG. 3). When a positive or negative current is applied to each inductive coil 518-530, it changes the polarity of the magnetized particles in the binary magnetic data cell 504-516 of the data track in the magnetic stripe 502 immediately above it, thereby creating a spatially varying binary code or magnetic signal in the magnetic stripe 502 material that can be read by standard magnetic card readers when such binary code is applied in accordance with ISO standards. Doughty '787 at [0051] Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader. The data rate is determined based on the minimum and maximum swipe speeds that standard readers can accommodate. In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502. Doughty '787 at [0051]–[0052] Note that the individual data cells 504-516 are normally empty of data. There are several ways in which the card can be activated so that the data transfer can be started. For example, the card can be initially activated by the authorized user using an on-card "enable button", such as a low-power capacitance sensor, that can be built into the ring of the biometrics sensor 302 (FIG. 3) and used to "wake up" the card when the user is ready to authenticate himself/herself and begin using the card. Authentication of the card user is time stamped for use in determining the length of time to allow transmission of the emulated data. In addition, the magnetic reader 330 (FIG. 3) may have a start sentinel that signals a detector on the card to alert the card that it is in the presence of the card reader 330 (FIG. 3). Once the card is alerted that it is being swiped through the reader 330 (FIG. 3), it begins transmission of the emulated time-varying data from the device processor to the inductive coils 552, thereby generating an exact emulation and transmission to the reader 330 (FIG. 3) of the data that would have been produced by swiping the card through the reader 330 (FIG. 3) with spatially varying data included in the individual data cells 504-516. All such transmission of emulated card data is contingent upon valid biometric authentication of the card user, followed by detection of the card that it is in the presence of the reader head and the reader 330 (FIG. 3) has recognized the start sentinel on the card so that the reader 330 (FIG. 3) is ready to accept the stream of emulated data provided by the device processor. The transmission of data from the device processor 314 (FIG. 3) is suspended once the initial reading of data by the magnetic card reader 330 (FIG. 3) has been completed. This action prevents skimming of card information after the basic transaction has been completed. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at [0055] If, however, the authentication data is valid, as determined in decision block 718, the information associated with the authenticated user is accessed in block 720 and provided to the device outputs in block 722. The information can be a simple approval or denial of the transaction, or private information of the user that is required to enable or complete the transaction. As previously described in reference to FIG. 3, the device outputs may include a magnetic field generator 308 (programmable magnetic stripe), a contactless interface 322, a smart card interface 324, or an optical or other I/O interface 326. Using the magnetic field generator 308 for example, this step would involve activating the magnetic field generator 308 and generating a magnetic signal corresponding to the information associated with the authenticated user. In addition, the authentication step (block 716), the information access step (block 720) or the information output step (block 722) may also display information to the user, allow the user to select the information to enable the transaction or allow the user to select the device output or interface to be used. Once the transaction is complete, as determined in decision block 724, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. If, however, the transaction is not complete, as determined in decision block 724 and the process has not timed out, as determined in decision block 726, the process continues to wait for the transaction to be completed. If the process has timed out, as determined in decision block 726, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	704. The process can be set to interrupt the transaction and deny it if the process times out (e.g., the magnetic field generator has been active for a specified period of time) or the biometric sensor no longer detects the authorized user. Note that this method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments, all of which are performed on the card/device. Doughty '787 at [0055]–[0056] Referring now to FIG. 8, one embodiment of an exemplary device 800 for effecting secure physical and commercial transactions in a contactless manner using biometrics is shown. As will be described later in greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media component 812, and a RF power conversion and power management unit 814. A number of inter-component communications paths 816 provide connections between various components of the device 800. Doughty '787 at [0057] The RF antenna 804 may perform multiple functions. For example, it may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The antenna 804 may be a single antenna capable of performing both functions or may comprise multiple antennae, with one antenna for capturing RF energy from the RF field and another antenna for supporting the two-way communication with the reader/writer device. The communications may include, for example, authenticated identification of a person operating the device 800, various purchases and financial transactions, air ticket booking and airport security check points, and other interactions between the device 800 and the reader/writer device. These communications may be secured using mechanisms such as data encryption. It is understood that other communications components, such as audio or optical components, may replace or supplement the antenna 804. In addition, the antenna 804 may be operable to function with wavelengths other than RF. Doughty '787 at [0059] The controller 806 interacts with the biometric sensor 802 and other components of the device 800 to perform various functions. For example, the controller 806 may capture the analog of the physical attribute for long term storage as a trusted template analog of an authorized user, as well as for immediate comparison to a stored trusted template analog during an authentication procedure. The controller 806 may also determine whether the comparison indicates a match between the template analog and the analog captured by the biometric sensor 802. In addition, the controller 806 may control the dynamic information

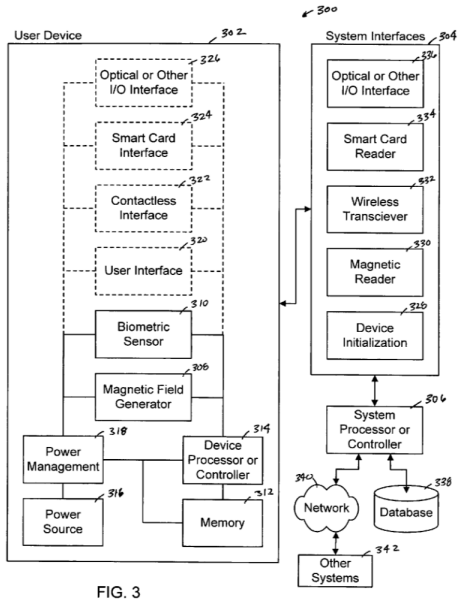
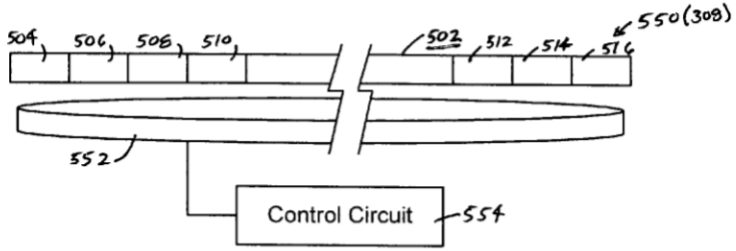
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	display 810, respond to input from the control buttons 810, and control the magnetic information media component 812. Furthermore, the controller 806 may support two-way communications with an associated reader/writer device (FIG. 9) via the RF antenna 804. The controller may be a single controller/processor or may comprise multiple controllers/processors. Doughty '787 at [0061] Referring now to FIG. 9, the device is illustrated in an exemplary environment 900 that enables contactless interaction with a reader/writer device 902. To achieve this contactless interaction, the device 800 is shown with the antenna 804, as described in reference to FIG. 8. The device 902 uses one or more antennae 903 to communicate with device 800, as well as emanate a RF field 906 with the purpose of supplying power to compatible devices, such as device 800. In operation, a two-way communication link 908 may be established between the reader/writer device 902 and the device 800. Doughty '787 at [0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the device 1100 includes several components, such as a fingerprint sensor 1102, a RF antenna 1104, a first controller 1106, a second controller 1108, function selector buttons 1110, an electro-luminescent display 1112 and a magnetic strip 1114. In the present example, the first controller 1106 is an application specific integrated circuit ("ASIC") chip and the second controller is a smart card chip, although it is understood that the functionality of both controllers may be provided by a single controller. Doughty '787 at [0077] Referring again to FIG. 11, the RF antenna 1104, which may include one or more antennae, may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The RF energy which is captured is converted to electrical energy and accumulated within the device 1100. In some embodiments of the device 1100, a rechargeable battery may power the electronic components when no RF energy field is present. Such a battery may be charged via a RF energy field or alternative charging means Doughty '787 at claim 1 a magnetic field generator disposed within the substrate that is normally inactive; Doughty '787 at claim 1

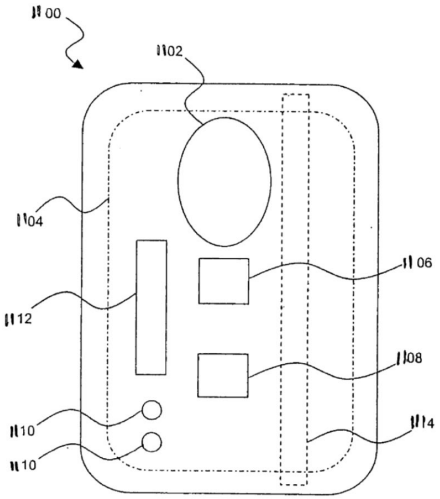
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	a processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified; and Doughty '787 at claim 2 2. The apparatus as recited in claim 1, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 4 a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a spatially varying or time-varying magnetic signal via the one or more induction coils and the magnetic stripe. Doughty '787 at claim 18 18. The apparatus as recited in claim 1, further comprising a smart card interface mounted on the substrate that is communicably coupled to the processor and electrically connected to the power source. Doughty '787 at claim 26 26. The apparatus as recited in claim 1, wherein the processor and the memory are integrated into a single integrated circuit. Doughty '787 at claim 31 31. A method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor, the method comprising the steps of: receiving authentication data from the biometric sensor; determining whether the authentication data is valid for one of the users; and activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid. Doughty '787 at claim 38 38. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at claim 42 42. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 53 53. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 57 57. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 60 60. A system comprising: one or more user devices, each user device comprising a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate, a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified, and a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor; one or more system interfaces operable to communicate with the user device; and a system processor communicably coupled to the one or more system interfaces. Doughty '787 at claim 64 64. The system as recited in claim 60, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at claim 69 69. The system as recited in claim 60, wherein the device processor comprises a smart card processor and an ASIC chip. Doughty '787 at claim 88 88. The system as recited in claim 60, wherein the device processor and the memory are integrated into a single integrated circuit. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	Doughty '787 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: Doughty '787 at [0046] The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc. Doughty '787 at claim 24

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	24. The apparatus as recited in claim 1, wherein the substrate is integrated into a personal communication device selected from a group consisting of a personal data assistant, a telecommunications device, a pager, a computer and an electronic mail transceiver. Doughty '787 at claim 86 86. The system as recited in claim 60, wherein the substrate is integrated into a personal communication device selected from a group consisting of a personal data assistant, a telecommunications device, a pager, a computer and an electronic mail transceiver. *See also* 1[pre] above. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: Doughty '787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at Fig. 3

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 3 Doughty '787 at Fig. 5B  FIG. 5B Doughty '787 at Figure 11

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 Fig. 1 Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0020] FIG. 5B depicts a block diagram of a programmable magnetic stripe using a single induction coil for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention; Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0046] The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc. Doughty ’787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty ’787 at [0050] Referring now to FIG. 5A, a block diagram of a programmable magnetic stripe 500 (308 FIG. 3) using multiple inductive coils 518-530 in accordance with one embodiment of the present invention is shown. The programmable magnetic stripe 500 (308 FIG. 3) includes a magnetic stripe 502, multiple inductive coils 518-530 and a control circuit 532. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The individual inductive coils 518-530 are mounted immediately beneath each of the binary magnetic data cells 504-516. Each inductive coil 518-530 is electrically connected to the control circuit 532, which may be integrated into the device processor 314 (FIG. 3). When a positive or negative current is applied to each inductive coil 518-530, it changes the polarity of the magnetized particles in the binary magnetic data cell 504-516 of the data track in the magnetic stripe 502 immediately above it, thereby creating a spatially varying binary code or magnetic signal in the magnetic stripe 502

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	material that can be read by standard magnetic card readers when such binary code is applied in accordance with ISO standards. Doughty '787 at [0051] Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader. The data rate is determined based on the minimum and maximum swipe speeds that standard readers can accommodate. In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502. Doughty '787 at [0051]–[0052] Note that the individual data cells 504-516 are normally empty of data. There are several ways in which the card can be activated so that the data transfer can be started. For example, the card can be initially activated by the authorized user using an on-card "enable button", such as a low-power capacitance sensor, that can be built into the ring of the biometrics sensor 302 (FIG. 3) and used to "wake up" the card when the user is ready to authenticate himself/herself and begin using the card. Authentication of the card user is time stamped for use in determining the length of time to allow transmission of the emulated data. In addition, the magnetic reader 330 (FIG. 3) may have a start sentinel that signals a detector on the card to alert the card that it is in the presence of the card reader 330 (FIG. 3). Once the card is alerted that it is

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	being swiped through the reader 330 (FIG. 3), it begins transmission of the emulated time-varying data from the device processor to the inductive coils 552, thereby generating an exact emulation and transmission to the reader 330 (FIG. 3) of the data that would have been produced by swiping the card through the reader 330 (FIG. 3) with spatially varying data included in the individual data cells 504-516. All such transmission of emulated card data is contingent upon valid biometric authentication of the card user, followed by detection of the card that it is in the presence of the reader head and the reader 330 (FIG. 3) has recognized the start sentinel on the card so that the reader 330 (FIG. 3) is ready to accept the stream of emulated data provided by the device processor. The transmission of data from the device processor 314 (FIG. 3) is suspended once the initial reading of data by the magnetic card reader 330 (FIG. 3) has been completed. This action prevents skimming of card information after the basic transaction has been completed. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at [0055] If, however, the authentication data is valid, as determined in decision block 718, the information associated with the authenticated user is accessed in block 720 and provided to the device outputs in block 722. The information can be a simple approval or denial of the transaction, or private information of the user that is required to enable or complete the transaction. As previously described in reference to FIG. 3, the device outputs may include a magnetic field generator 308 (programmable magnetic stripe), a contactless interface 322, a smart card interface 324, or an optical or other I/O interface 326. Using the magnetic field generator 308 for example, this step would involve activating the magnetic field generator 308 and generating a magnetic signal corresponding to the information associated with the authenticated user. In addition, the authentication step (block 716), the information access step (block 720) or the information output step (block 722) may also display information to the user, allow the user to select the information to enable the transaction or allow the user to select the device output or interface to be used. Once the transaction is complete, as determined in decision block 724, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. If, however, the transaction is not complete, as determined in decision block 724 and the process has not timed out, as determined in decision block 726, the process continues to wait for the transaction to be completed. If the process has timed out, as determined in decision block 726, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. The process can be set to interrupt the transaction and deny it if the process times out (e.g., the magnetic field generator has been active for a specified period of time) or the biometric sensor no longer detects the authorized user. Note that this method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments, all of which are performed on the card/device. Doughty '787 at [0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the device 1100 includes several components, such as a fingerprint sensor 1102, a RF antenna 1104, a first controller 1106, a second controller 1108, function selector buttons 1110, an electro-luminescent display 1112 and a magnetic strip 1114. In the present example, the first controller 1106 is an application specific

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	integrated circuit ("ASIC") chip and the second controller is a smart card chip, although it is understood that the functionality of both controllers may be provided by a single controller. Doughty '787 at [0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an "electronic purse" functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty '787 at [0078] The electro-luminescent display 1112 provides the capability to display information to a user of the device 1100. For example, the information may include a credit card number to support "card not present" transactions, a residual balance of an "electronic purse," air travel flight and seat assignment information, and similar information. Furthermore, interaction with the display 1112 may be accomplished via the function control buttons 1110. For example, the buttons 1110 may be used to select a credit card number (if the device 1100 stores multiple numbers) viewed via the display 1112 or to enter a personal identification number. The pliability of the electro-luminescent display 1112 aids its use in the card-like form factor of the device 1100. While two control buttons 1110 are illustrated, it is understood that other numbers and configurations of function control buttons may be used. Doughty '787 at [0079] A dynamic magnetic strip 1114 is provided to provide compatibility with existing reader devices. The dynamic magnetic strip 1114 may be used in either fixed or dynamic mode. In dynamic mode, magnetically stored information—such as a credit card number—may be changed under control of the ASIC 1106. Doughty '787 at claim 22

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	22. The apparatus as recited in claim 1, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card. Doughty '787 at claim 38 38. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 42 42. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 53 53. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 57 57. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 64 64. The system as recited in claim 60, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 84 84. The system as recited in claim 60, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Doughty '787 at [0008] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention; Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty '787 at [0054]

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty ’787 at [0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an “electronic purse” functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty '787 at [0078] The electro-luminescent display 1112 provides the capability to display information to a user of the device 1100. For example, the information may include a credit card number to support "card not present" transactions, a residual balance of an "electronic purse," air travel flight and seat assignment information, and similar information. Furthermore, interaction with the display 1112 may be accomplished via the function control buttons 1110. For example, the buttons 1110 may be used to select a credit card number (if the device 1100 stores multiple numbers) viewed via the display 1112 or to enter a personal identification number. The pliability of the electro-luminescent display 1112 aids its use in the card-like form factor of the device 1100. While two control buttons 1110 are illustrated, it is understood that other numbers and configurations of function control buttons may be used. Doughty '787 at [0079] A dynamic magnetic strip 1114 is provided to provide compatibility with existing reader devices. The dynamic magnetic strip 1114 may be used in either fixed or dynamic mode. In dynamic mode, magnetically stored information—such as a credit card number—may be changed under control of the ASIC 1106. Doughty '787 at [0095] Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment includes making retail purchases in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions. Doughty '787 at [0096] Payments for retail purchases are generally accomplished in one of three ways: with cash; with a check; or with a credit or debit card. In a cash transaction, there is generally no need for validating the identification of the buyer. In a transaction where a check is used, there generally is a need for identification of the buyer. This identification may occur by way of the buyer's presentation of a driver's license or alternate, approved identification card, presentation of a credit card to indicate credit-worthiness, or by a

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	telecommunication connection to check security processing service to assure fund availability for, and legitimacy of, the check presented for payment. Doughty '787 at [0097] In a transaction where a credit or debit card is used, there are generally various procedural mechanisms in place to assure buyer identification and legitimate ownership of the card presented for the payment transaction. For example, the payment may require the entry of numeric PIN ("Personal Identification Number") security code by the buyer and assumed owner of the card. Alternatively, sales personnel may compare the buyer's signature on the back of the card presented for payment versus the requested signature on the purchase receipt provided for the goods or services purchased. In some cases, cards have a photograph of the card owner on them, and sales personnel may make cursory comparisons of this photograph with the buyer to establish identification. However, both photographic comparison and PIN-based card authorization have weaknesses for assuring identification, and both have potential risk for fraudulent processing. Photographs can be falsified and PIN numbers can be stolen. In the case of on-line purchases, buyers are not present to provide authorizing signatures, photographic comparisons cannot be made with existing processing infrastructure, and PIN-based transactions can be compromised with identity theft. Doughty '787 at claim 36 36. The method as recited in claim 31, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. Doughty '787 at claim 51 51. The computer program as recited in claim 46, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Doughty '787 at [0008]

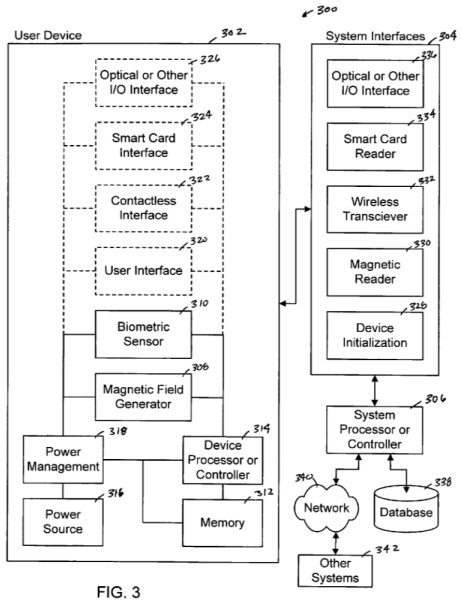
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention; Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.

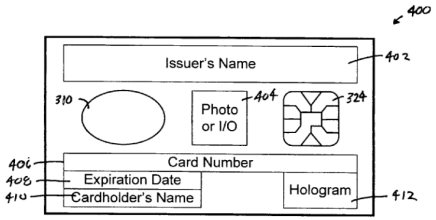
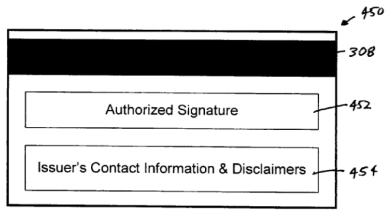
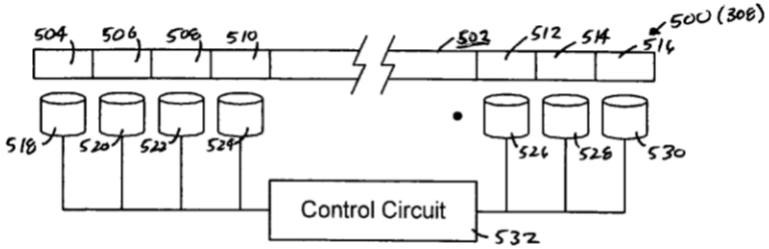
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a

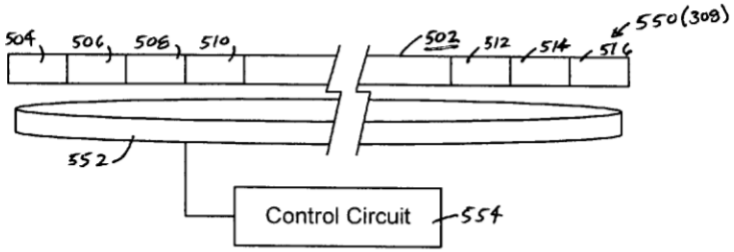
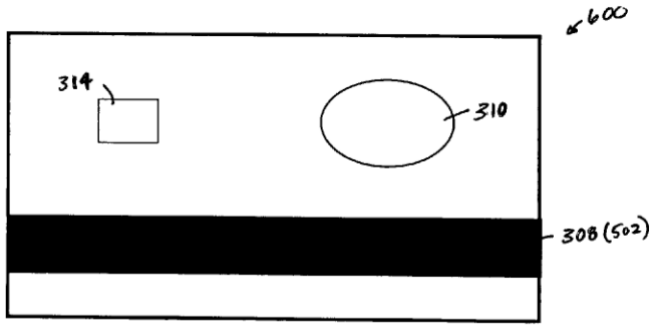
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at [0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an "electronic purse" functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty '787 at [0078]

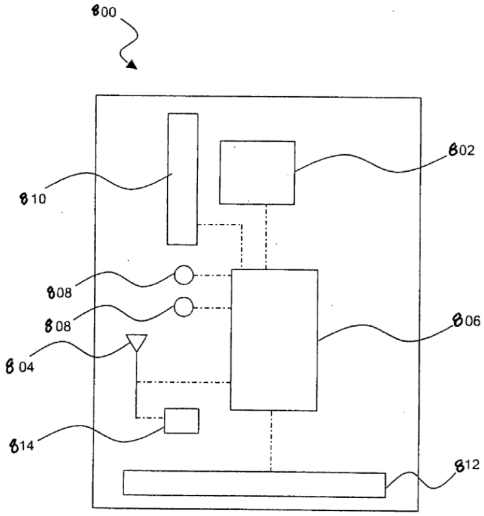
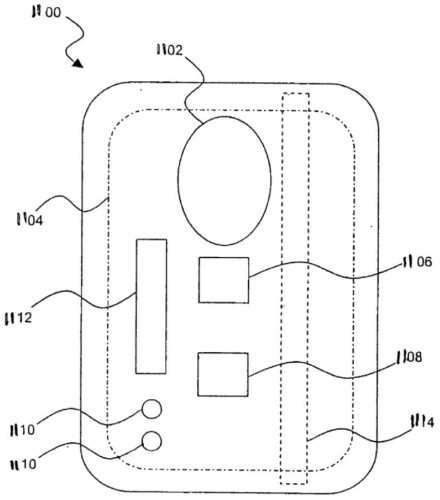
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	The electro-luminescent display 1112 provides the capability to display information to a user of the device 1100. For example, the information may include a credit card number to support "card not present" transactions, a residual balance of an "electronic purse," air travel flight and seat assignment information, and similar information. Furthermore, interaction with the display 1112 may be accomplished via the function control buttons 1110. For example, the buttons 1110 may be used to select a credit card number (if the device 1100 stores multiple numbers) viewed via the display 1112 or to enter a personal identification number. The pliability of the electro-luminescent display 1112 aids its use in the card-like form factor of the device 1100. While two control buttons 1110 are illustrated, it is understood that other numbers and configurations of function control buttons may be used. Doughty '787 at [0079] A dynamic magnetic strip 1114 is provided to provide compatibility with existing reader devices. The dynamic magnetic strip 1114 may be used in either fixed or dynamic mode. In dynamic mode, magnetically stored information—such as a credit card number—may be changed under control of the ASIC 1106. Doughty '787 at [0095] Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment includes making retail purchases in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions. Doughty '787 at [0096] Payments for retail purchases are generally accomplished in one of three ways: with cash; with a check; or with a credit or debit card. In a cash transaction, there is generally no need for validating the identification of the buyer. In a transaction where a check is used, there generally is a need for identification of the buyer. This identification may occur by way of the buyer's presentation of a driver's license or alternate, approved identification card, presentation of a credit card to indicate credit-worthiness, or by a telecommunication connection to check security processing service to assure fund availability for, and legitimacy of, the check presented for payment. Doughty '787 at [0097]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	In a transaction where a credit or debit card is used, there are generally various procedural mechanisms in place to assure buyer identification and legitimate ownership of the card presented for the payment transaction. For example, the payment may require the entry of numeric PIN ("Personal Identification Number") security code by the buyer and assumed owner of the card. Alternatively, sales personnel may compare the buyer's signature on the back of the card presented for payment versus the requested signature on the purchase receipt provided for the goods or services purchased. In some cases, cards have a photograph of the card owner on them, and sales personnel may make cursory comparisons of this photograph with the buyer to establish identification. However, both photographic comparison and PIN-based card authorization have weaknesses for assuring identification, and both have potential risk for fraudulent processing. Photographs can be falsified and PIN numbers can be stolen. In the case of on-line purchases, buyers are not present to provide authorizing signatures, photographic comparisons cannot be made with existing processing infrastructure, and PIN-based transactions can be compromised with identity theft. Doughty '787 at claim 22 22. The apparatus as recited in claim 1, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card. Doughty '787 at claim 36 36. The method as recited in claim 31, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. Doughty '787 at claim 51 51. The computer program as recited in claim 46, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example:

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
circuitry coupled to the memory and the processor.	Doughty '787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at Fig. 3  FIG. 3 Doughty '787 at Fig. 4A–B

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 4A  FIG. 4B Doughty '787 at Fig. 5A  FIG. 5A Doughty '787 at Fig. 5B

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 5B Doughty '787 at Fig. 6  FIG. 6 Doughty '787 at Figure 8

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 Fig. 8 Doughty '787 at Figure 11  Fig. 11

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0008] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0012] In addition, the present invention provides a system having one or more user devices, one or more system interfaces operable to communicate with the user device and a system processor communicably coupled to the one or more system interfaces. Each user device includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory. The device processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. The user device also includes a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor. Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0040] Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified. Doughty '787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0045] The device 302 may also include a user interface 320 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The user interface 320 may include a touch pad, one or more buttons, a display, a voice sensor or other known user interfaces. The device 302 may also include a contactless interface 322 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The contactless interface 322 may include an antenna for wireless communication, an optical transceiver or other known contactless communication methods. In addition, device 302 may also include a smart card interface 324 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Moreover, device 302 may include an optical or other type of input/output (VO) interface 326 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Doughty '787 at [0046] The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc. Doughty '787 at [0047] The one or more system interfaces 304 may include a device initialization interface 328, a magnetic reader 330, a wireless communications interface (transceiver) 332, a smart card reader 334, or an optical or other input/output interface 336. The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly, depending on the desired application and implementation. Other non-system interfaces may include a battery recharger, personal computer interface or personal data assistant (PDA). The one or more system interfaces 304 are communicably coupled to a system processor or controller 306, which in turn may be communicably coupled to a database 338 or one or more remote systems or computers 342 via network 340. Network 340 may be a local area network or wide area network, such as the Internet. Doughty '787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty '787 at [0050] Referring now to FIG. 5A, a block diagram of a programmable magnetic stripe 500 (308 FIG. 3) using multiple inductive coils 518-530 in accordance with one embodiment of the present invention is shown. The programmable magnetic stripe 500 (308 FIG. 3) includes a magnetic stripe 502, multiple inductive coils 518-530 and a control circuit 532. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The individual inductive coils 518-530 are mounted immediately beneath

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	each of the binary magnetic data cells 504-516. Each inductive coil 518-530 is electrically connected to the control circuit 532, which may be integrated into the device processor 314 (FIG. 3). When a positive or negative current is applied to each inductive coil 518-530, it changes the polarity of the magnetized particles in the binary magnetic data cell 504-516 of the data track in the magnetic stripe 502 immediately above it, thereby creating a spatially varying binary code or magnetic signal in the magnetic stripe 502 material that can be read by standard magnetic card readers when such binary code is applied in accordance with ISO standards. Doughty '787 at [0051] Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader. The data rate is determined based on the minimum and maximum swipe speeds that standard readers can accommodate. In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502. Doughty '787 at [0055]–[0056] Referring now to FIG. 8, one embodiment of an exemplary device 800 for effecting secure physical and commercial transactions in a contactless manner using biometrics is shown. As will be described later in greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio

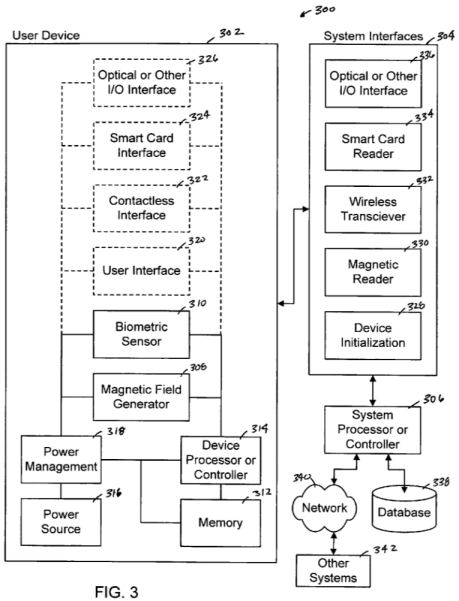
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media component 812, and a RF power conversion and power management unit 814. A number of inter-component communications paths 816 provide connections between various components of the device 800. Doughty '787 at [0059] The controller 806 interacts with the biometric sensor 802 and other components of the device 800 to perform various functions. For example, the controller 806 may capture the analog of the physical attribute for long term storage as a trusted template analog of an authorized user, as well as for immediate comparison to a stored trusted template analog during an authentication procedure. The controller 806 may also determine whether the comparison indicates a match between the template analog and the analog captured by the biometric sensor 802. In addition, the controller 806 may control the dynamic information display 810, respond to input from the control buttons 810, and control the magnetic information media component 812. Furthermore, the controller 806 may support two-way communications with an associated reader/writer device (FIG. 9) via the RF antenna 804. The controller may be a single controller/processor or may comprise multiple controllers/processors. Doughty '787 at [0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the device 1100 includes several components, such as a fingerprint sensor 1102, a RF antenna 1104, a first controller 1106, a second controller 1108, function selector buttons 1110, an electro-luminescent display 1112 and a magnetic strip 1114. In the present example, the first controller 1106 is an application specific integrated circuit ("ASIC") chip and the second controller is a smart card chip, although it is understood that the functionality of both controllers may be provided by a single controller. Doughty '787 at [0065] The ASIC 1106 is a custom integrated circuit chip developed for use in the device 1100. The ASIC 1106 includes Random Access Memory ("RAM") which may be used for temporarily storing a current fingerprint analog detected by the fingerprint sensor 1102 and for temporarily storing intermediate results of processing calculations (e.g., fingerprint comparisons, etc.). The ASIC 1106 may also include non-volatile memory (e.g., Flash memory or EEPROM) to store and retrieve one or more fingerprint template analogs that are used for comparison against the current fingerprint analog. Doughty '787 at [0067]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an "electronic purse" functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty '787 at claim 4 a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a spatially varying or time-varying magnetic signal via the one or more induction coils and the magnetic stripe. Doughty '787 at claim 7 7. The apparatus as recited in claim 1, wherein the processor comprises a smart card processor and an ASIC chip. Doughty '787 at claim 18 18. The apparatus as recited in claim 1, further comprising a smart card interface mounted on the substrate that is communicably coupled to the processor and electrically connected to the power source. Doughty '787 at claim 26 26. The apparatus as recited in claim 1, wherein the processor and the memory are integrated into a single integrated circuit. Doughty '787 at claim 61 61. The system as recited in claim 60, wherein the one or more system interfaces includes an optical interface, a smart card interface, a wireless communication interface, a magnetic reader, an initialization interface or a recharger. Doughty '787 at claim 69

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	69. The system as recited in claim 60, wherein the device processor comprises a smart card processor and an ASIC chip. Doughty '787 at claim 80 80. The system as recited in claim 60, further comprising a smart card interface mounted on the substrate that is communicably coupled to the device processor and electrically connected to the power source. Doughty '787 at claim 88 88. The system as recited in claim 60, wherein the device processor and the memory are integrated into a single integrated circuit. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at claim 38 38. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at claim 42 42. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 53 53. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 57 57. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 64 64. The system as recited in claim 60, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Doughty '787 discloses or renders obvious "[a] mobile device." For example: *See* above at 1[pre]. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Doughty '787 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a].

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Doughty '787 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Doughty '787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at Fig. 3  FIG. 3

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at Fig. 4A–B

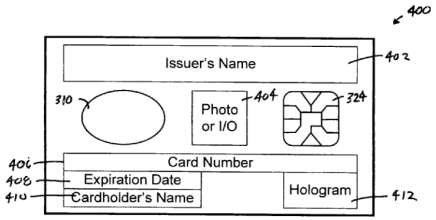


FIG. 4A

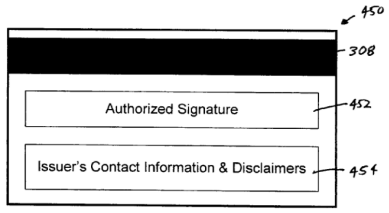


FIG. 4B

Doughty '787 at Fig. 5A

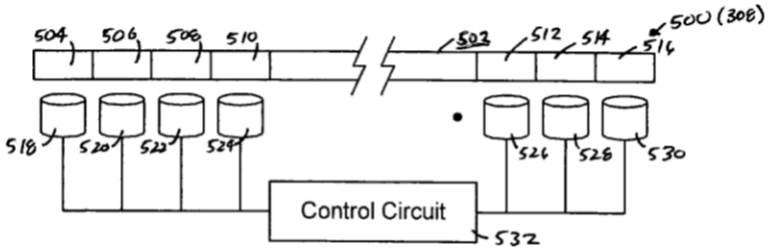
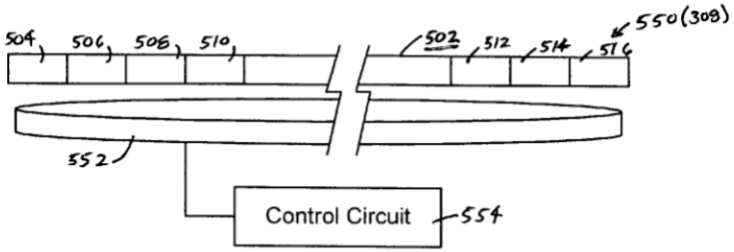
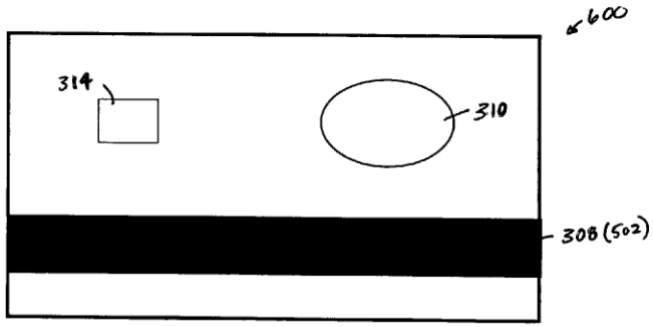
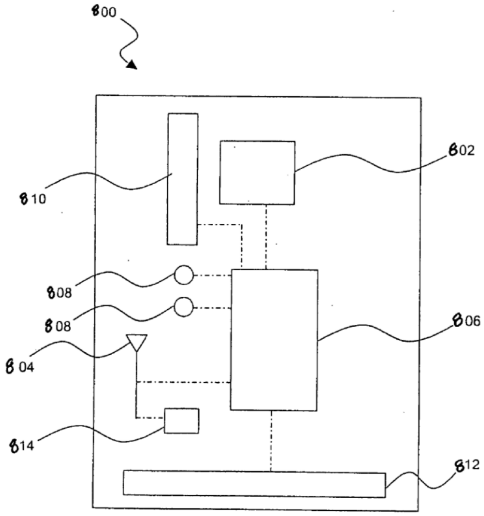
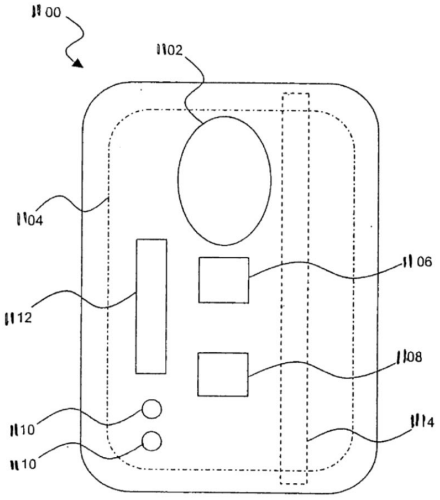


FIG. 5A

Doughty '787 at Fig. 5B

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 5B Doughty '787 at Fig. 6  FIG. 6 Doughty '787 at Figure 8

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 Fig. 8 Doughty '787 at Figure 11  Fig. 11

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0002] The present invention relates generally to the field of electronic devices and equipment used in the authentication and processing of commercial and security related transactions and, more particularly, to a system, method and apparatus for enabling transactions using biometrically enabled programmable magnetic stripes Doughty '787 at [0008] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention; Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0040]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified. Doughty '787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0045]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	The device 302 may also include a user interface 320 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The user interface 320 may include a touch pad, one or more buttons, a display, a voice sensor or other known user interfaces. The device 302 may also include a contactless interface 322 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The contactless interface 322 may include an antenna for wireless communication, an optical transceiver or other known contactless communication methods. In addition, device 302 may also include a smart card interface 324 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Moreover, device 302 may include an optical or other type of input/output (VO) interface 326 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Doughty '787 at [0046] The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc. Doughty '787 at [0047] The one or more system interfaces 304 may include a device initialization interface 328, a magnetic reader 330, a wireless communications interface (transceiver) 332, a smart card reader 334, or an optical or other input/output interface 336. The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly, depending on the desired application and implementation. Other non-system interfaces may include a battery recharger, personal computer interface or personal data

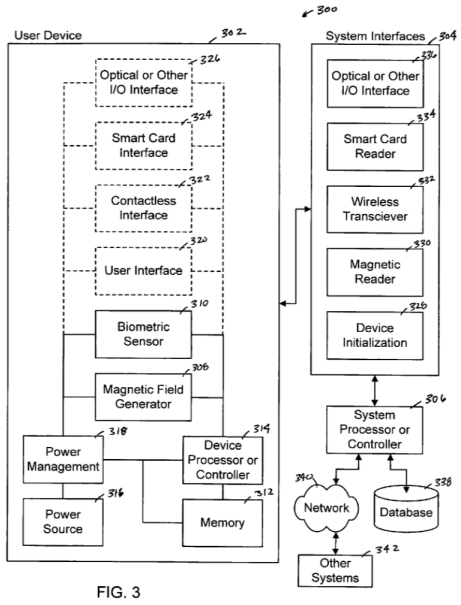
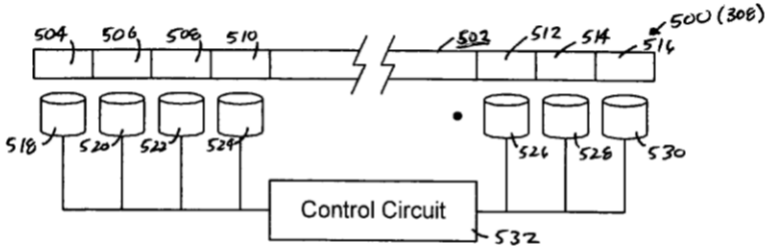
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	assistant (PDA). The one or more system interfaces 304 are communicably coupled to a system processor or controller 306, which in turn may be communicably coupled to a database 338 or one or more remote systems or computers 342 via network 340. Network 340 may be a local area network or wide area network, such as the Internet. Doughty '787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored

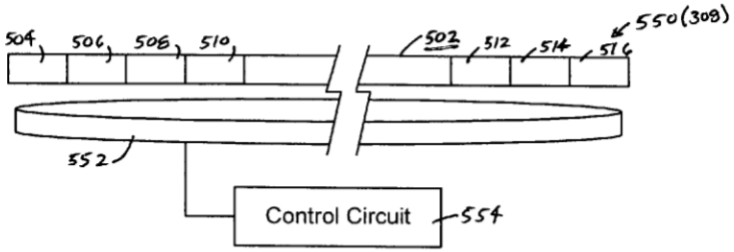
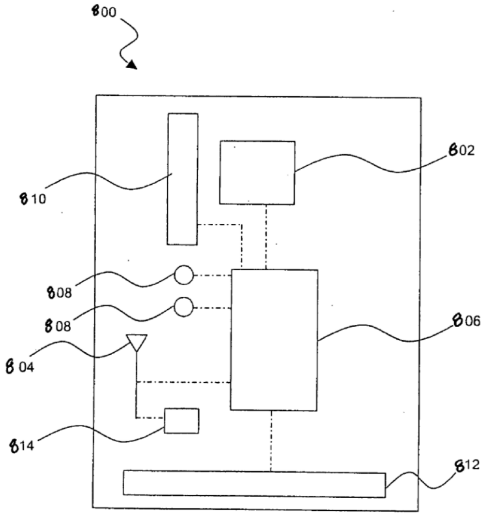
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at [0055]–[0056] Referring now to FIG. 8, one embodiment of an exemplary device 800 for effecting secure physical and commercial transactions in a contactless manner using biometrics is shown. As will be described later in greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media component 812, and a RF power conversion and power management unit 814. A number of inter-component communications paths 816 provide connections between various components of the device 800. Doughty '787 at [0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the device 1100 includes several components, such as a fingerprint sensor 1102, a RF antenna 1104, a first controller 1106, a second controller 1108, function selector buttons 1110, an electro-luminescent display 1112 and a magnetic strip 1114. In the present example, the first controller 1106 is an application specific integrated circuit ("ASIC") chip and the second controller is a smart card chip, although it is understood that the functionality of both controllers may be provided by a single controller. Doughty '787 at [0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an "electronic purse" functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the

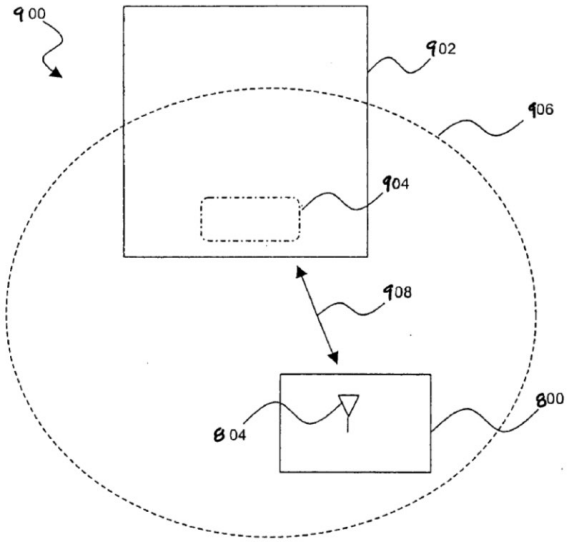
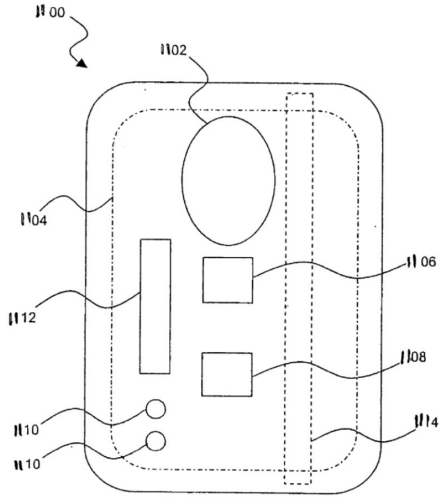
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty '787 at [0079] A dynamic magnetic strip 1114 is provided to provide compatibility with existing reader devices. The dynamic magnetic strip 1114 may be used in either fixed or dynamic mode. In dynamic mode, magnetically stored information—such as a credit card number—may be changed under control of the ASIC 1106. Doughty '787 at [0095] Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment includes making retail purchases in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions. Doughty '787 at [0096] Payments for retail purchases are generally accomplished in one of three ways: with cash; with a check; or with a credit or debit card. In a cash transaction, there is generally no need for validating the identification of the buyer. In a transaction where a check is used, there generally is a need for identification of the buyer. This identification may occur by way of the buyer's presentation of a driver's license or alternate, approved identification card, presentation of a credit card to indicate credit-worthiness, or by a telecommunication connection to check security processing service to assure fund availability for, and legitimacy of, the check presented for payment. Doughty '787 at [0097] In a transaction where a credit or debit card is used, there are generally various procedural mechanisms in place to assure buyer identification and legitimate ownership of the card presented for the payment transaction. For example, the payment may require the entry of numeric PIN ("Personal Identification Number") security code by the buyer and assumed owner of the card. Alternatively, sales personnel may compare the buyer's signature on the back of the card presented for payment versus the requested signature on the purchase receipt provided for the goods or services purchased. In some cases, cards have a photograph of the card owner on them, and sales personnel may make cursory comparisons of this

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	photograph with the buyer to establish identification. However, both photographic comparison and PIN-based card authorization have weaknesses for assuring identification, and both have potential risk for fraudulent processing. Photographs can be falsified and PIN numbers can be stolen. In the case of on-line purchases, buyers are not present to provide authorizing signatures, photographic comparisons cannot be made with existing processing infrastructure, and PIN-based transactions can be compromised with identity theft. Doughty '787 at claim 7 7. The apparatus as recited in claim 1, wherein the processor comprises a smart card processor and an ASIC chip. Doughty '787 at claim 18 18. The apparatus as recited in claim 1, further comprising a smart card interface mounted on the substrate that is communicably coupled to the processor and electrically connected to the power source. Doughty '787 at claim 26 26. The apparatus as recited in claim 1, wherein the processor and the memory are integrated into a single integrated circuit. Doughty '787 at claim 32 32. The method as recited in claim 31, wherein the information associated with the authenticated user enables approval of the transaction. Doughty '787 at claim 36 36. The method as recited in claim 31, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. Doughty '787 at claim 51 51. The computer program as recited in claim 46, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. Doughty '787 at claim 61 61. The system as recited in claim 60, wherein the one or more system interfaces includes an optical interface, a smart card interface, a wireless communication interface, a magnetic reader, an initialization interface or a recharger.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at claim 69 69. The system as recited in claim 60, wherein the device processor comprises a smart card processor and an ASIC chip. Doughty '787 at claim 80 80. The system as recited in claim 60, further comprising a smart card interface mounted on the substrate that is communicably coupled to the device processor and electrically connected to the power source. Doughty '787 at claim 84 84. The system as recited in claim 60, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card. *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Doughty '787 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Doughty '787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at Fig. 3

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 3 Doughty '787 at Fig. 5A  FIG. 5A Doughty '787 at Fig. 5B

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 5B Doughty '787 at Figure 8  Fig. 8 Doughty '787 at Figure 9

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 Fig. 9 Doughty '787 at Figure 11  Fig. 11

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty '787 at [0011]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	The present invention also provides a method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The method includes the steps of receiving authentication data from the biometric sensor, determining whether the authentication data is valid for one of the users, and activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments. Doughty '787 at [0012] In addition, the present invention provides a system having one or more user devices, one or more system interfaces operable to communicate with the user device and a system processor communicably coupled to the one or more system interfaces. Each user device includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory. The device processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. The user device also includes a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor. Doughty '787 at [0020] FIG. 5B depicts a block diagram of a programmable magnetic stripe using a single induction coil for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention; Doughty '787 at [0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention; Doughty '787 at [0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0040] Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified. Doughty '787 at [0041]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0045] The device 302 may also include a user interface 320 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The user interface 320 may include a touch pad, one or more buttons, a display, a voice sensor or other known user interfaces. The device 302 may also include a contactless interface 322 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The contactless interface 322 may include an antenna for wireless communication, an optical transceiver or other known contactless communication methods. In addition, device 302 may also include a smart card interface 324 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Moreover, device 302 may include an optical or other type of input/output (VO) interface 326 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Doughty '787 at [0050] Referring now to FIG. 5A, a block diagram of a programmable magnetic stripe 500 (308 FIG. 3) using multiple inductive coils 518-530 in accordance with one embodiment of the present invention is shown. The programmable magnetic stripe 500 (308 FIG. 3) includes a magnetic stripe 502, multiple inductive coils 518-530 and a control circuit 532. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The individual inductive coils 518-530 are mounted immediately beneath each of the binary magnetic data cells 504-516. Each inductive coil 518-530 is electrically connected to

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	the control circuit 532, which may be integrated into the device processor 314 (FIG. 3). When a positive or negative current is applied to each inductive coil 518-530, it changes the polarity of the magnetized particles in the binary magnetic data cell 504-516 of the data track in the magnetic stripe 502 immediately above it, thereby creating a spatially varying binary code or magnetic signal in the magnetic stripe 502 material that can be read by standard magnetic card readers when such binary code is applied in accordance with ISO standards. Doughty '787 at [0051] Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader. The data rate is determined based on the minimum and maximum swipe speeds that standard readers can accommodate. In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502. Doughty '787 at [0051]–[0052] Note that the individual data cells 504-516 are normally empty of data. There are several ways in which the card can be activated so that the data transfer can be started. For example, the card can be initially activated by the authorized user using an on-card "enable button", such as a low-power capacitance sensor, that can be built into the ring of the biometrics sensor 302 (FIG. 3) and used to "wake up" the card

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	when the user is ready to authenticate himself/herself and begin using the card. Authentication of the card user is time stamped for use in determining the length of time to allow transmission of the emulated data. In addition, the magnetic reader 330 (FIG. 3) may have a start sentinel that signals a detector on the card to alert the card that it is in the presence of the card reader 330 (FIG. 3). Once the card is alerted that it is being swiped through the reader 330 (FIG. 3), it begins transmission of the emulated time-varying data from the device processor to the inductive coils 552, thereby generating an exact emulation and transmission to the reader 330 (FIG. 3) of the data that would have been produced by swiping the card through the reader 330 (FIG. 3) with spatially varying data included in the individual data cells 504-516. All such transmission of emulated card data is contingent upon valid biometric authentication of the card user, followed by detection of the card that it is in the presence of the reader head and the reader 330 (FIG. 3) has recognized the start sentinel on the card so that the reader 330 (FIG. 3) is ready to accept the stream of emulated data provided by the device processor. The transmission of data from the device processor 314 (FIG. 3) is suspended once the initial reading of data by the magnetic card reader 330 (FIG. 3) has been completed. This action prevents skimming of card information after the basic transaction has been completed. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored

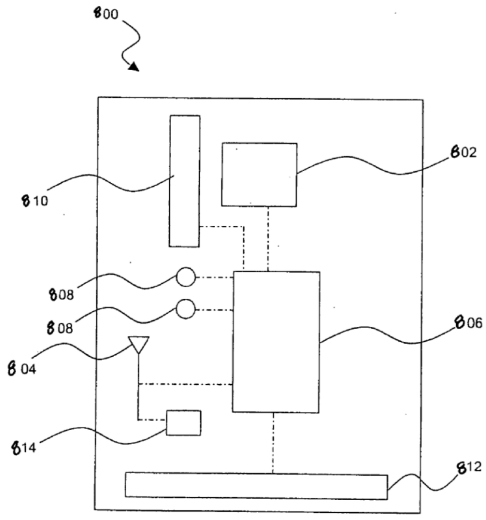
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at [0055] If, however, the authentication data is valid, as determined in decision block 718, the information associated with the authenticated user is accessed in block 720 and provided to the device outputs in block 722. The information can be a simple approval or denial of the transaction, or private information of the user that is required to enable or complete the transaction. As previously described in reference to FIG. 3, the device outputs may include a magnetic field generator 308 (programmable magnetic stripe), a contactless interface 322, a smart card interface 324, or an optical or other I/O interface 326. Using the magnetic field generator 308 for example, this step would involve activating the magnetic field generator 308 and generating a magnetic signal corresponding to the information associated with the authenticated user. In addition, the authentication step (block 716), the information access step (block 720) or the information output step (block 722) may also display information to the user, allow the user to select the information to enable the transaction or allow the user to select the device output or interface to be used. Once the transaction is complete, as determined in decision block 724, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. If, however, the transaction is not complete, as determined in decision block 724 and the process has not timed out, as determined in decision block 726, the process continues to wait for the transaction to be completed. If the process has timed out, as determined in decision block 726, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. The process can be set to interrupt the transaction and deny it if the process times out (e.g., the magnetic field generator has been active for a specified period of time) or the biometric sensor no longer detects the authorized user. Note that this method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments, all of which are performed on the card/device. Doughty '787 at [0055]–[0056] Referring now to FIG. 8, one embodiment of an exemplary device 800 for effecting secure physical and commercial transactions in a contactless manner using biometrics is shown. As will be described later in

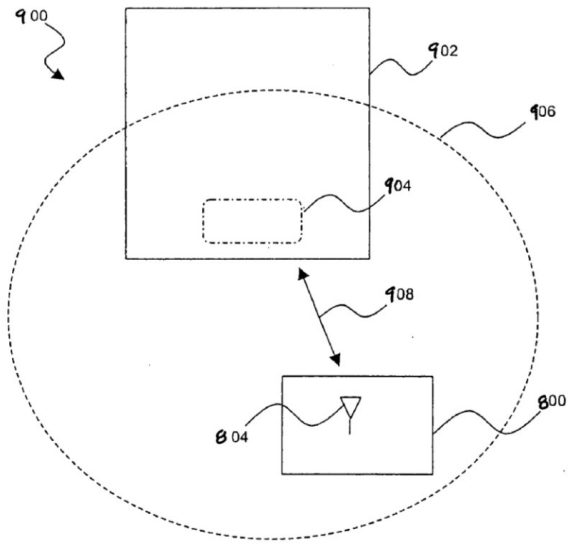
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media component 812, and a RF power conversion and power management unit 814. A number of inter-component communications paths 816 provide connections between various components of the device 800. Doughty '787 at [0057] The RF antenna 804 may perform multiple functions. For example, it may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The antenna 804 may be a single antenna capable of performing both functions or may comprise multiple antennae, with one antenna for capturing RF energy from the RF field and another antenna for supporting the two-way communication with the reader/writer device. The communications may include, for example, authenticated identification of a person operating the device 800, various purchases and financial transactions, air ticket booking and airport security check points, and other interactions between the device 800 and the reader/writer device. These communications may be secured using mechanisms such as data encryption. It is understood that other communications components, such as audio or optical components, may replace or supplement the antenna 804. In addition, the antenna 804 may be operable to function with wavelengths other than RF. Doughty '787 at [0059] The controller 806 interacts with the biometric sensor 802 and other components of the device 800 to perform various functions. For example, the controller 806 may capture the analog of the physical attribute for long term storage as a trusted template analog of an authorized user, as well as for immediate comparison to a stored trusted template analog during an authentication procedure. The controller 806 may also determine whether the comparison indicates a match between the template analog and the analog captured by the biometric sensor 802. In addition, the controller 806 may control the dynamic information display 810, respond to input from the control buttons 810, and control the magnetic information media component 812. Furthermore, the controller 806 may support two-way communications with an associated reader/writer device (FIG. 9) via the RF antenna 804. The controller may be a single controller/processor or may comprise multiple controllers/processors. Doughty '787 at [0061] Referring now to FIG. 9, the device is illustrated in an exemplary environment 900 that enables contactless interaction with a reader/writer device 902. To achieve this contactless interaction, the device 800 is shown with the antenna 804, as described in reference to FIG. 8. The device 902 uses one or more

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	antennae 903 to communicate with device 800, as well as emanate a RF field 906 with the purpose of supplying power to compatible devices, such as device 800. In operation, a two-way communication link 908 may be established between the reader/writer device 902 and the device 800. Doughty '787 at [0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the device 1100 includes several components, such as a fingerprint sensor 1102, a RF antenna 1104, a first controller 1106, a second controller 1108, function selector buttons 1110, an electro-luminescent display 1112 and a magnetic strip 1114. In the present example, the first controller 1106 is an application specific integrated circuit ("ASIC") chip and the second controller is a smart card chip, although it is understood that the functionality of both controllers may be provided by a single controller. Doughty '787 at [0077] Referring again to FIG. 11, the RF antenna 1104, which may include one or more antennae, may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The RF energy which is captured is converted to electrical energy and accumulated within the device 1100. In some embodiments of the device 1100, a rechargeable battery may power the electronic components when no RF energy field is present. Such a battery may be charged via a RF energy field or alternative charging means Doughty '787 at claim 1 a magnetic field generator disposed within the substrate that is normally inactive; Doughty '787 at claim 1 a processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified; and Doughty '787 at claim 2 2. The apparatus as recited in claim 1, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at claim 4 a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a spatially varying or time-varying magnetic signal via the one or more induction coils and the magnetic stripe. Doughty '787 at claim 18 18. The apparatus as recited in claim 1, further comprising a smart card interface mounted on the substrate that is communicably coupled to the processor and electrically connected to the power source. Doughty '787 at claim 26 26. The apparatus as recited in claim 1, wherein the processor and the memory are integrated into a single integrated circuit. Doughty '787 at claim 31 31. A method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor, the method comprising the steps of: receiving authentication data from the biometric sensor; determining whether the authentication data is valid for one of the users; and activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid. Doughty '787 at claim 38 38. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 42 42. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 53 53. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at claim 57 57. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 60 60. A system comprising: one or more user devices, each user device comprising a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate, a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified, and a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor; one or more system interfaces operable to communicate with the user device; and a system processor communicably coupled to the one or more system interfaces. Doughty '787 at claim 64 64. The system as recited in claim 60, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty '787 at claim 69 69. The system as recited in claim 60, wherein the device processor comprises a smart card processor and an ASIC chip. Doughty '787 at claim 88 88. The system as recited in claim 60, wherein the device processor and the memory are integrated into a single integrated circuit. *See also* 1[c] and claim 5 above.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	Doughty '787 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: *See* above at [1d]. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Doughty '787 at Figure 8  Fig. 8 Doughty '787 at Figure 9

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 Fig. 9 Doughty '787 at [0002] The present invention relates generally to the field of electronic devices and equipment used in the authentication and processing of commercial and security related transactions and, more particularly, to a system, method and apparatus for enabling transactions using biometrically enabled programmable magnetic stripes Doughty '787 at [0008] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty '787 at [0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention; Doughty '787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty '787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty '787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty '787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If,

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out. Doughty '787 at [0061] Referring now to FIG. 9, the device is illustrated in an exemplary environment 900 that enables contactless interaction with a reader/writer device 902. To achieve this contactless interaction, the device 800 is shown with the antenna 804, as described in reference to FIG. 8. The device 902 uses one or more antennae 903 to communicate with device 800, as well as emanate a RF field 906 with the purpose of supplying power to compatible devices, such as device 800. In operation, a two-way communication link 908 may be established between the reader/writer device 902 and the device 800. Doughty '787 at [0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an "electronic purse" functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty '787 at [0079] A dynamic magnetic strip 1114 is provided to provide compatibility with existing reader devices. The dynamic magnetic strip 1114 may be used in either fixed or dynamic mode. In dynamic mode,

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	magnetically stored information—such as a credit card number—may be changed under control of the ASIC 1106. Doughty '787 at [0095] Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment includes making retail purchases in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions. Doughty '787 at [0096] Payments for retail purchases are generally accomplished in one of three ways: with cash; with a check; or with a credit or debit card. In a cash transaction, there is generally no need for validating the identification of the buyer. In a transaction where a check is used, there generally is a need for identification of the buyer. This identification may occur by way of the buyer's presentation of a driver's license or alternate, approved identification card, presentation of a credit card to indicate credit-worthiness, or by a telecommunication connection to check security processing service to assure fund availability for, and legitimacy of, the check presented for payment. Doughty '787 at [0097] In a transaction where a credit or debit card is used, there are generally various procedural mechanisms in place to assure buyer identification and legitimate ownership of the card presented for the payment transaction. For example, the payment may require the entry of numeric PIN ("Personal Identification Number") security code by the buyer and assumed owner of the card. Alternatively, sales personnel may compare the buyer's signature on the back of the card presented for payment versus the requested signature on the purchase receipt provided for the goods or services purchased. In some cases, cards have a photograph of the card owner on them, and sales personnel may make cursory comparisons of this photograph with the buyer to establish identification. However, both photographic comparison and PIN-based card authorization have weaknesses for assuring identification, and both have potential risk for fraudulent processing. Photographs can be falsified and PIN numbers can be stolen. In the case of on-line purchases, buyers are not present to provide authorizing signatures, photographic comparisons cannot be made with existing processing infrastructure, and PIN-based transactions can be compromised with identity theft.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at claim 32 32. The method as recited in claim 31, wherein the information associated with the authenticated user enables approval of the transaction. Doughty '787 at claim 36 36. The method as recited in claim 31, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. Doughty '787 at claim 51 51. The computer program as recited in claim 46, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. Doughty '787 at claim 69 69. The system as recited in claim 60, wherein the device processor comprises a smart card processor and an ASIC chip. Doughty '787 at claim 84 84. The system as recited in claim 60, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card. *See also* claim 8 above. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example: *See* above at claim 3. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	See also claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Doughty '787 discloses or renders obvious "[t]he mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: *See* above at claim 2. To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

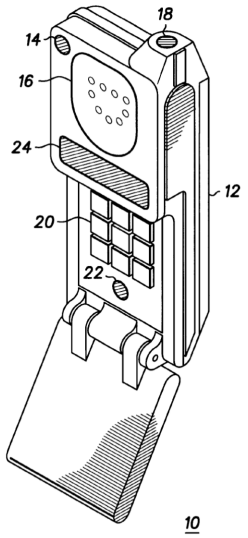
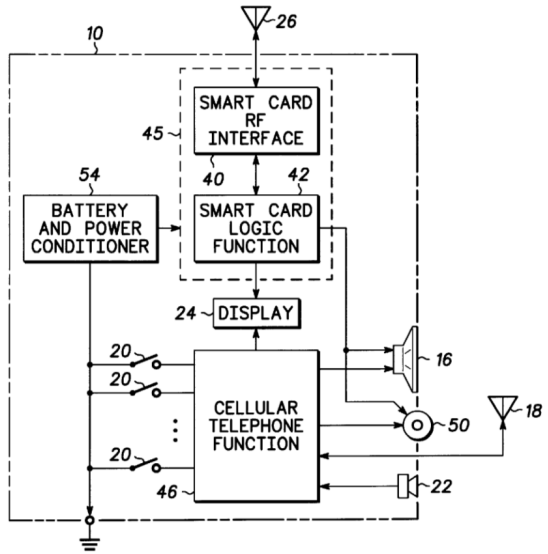
DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,202,156

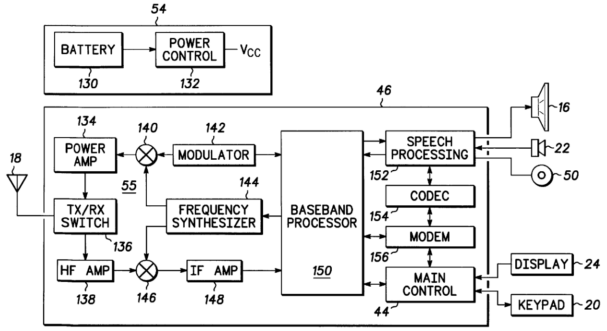
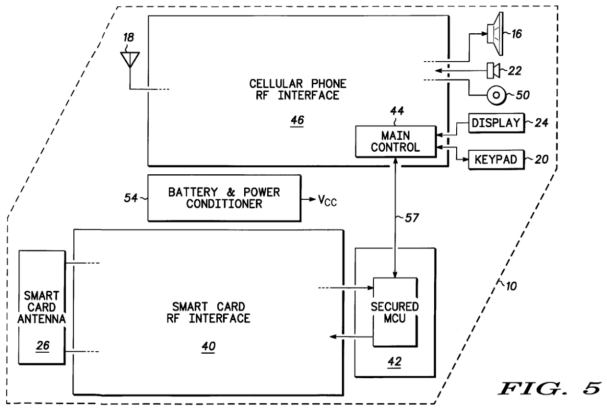
EXHIBIT E5: US5943624A ("Fox '624")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Fox '624 and (b) under 35 U.S.C. § 103(a) as obvious over Fox '624 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to US5943624A ("Fox '624")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Fox '624 discloses or renders obvious "[a] mobile device." For example: Fox '624 at Fig. 1

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	 *FIG. 1* Fox '624 at Fig. 2  *FIG. 2*

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at Fig. 4  FIG. 4 Fox '624 at Fig. 5  FIG. 5 Fox '624 at 1:9–30 Smartcards are fast becoming the common media to transfer information of many types relative to banking, transportation, subscriber, health, identification, etc. Typically, smartcards are housed within a plastic card, taking the form and size, for example, of a plastic credit card. Such smartcards include a microcomputer having some form of memory for storing and processing data. When a transaction within the capability of the smartcard is to be performed, the smartcard interacts with an external system which may be, for example, an automated teller machine, a merchant's point of sale system, etc. In performing such a transaction, typically the smartcard is inserted into a card reader associated with the external system through which electrical contact is made between the card reader and the smartcard. However,

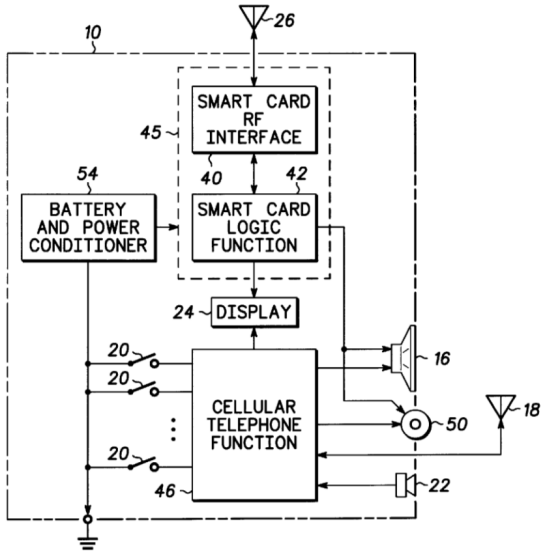
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	such systems requiring the smartcard to come into contact with the external system suffer from the disadvantages that the smartcard must be physically inserted into the external reader, the contacts between the smartcard and the external reader must be aligned for proper signal transfer, and the contacts may become worn or dirty thereby causing unreliability through signal degradation or signal interruption. Fox '624 at 2:1–2 FIG. 4 is a more detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 2.; and Fox '624 at 2:3–7 FIG. 5 is a detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 4 and the smartcard circuitry of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. Fox '624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 2:43–52 Referring to FIG. 2, a detailed block diagram illustrating the electronics associated with cellular telephone 10. As mentioned earlier, cellular telephone 10 includes the electronic circuitry for performing both a cellular telephone function and a contactless smartcard function whereby the human interface that selects the cellular telephone and the smartcard functions is accessed through the selector buttons 20 that are on the exterior of the cellular telephone housing case 12, as shown in FIG. 1 and represented electronically as switches in FIG. 2.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 2:64–3:2 Cellular telephone 10 also includes cellular telephone function circuitry 46 (or simply cellular telephone circuitry) for performing the necessary functions of operating a cellular telephone. Telephone circuitry 46 may take the form of any electronics for performing a cellular telephone function, whereby one embodiment is shown in detail in FIG. 4. Fox '624 at 3:3–9 Cellular telephone 10 also includes display 24 coupled to both smartcard logic function 42 and cellular telephone function circuitry 46 for displaying information to a user of cellular telephone 10. Display 24 may take the form of a liquid crystal display (LCD) or light emitting diode (LED) display that is typically incorporated into existing cellular telephones. Fox '624 at 3:10–22 ellular telephone 10 also includes speaker 16 and vibrator 50 coupled to both smartcard logic function circuitry 42 and cellular telephone function circuitry 46 for providing audible or tactile feedback to the user. For example, component 50 may be an audible speaker such as a vibrating cone commonly found in existing cellular phones for providing audible feedback. Alternately, component 50 may be a piezoelectric device for providing tactile feedback via vibration to the skin. Accordingly, the smartcard function may provide feedback to the user audibly or tactually to notify the user of RF interrogation by either an audible beep from the speaker or a vibration that originates within the case. Fox '624 at 3:23–26 RF interface 40, smartcard circuitry 42 and cellular telephone circuitry 46 may be fabricated on a single semiconductor integrated circuit 45 for achieving greater reliability and reducing overall cost. Fox '624 at 3:27–34 The present invention provides a cellular telephone that incorporates the electronic circuitry for implementing both a cellular telephone function and a smartcard function functions via smartcard circuitry 42 and cellular telephone circuitry 46, respectively. This allows the smartcard electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. Fox '624 at 4:43–56

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox '624 at 5:35–46 Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:2–3 1. A cellular telephone having the capability of performing smartcard functions, comprising: Fox '624 at 6:6–10 smartcard circuitry, including a smartcard controller, for performing smartcard functions, said smartcard controller being coupled to said main controller of said cellular telephone circuitry for communicating therewith;

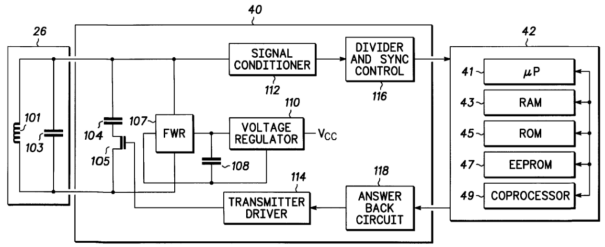
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account. Fox '624 at 6:31–35 2. The cellular telephone according to claim 1 further including a speaker, coupled to said smartcard circuitry and to said cellular telephone circuitry, for providing audible feedback to a user when performing said smartcard functions and said cellular telephone functions. Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox '624 at 6:49–51 6. The cellular telephone according to claim 1 wherein said smartcard circuitry and said RF interface are included within a housing of said cellular telephone circuitry. Fox '624 at 6:52–57 7. A method for incorporating a smartcard and its associated smartcard functions into a cellular telephone, the cellular telephone including a housing having a display incorporated therein for displaying information to a user and user accessible selector buttons for user command entry, the method comprising the steps of: Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox '624 at 7:1–6

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	ncorporating said integrated circuit into the housing of the cellular telephone so that said integrated circuit is coupled to the display and to the user accessible selector buttons to provide an interface between the user and both said smartcard circuitry and said cellular telephone circuitry; Fox '624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox '624 at 7:34 10. A cellular telephone comprising: Fox '624 at 7:36–41 cellular telephone circuitry for performing cellular telephone functions, said cellular telephone functions including establishing a communications connection between the cellular telephone and a remote communications entity via an external cellular communications system; Fox '624 at 8:1–9 smartcard circuitry, including a microprocessor unit (MPU), for performing smartcard functions, said smartcard functions including establishing a communications connection between the cellular telephone and an external smartcard reader via a direct radio frequency (RF) channel between the cellular telephone and the external smartcard reader, said MPU being coupled to said cellular telephone circuitry for communicating therewith; and Fox '624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. Fox '624 at 8:34–37 13. The cellular telephone of claim 10 wherein said smartcard circuitry, said RF interface, and said cellular telephone circuitry are fabricated on a single semiconductor chip as an integrated circuit.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 8:38–41 14. The cellular telephone of claim 10 wherein said cellular telephone circuitry, said smartcard circuitry, and said RF interface are included within a housing of the cellular telephone. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Fox '624 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Fox '624 at Fig. 2  FIG. 2 Fox '624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry

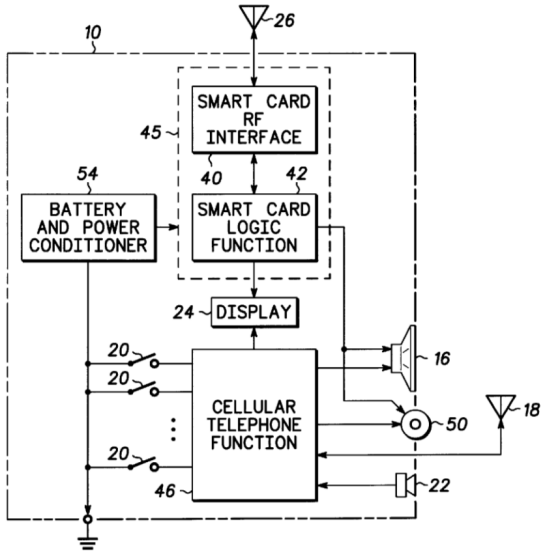
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 2:53–59 Cellular telephone 10 of FIG. 2 includes smartcard radio-frequency (RF) interface 40 coupled to antenna 26 for transmission and reception of RF data. The transmission/reception of RF data is utilized for performing and executing various smartcard functions while not suffering from the problems described earlier with respect to smartcard contact interfaces. Fox '624 at 4:9–13 Cellular telephone circuitry 46 includes RF interface comprising a transmit/receive switch 136 to direct energy in RF interface 55 for receipt of calls via the antenna 18, or to direct energy out of RF interface 55 when transmitting from the phone. Fox '624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a

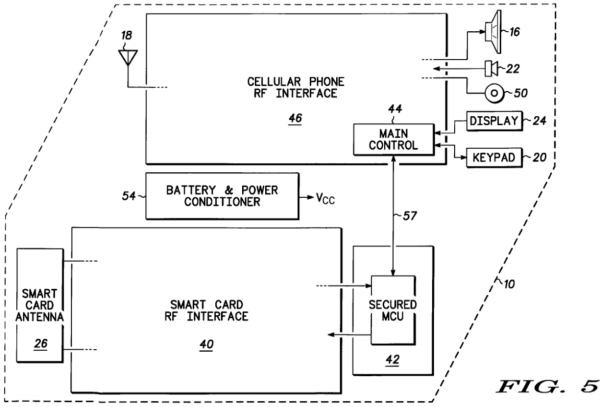
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:11–13 an RF interface, coupled to said smartcard circuitry, for transmitting and receiving information associated with said smartcard functions; and Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a memory to hold transaction data; and	Fox '624 discloses or renders obvious "a memory to hold transaction data." For example: Fox '624 at Fig. 3

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	 45 FIG. 3 Fox ’624 at 1:5–8 This invention relates to smartcard electronic devices and, more particularly, to the incorporation of smartcard devices in a cellular telephone for enhanced verification, security and accessibility to data stored on the smartcard. Fox ’624 at 1:9–30 Smartcards are fast becoming the common media to transfer information of many types relative to banking, transportation, subscriber, health, identification, etc. Typically, smartcards are housed within a plastic card, taking the form and size, for example, of a plastic credit card. Such smartcards include a microcomputer having some form of memory for storing and processing data. When a transaction within the capability of the smartcard is to be performed, the smartcard interacts with an external system which may be, for example, an automated teller machine, a merchant's point of sale system, etc. In performing such a transaction, typically the smartcard is inserted into a card reader associated with the external system through which electrical contact is made between the card reader and the smartcard. However, such systems requiring the smartcard to come into contact with the external system suffer from the disadvantages that the smartcard must be physically inserted into the external reader, the contacts between the smartcard and the external reader must be aligned for proper signal transfer, and the contacts may become worn or dirty thereby causing unreliability through signal degradation or signal interruption. Fox ’624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM)45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox '624 at 4:43–56 Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox '624 at 5:27–34 Smartcard data may also be accessed and displayed on display 24 through the use of selector buttons 20. For example, the balance of a smartcard may be displayed on display 24. Additionally, a menu system enabling the display of different data types, for example, medical information or multiple account balances or transaction lists, could also provided on display 24 and of which could be accessed via selector buttons 20. Fox '624 at 5:35–46

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account. Fox '624 at 7:1–6 ncorporating said integrated circuit into the housing of the cellular telephone so that said integrated circuit is coupled to the display and to the user accessible selector buttons to provide an interface between the user and both said smartcard circuitry and said cellular telephone circuitry; Fox '624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox '624 at 8:16–19

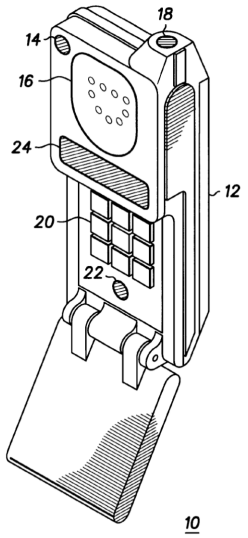
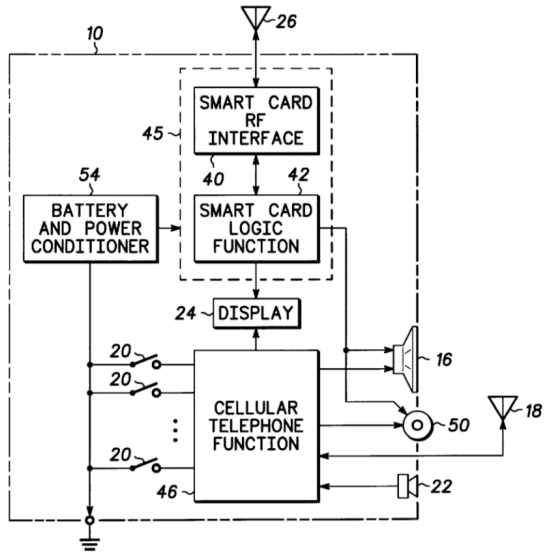
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	wherein said smartcard circuitry includes means for utilizing said cellular telephone circuitry to update information associated with said smartcard functions that is stored in said cellular telephone; Fox '624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Fox '624 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Fox '624 at Fig. 2  FIG. 2 Fox '624 at Fig. 5

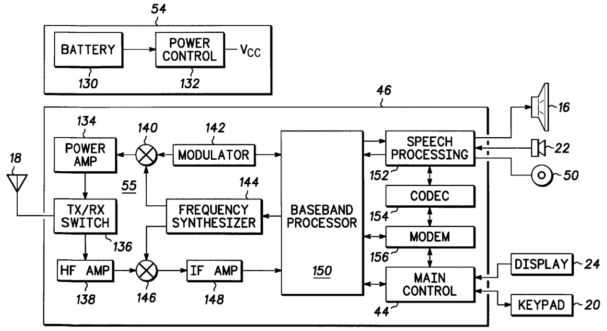
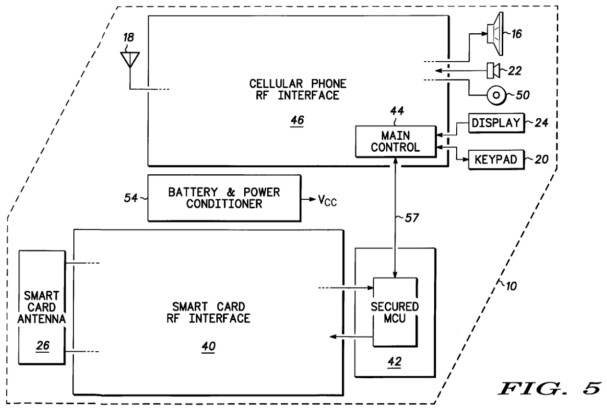
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	 FIG. 5 Fox '624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 2:53–59 Cellular telephone 10 of FIG. 2 includes smartcard radio-frequency (RF) interface 40 coupled to antenna 26 for transmission and reception of RF data. The transmission/reception of RF data is utilized for performing and executing various smartcard functions while not suffering from the problems described earlier with respect to smartcard contact interfaces. Fox '624 at 3:23–26 RF interface 40, smartcard circuitry 42 and cellular telephone circuitry 46 may be fabricated on a single semiconductor integrated circuit 45 for achieving greater reliability and reducing overall cost.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM)45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox '624 at 4:9–13 Cellular telephone circuitry 46 includes RF interface comprising a transmit/receive switch 136 to direct energy in RF interface 55 for receipt of calls via the antenna 18, or to direct energy out of RF interface 55 when transmitting from the phone. Fox '624 at 4:43–56 Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox '624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:4–5 cellular telephone circuitry, including a main controller, for performing cellular telephone functions; Fox '624 at 6:6–10 smartcard circuitry, including a smartcard controller, for performing smartcard functions, said smartcard controller being coupled to said main controller of said cellular telephone circuitry for communicating therewith; Fox '624 at 6:11–13 an RF interface, coupled to said smartcard circuitry, for transmitting and receiving information associated with said smartcard functions; and Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 6:45–48 5. The cellular telephone according to claim 1 wherein said smartcard circuitry, said cellular telephone circuitry and said RF interface are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox '624 at 8:1–9 smartcard circuitry, including a microprocessor unit (MPU), for performing smartcard functions, said smartcard functions including establishing a communications connection between the cellular telephone and an external smartcard reader via a direct radio frequency (RF) channel between the cellular telephone and the external smartcard reader, said MPU being coupled to said cellular telephone circuitry for communicating therewith; and To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	Fox '624 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: Fox '624 at Abstract A cellular telephone (10) incorporates the electronics for implementing both a cellular telephone function (46) and a smartcard function (45). This allows the electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone 10 also includes an RF interface (40) for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at Fig. 1

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	 *FIG. 1* Fox '624 at Fig. 2  *FIG. 2*

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at Fig. 4  FIG. 4 Fox '624 at Fig. 5  FIG. 5 Fox '624 at 1:5–8 This invention relates to smartcard electronic devices and, more particularly, to the incorporation of smartcard devices in a cellular telephone for enhanced verification, security and accessibility to data stored on the smartcard. Fox '624 at 1:60–61 FIG. 1 is a pictorial diagram illustrating a cellular telephone for incorporating a smartcard function therein;

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 1:62–64 FIG. 2 is a detailed block diagram illustrating the electronics for incorporating both a smartcard function and a cellular telephone function; Fox '624 at 2:1–2 FIG. 4 is a more detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 2.; and Fox '624 at 2:3–7 FIG. 5 is a detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 4 and the smartcard circuitry of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. Fox '624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 2:30–37 Cellular telephone 10 includes casing 12 for housing the electronics for implementing both a smartcard function and a cellular telephone function as will be described and shown in more detail with respect to FIG. 2. Cellular telephone 10 includes on-off switch 14, speaker 16 and cellular telephone antenna 18. Additionally, cellular telephone 10 includes selector buttons 20, voice input/microphone 22 and display 24.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 2:39–42 Housing 12 may take the form of any housing for a cellular phone, for example, the housing for Motorola cellular telephones such as the Microtac® phone or Startac® phone. Fox '624 at 2:43–52 Referring to FIG. 2, a detailed block diagram illustrating the electronics associated with cellular telephone 10. As mentioned earlier, cellular telephone 10 includes the electronic circuitry for performing both a cellular telephone function and a contactless smartcard function whereby the human interface that selects the cellular telephone and the smartcard functions is accessed through the selector buttons 20 that are on the exterior of the cellular telephone housing case 12, as shown in FIG. 1 and represented electronically as switches in FIG. 2. Fox '624 at 2:64–3:2 Cellular telephone 10 also includes cellular telephone function circuitry 46 (or simply cellular telephone circuitry) for performing the necessary functions of operating a cellular telephone. Telephone circuitry 46 may take the form of any electronics for performing a cellular telephone function, whereby one embodiment is shown in detail in FIG. 4. Fox '624 at 3:3–9 Cellular telephone 10 also includes display 24 coupled to both smartcard logic function 42 and cellular telephone function circuitry 46 for displaying information to a user of cellular telephone 10. Display 24 may take the form of a liquid crystal display (LCD) or light emitting diode (LED) display that is typically incorporated into existing cellular telephones. Fox '624 at 3:10–22 ellular telephone 10 also includes speaker 16 and vibrator 50 coupled to both smartcard logic function circuitry 42 and cellular telephone function circuitry 46 for providing audible or tactile feedback to the user. For example, component 50 may be an audible speaker such as a vibrating cone commonly found in existing cellular phones for providing audible feedback. Alternately, component 50 may be a piezoelectric device for providing tactile feedback via vibration to the skin. Accordingly, the smartcard function may provide feedback to the user audibly or tactually to notify the user of RF interrogation by either an audible beep from the speaker or a vibration that originates within the case. Fox '624 at 3:23–26

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	RF interface 40, smartcard circuitry 42 and cellular telephone circuitry 46 may be fabricated on a single semiconductor integrated circuit 45 for achieving greater reliability and reducing overall cost. Fox '624 at 3:27–34 The present invention provides a cellular telephone that incorporates the electronic circuitry for implementing both a cellular telephone function and a smartcard function functions via smartcard circuitry 42 and cellular telephone circuitry 46, respectively. This allows the smartcard electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. Fox '624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM)45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox '624 at 4:43–56 Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector

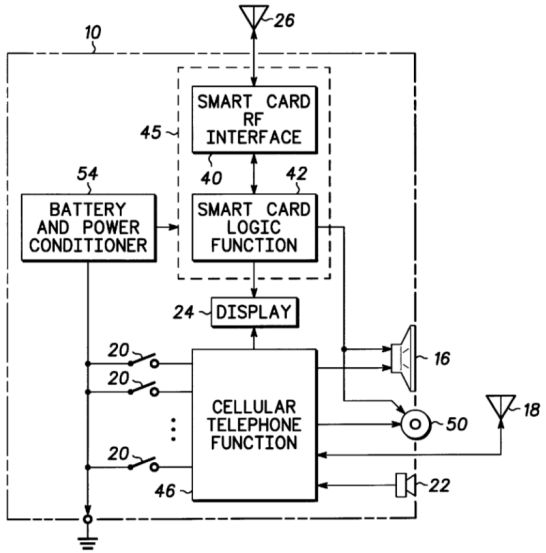
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 5:27–34 Smartcard data may also be accessed and displayed on display 24 through the use of selector buttons 20. For example, the balance of a smartcard may be displayed on display 24. Additionally, a menu system enabling the display of different data types, for example, medical information or multiple account balances or transaction lists, could also provided on display 24 and of which could be accessed via selector buttons 20. Fox '624 at 5:35–46 Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:2–3 1. A cellular telephone having the capability of performing smartcard functions, comprising: Fox '624 at 6:6–10

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	smartcard circuitry, including a smartcard controller, for performing smartcard functions, said smartcard controller being coupled to said main controller of said cellular telephone circuitry for communicating therewith; Fox '624 at 6:20–22 wherein said cellular telephone circuitry is utilized for updating information associated with said smartcard functions; and Fox '624 at 6:31–35 2. The cellular telephone according to claim 1 further including a speaker, coupled to said smartcard circuitry and to said cellular telephone circuitry, for providing audible feedback to a user when performing said smartcard functions and said cellular telephone functions. Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox '624 at 6:45–48 5. The cellular telephone according to claim 1 wherein said smartcard circuitry, said cellular telephone circuitry and said RF interface are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 6:49–51 6. The cellular telephone according to claim 1 wherein said smartcard circuitry and said RF interface are included within a housing of said cellular telephone circuitry. Fox '624 at 6:52–57 7. A method for incorporating a smartcard and its associated smartcard functions into a cellular telephone, the cellular telephone including a housing having a display incorporated therein for displaying information to a user and user accessible selector buttons for user command entry, the method comprising the steps of: Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox '624 at 7:1–6 ncorporating said integrated circuit into the housing of the cellular telephone so that said integrated circuit is coupled to the display and to the user accessible selector buttons to provide an interface between the user and both said smartcard circuitry and said cellular telephone circuitry; Fox '624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox '624 at 7:34 10. A cellular telephone comprising: Fox '624 at 7:36–41 cellular telephone circuitry for performing cellular telephone functions, said cellular telephone functions including establishing a communications connection between the cellular telephone and a remote communications entity via an external cellular communications system; Fox '624 at 8:1–9 smartcard circuitry, including a microprocessor unit (MPU), for performing smartcard functions, said smartcard functions including establishing a communications connection between the cellular telephone and an external smartcard reader via a direct radio frequency (RF) channel between the cellular telephone and the external smartcard reader, said MPU being coupled to said cellular telephone circuitry for communicating therewith; and Fox '624 at 8:16–19 wherein said smartcard circuitry includes means for utilizing said cellular telephone circuitry to update information associated with said smartcard functions that is stored in said cellular telephone; Fox '624 at 8:20–27

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. Fox '624 at 8:34–37 13. The cellular telephone of claim 10 wherein said smartcard circuitry, said RF interface, and said cellular telephone circuitry are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 8:38–41 14. The cellular telephone of claim 10 wherein said cellular telephone circuitry, said smartcard circuitry, and said RF interface are included within a housing of the cellular telephone. *See also* 1[pre] above. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Fox '624 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM).

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Fox '624 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Fox '624 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Fox '624 at Abstract A cellular telephone (10) incorporates the electronics for implementing both a cellular telephone function (46) and a smartcard function (45). This allows the electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone 10 also includes an RF interface (40) for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at Fig. 2  *FIG. 2* Fox '624 at Fig. 3

Claim Element	Exemplary Citations to US5943624A ("Fox '624")

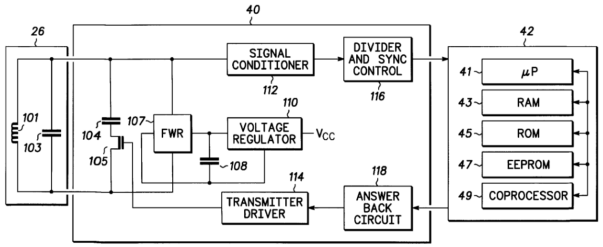


FIG. 3

Fox '624 at Fig. 5

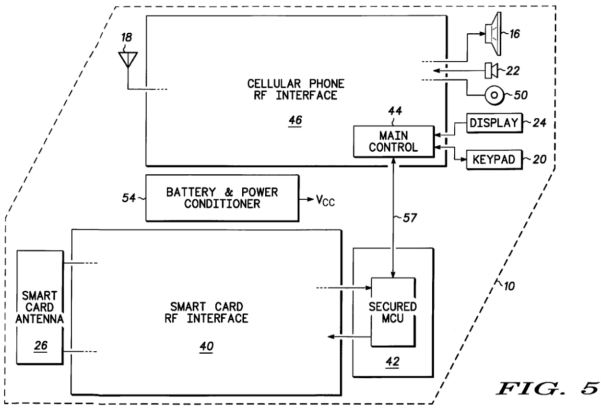


FIG. 5

Fox '624 at 1:5–8

> This invention relates to smartcard electronic devices and, more particularly, to the incorporation of smartcard devices in a cellular telephone for enhanced verification, security and accessibility to data stored on the smartcard.

Fox '624 at 1:9–30

> Smartcards are fast becoming the common media to transfer information of many types relative to banking, transportation, subscriber, health, identification, etc. Typically, smartcards are housed within a plastic card, taking the form and size, for example, of a plastic credit card. Such smartcards include a microcomputer having some form of memory for storing and processing data. When a transaction within the capability of the smartcard is to be performed, the smartcard interacts with an external system which may be, for example, an automated teller machine, a merchant's point of sale system, etc. In performing such a transaction, typically the smartcard is inserted into a card reader associated with the external

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	system through which electrical contact is made between the card reader and the smartcard. However, such systems requiring the smartcard to come into contact with the external system suffer from the disadvantages that the smartcard must be physically inserted into the external reader, the contacts between the smartcard and the external reader must be aligned for proper signal transfer, and the contacts may become worn or dirty thereby causing unreliability through signal degradation or signal interruption. Fox '624 at 1:60–61 FIG. 1 is a pictorial diagram illustrating a cellular telephone for incorporating a smartcard function therein; Fox '624 at 1:62–64 FIG. 2 is a detailed block diagram illustrating the electronics for incorporating both a smartcard function and a cellular telephone function; Fox '624 at 2:3–7 FIG. 5 is a detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 4 and the smartcard circuitry of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. Fox '624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 2:30–37

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Cellular telephone 10 includes casing 12 for housing the electronics for implementing both a smartcard function and a cellular telephone function as will be described and shown in more detail with respect to FIG. 2. Cellular telephone 10 includes on-off switch 14, speaker 16 and cellular telephone antenna 18. Additionally, cellular telephone 10 includes selector buttons 20, voice input/microphone 22 and display 24. Fox '624 at 2:43–52 Referring to FIG. 2, a detailed block diagram illustrating the electronics associated with cellular telephone 10. As mentioned earlier, cellular telephone 10 includes the electronic circuitry for performing both a cellular telephone function and a contactless smartcard function whereby the human interface that selects the cellular telephone and the smartcard functions is accessed through the selector buttons 20 that are on the exterior of the cellular telephone housing case 12, as shown in FIG. 1 and represented electronically as switches in FIG. 2. Fox '624 at 2:53–59 Cellular telephone 10 of FIG. 2 includes smartcard radio-frequency (RF) interface 40 coupled to antenna 26 for transmission and reception of RF data. The transmission/reception of RF data is utilized for performing and executing various smartcard functions while not suffering from the problems described earlier with respect to smartcard contact interfaces. Fox '624 at 3:3–9 Cellular telephone 10 also includes display 24 coupled to both smartcard logic function 42 and cellular telephone function circuitry 46 for displaying information to a user of cellular telephone 10. Display 24 may take the form of a liquid crystal display (LCD) or light emitting diode (LED) display that is typically incorporated into existing cellular telephones. Fox '624 at 3:10–22 ellular telephone 10 also includes speaker 16 and vibrator 50 coupled to both smartcard logic function circuitry 42 and cellular telephone function circuitry 46 for providing audible or tactile feedback to the user. For example, component 50 may be an audible speaker such as a vibrating cone commonly found in existing cellular phones for providing audible feedback. Alternately, component 50 may be a piezoelectric device for providing tactile feedback via vibration to the skin. Accordingly, the smartcard function may provide feedback to the user audibly or tactually to notify the user of RF interrogation by either an audible beep from the speaker or a vibration that originates within the case.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 3:23–26 RF interface 40, smartcard circuitry 42 and cellular telephone circuitry 46 may be fabricated on a single semiconductor integrated circuit 45 for achieving greater reliability and reducing overall cost. Fox '624 at 3:27–34 The present invention provides a cellular telephone that incorporates the electronic circuitry for implementing both a cellular telephone function and a smartcard function functions via smartcard circuitry 42 and cellular telephone circuitry 46, respectively. This allows the smartcard electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. Fox '624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM)45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox '624 at 3:49–59 Smartcard antenna 26 may take the form, for example, of capacitor 103 and a wire such as inductor 101. These two components form a tuned circuit that is resonant at the desired frequency of information and/or power transmission into the smartcard. The resonance is modified by the capacitor 104 and FET switch 105 under control of the logic function 42 via the answer back circuit 118 and transmitter driver 114, when information is transmitted out of the smartcard. The answer back circuit 118 receives the digital message from 42, formats and encodes it for RF transmission. Fox '624 at 4:43–56 Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox '624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 5:27–34 Smartcard data may also be accessed and displayed on display 24 through the use of selector buttons 20. For example, the balance of a smartcard may be displayed on display 24. Additionally, a menu system enabling the display of different data types, for example, medical information or multiple account balances or transaction lists, could also provided on display 24 and of which could be accessed via selector buttons 20. Fox '624 at 5:35–46 Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may

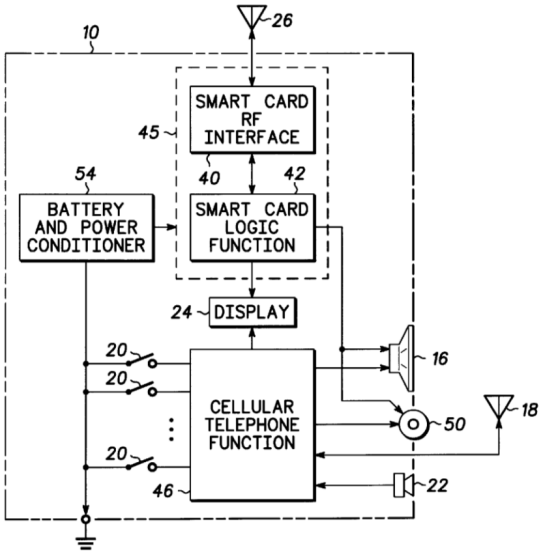
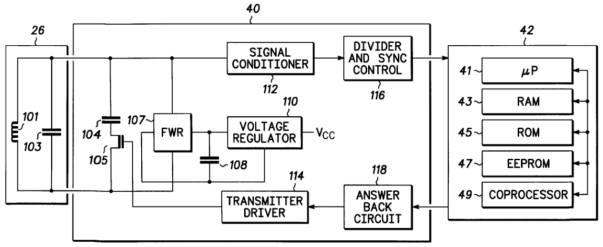
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:2–3 1. A cellular telephone having the capability of performing smartcard functions, comprising: Fox '624 at 6:4–5 cellular telephone circuitry, including a main controller, for performing cellular telephone functions; Fox '624 at 6:6–10 smartcard circuitry, including a smartcard controller, for performing smartcard functions, said smartcard controller being coupled to said main controller of said cellular telephone circuitry for communicating therewith; Fox '624 at 6:20–22 wherein said cellular telephone circuitry is utilized for updating information associated with said smartcard functions; and Fox '624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account.

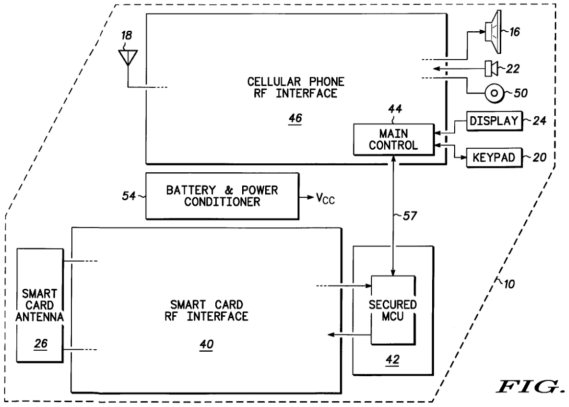
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 6:31–35 2. The cellular telephone according to claim 1 further including a speaker, coupled to said smartcard circuitry and to said cellular telephone circuitry, for providing audible feedback to a user when performing said smartcard functions and said cellular telephone functions. Fox '624 at 6:45–48 5. The cellular telephone according to claim 1 wherein said smartcard circuitry, said cellular telephone circuitry and said RF interface are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 6:52–57 7. A method for incorporating a smartcard and its associated smartcard functions into a cellular telephone, the cellular telephone including a housing having a display incorporated therein for displaying information to a user and user accessible selector buttons for user command entry, the method comprising the steps of: Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox '624 at 7:1–6 ncorporating said integrated circuit into the housing of the cellular telephone so that said integrated circuit is coupled to the display and to the user accessible selector buttons to provide an interface between the user and both said smartcard circuitry and said cellular telephone circuitry; Fox '624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox '624 at 8:1–9

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	smartcard circuitry, including a microprocessor unit (MPU), for performing smartcard functions, said smartcard functions including establishing a communications connection between the cellular telephone and an external smartcard reader via a direct radio frequency (RF) channel between the cellular telephone and the external smartcard reader, said MPU being coupled to said cellular telephone circuitry for communicating therewith; and Fox '624 at 8:16–19 wherein said smartcard circuitry includes means for utilizing said cellular telephone circuitry to update information associated with said smartcard functions that is stored in said cellular telephone; Fox '624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. Fox '624 at 8:34–37 13. The cellular telephone of claim 10 wherein said smartcard circuitry, said RF interface, and said cellular telephone circuitry are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 8:38–41 14. The cellular telephone of claim 10 wherein said cellular telephone circuitry, said smartcard circuitry, and said RF interface are included within a housing of the cellular telephone. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Fox '624 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Fox '624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Fox '624 discloses or renders obvious "[a] mobile device." For example:

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	See above at 1[pre]. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Fox '624 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a]. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Fox '624 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Fox '624 at Abstract A cellular telephone (10) incorporates the electronics for implementing both a cellular telephone function (46) and a smartcard function (45). This allows the electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone 10 also includes an RF interface (40) for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at Fig. 2

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	 FIG. 2 Fox '624 at Fig. 3  45 FIG. 3 Fox '624 at Fig. 5

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	 FIG. 5 Fox '624 at 1:5–8 This invention relates to smartcard electronic devices and, more particularly, to the incorporation of smartcard devices in a cellular telephone for enhanced verification, security and accessibility to data stored on the smartcard. Fox '624 at 1:9–30 Smartcards are fast becoming the common media to transfer information of many types relative to banking, transportation, subscriber, health, identification, etc. Typically, smartcards are housed within a plastic card, taking the form and size, for example, of a plastic credit card. Such smartcards include a microcomputer having some form of memory for storing and processing data. When a transaction within the capability of the smartcard is to be performed, the smartcard interacts with an external system which may be, for example, an automated teller machine, a merchant's point of sale system, etc. In performing such a transaction, typically the smartcard is inserted into a card reader associated with the external system through which electrical contact is made between the card reader and the smartcard. However, such systems requiring the smartcard to come into contact with the external system suffer from the disadvantages that the smartcard must be physically inserted into the external reader, the contacts between the smartcard and the external reader must be aligned for proper signal transfer, and the contacts may become worn or dirty thereby causing unreliability through signal degradation or signal interruption. Fox '624 at 1:60–61 FIG. 1 is a pictorial diagram illustrating a cellular telephone for incorporating a smartcard function therein;

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 1:62–64 FIG. 2 is a detailed block diagram illustrating the electronics for incorporating both a smartcard function and a cellular telephone function; Fox '624 at 2:3–7 FIG. 5 is a detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 4 and the smartcard circuitry of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. Fox '624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 2:30–37 Cellular telephone 10 includes casing 12 for housing the electronics for implementing both a smartcard function and a cellular telephone function as will be described and shown in more detail with respect to FIG. 2. Cellular telephone 10 includes on-off switch 14, speaker 16 and cellular telephone antenna 18. Additionally, cellular telephone 10 includes selector buttons 20, voice input/microphone 22 and display 24. Fox '624 at 2:43–52 Referring to FIG. 2, a detailed block diagram illustrating the electronics associated with cellular telephone 10. As mentioned earlier, cellular telephone 10 includes the electronic circuitry for performing both a cellular telephone function and a contactless smartcard function whereby the human interface that selects

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	the cellular telephone and the smartcard functions is accessed through the selector buttons 20 that are on the exterior of the cellular telephone housing case 12, as shown in FIG. 1 and represented electronically as switches in FIG. 2. Fox '624 at 2:53–59 Cellular telephone 10 of FIG. 2 includes smartcard radio-frequency (RF) interface 40 coupled to antenna 26 for transmission and reception of RF data. The transmission/reception of RF data is utilized for performing and executing various smartcard functions while not suffering from the problems described earlier with respect to smartcard contact interfaces. Fox '624 at 3:3–9 Cellular telephone 10 also includes display 24 coupled to both smartcard logic function 42 and cellular telephone function circuitry 46 for displaying information to a user of cellular telephone 10. Display 24 may take the form of a liquid crystal display (LCD) or light emitting diode (LED) display that is typically incorporated into existing cellular telephones. Fox '624 at 3:10–22 ellular telephone 10 also includes speaker 16 and vibrator 50 coupled to both smartcard logic function circuitry 42 and cellular telephone function circuitry 46 for providing audible or tactile feedback to the user. For example, component 50 may be an audible speaker such as a vibrating cone commonly found in existing cellular phones for providing audible feedback. Alternately, component 50 may be a piezoelectric device for providing tactile feedback via vibration to the skin. Accordingly, the smartcard function may provide feedback to the user audibly or tactually to notify the user of RF interrogation by either an audible beep from the speaker or a vibration that originates within the case. Fox '624 at 3:23–26 RF interface 40, smartcard circuitry 42 and cellular telephone circuitry 46 may be fabricated on a single semiconductor integrated circuit 45 for achieving greater reliability and reducing overall cost. Fox '624 at 3:27–34 The present invention provides a cellular telephone that incorporates the electronic circuitry for implementing both a cellular telephone function and a smartcard function functions via smartcard circuitry 42 and cellular telephone circuitry 46, respectively. This allows the smartcard electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM)45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox '624 at 3:49–59 Smartcard antenna 26 may take the form, for example, of capacitor 103 and a wire such as inductor 101. These two components form a tuned circuit that is resonant at the desired frequency of information and/or power transmission into the smartcard. The resonance is modified by the capacitor 104 and FET switch 105 under control of the logic function 42 via the answer back circuit 118 and transmitter driver 114, when information is transmitted out of the smartcard. The answer back circuit 118 receives the digital message from 42, formats and encodes it for RF transmission. Fox '624 at 4:43–56 Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox '624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 5:27–34 Smartcard data may also be accessed and displayed on display 24 through the use of selector buttons 20. For example, the balance of a smartcard may be displayed on display 24. Additionally, a menu system enabling the display of different data types, for example, medical information or multiple account balances or transaction lists, could also provided on display 24 and of which could be accessed via selector buttons 20. Fox '624 at 5:35–46 Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:2–3 1. A cellular telephone having the capability of performing smartcard functions, comprising: Fox '624 at 6:6–10 smartcard circuitry, including a smartcard controller, for performing smartcard functions, said smartcard controller being coupled to said main controller of said cellular telephone circuitry for communicating therewith; Fox '624 at 6:20–22 wherein said cellular telephone circuitry is utilized for updating information associated with said smartcard functions; and Fox '624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account. Fox '624 at 6:31–35 2. The cellular telephone according to claim 1 further including a speaker, coupled to said smartcard circuitry and to said cellular telephone circuitry, for providing audible feedback to a user when performing said smartcard functions and said cellular telephone functions. Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox '624 at 6:45–48 5. The cellular telephone according to claim 1 wherein said smartcard circuitry, said cellular telephone circuitry and said RF interface are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 6:52–57

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	7. A method for incorporating a smartcard and its associated smartcard functions into a cellular telephone, the cellular telephone including a housing having a display incorporated therein for displaying information to a user and user accessible selector buttons for user command entry, the method comprising the steps of: Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox '624 at 7:1–6 ncorporating said integrated circuit into the housing of the cellular telephone so that said integrated circuit is coupled to the display and to the user accessible selector buttons to provide an interface between the user and both said smartcard circuitry and said cellular telephone circuitry; Fox '624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox '624 at 8:1–9 smartcard circuitry, including a microprocessor unit (MPU), for performing smartcard functions, said smartcard functions including establishing a communications connection between the cellular telephone and an external smartcard reader via a direct radio frequency (RF) channel between the cellular telephone and the external smartcard reader, said MPU being coupled to said cellular telephone circuitry for communicating therewith; and Fox '624 at 8:16–19 wherein said smartcard circuitry includes means for utilizing said cellular telephone circuitry to update information associated with said smartcard functions that is stored in said cellular telephone; Fox '624 at 8:20–27

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. Fox '624 at 8:34–37 13. The cellular telephone of claim 10 wherein said smartcard circuitry, said RF interface, and said cellular telephone circuitry are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 8:38–41 14. The cellular telephone of claim 10 wherein said cellular telephone circuitry, said smartcard circuitry, and said RF interface are included within a housing of the cellular telephone. *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Fox '624 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Fox '624 at Fig. 2

Claim Element	Exemplary Citations to US5943624A ("Fox '624")

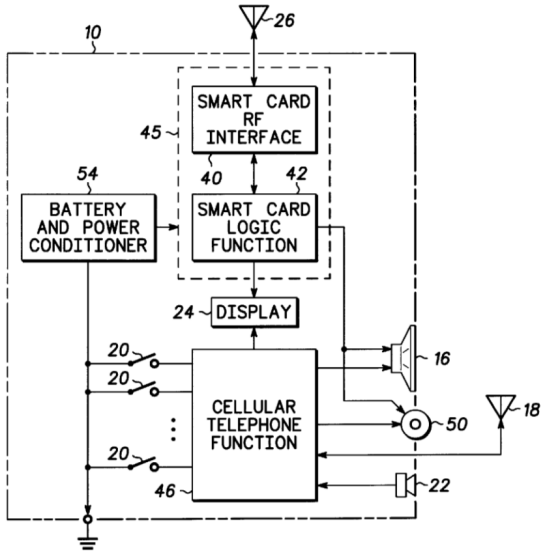


FIG. 2

Fox '624 at Fig. 5

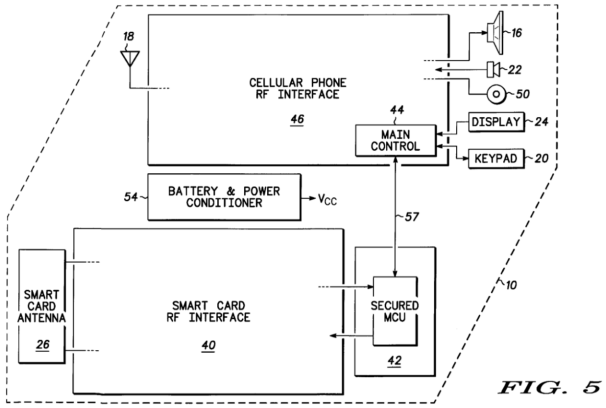


FIG. 5

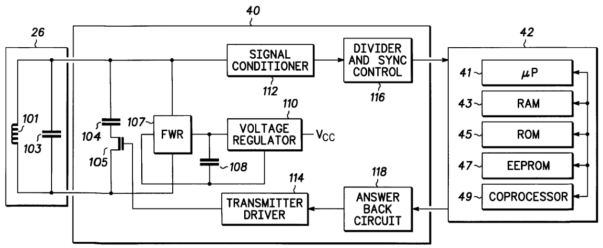
Fox '624 at 2:10–29

> Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox '624 at 2:53–59 Cellular telephone 10 of FIG. 2 includes smartcard radio-frequency (RF) interface 40 coupled to antenna 26 for transmission and reception of RF data. The transmission/reception of RF data is utilized for performing and executing various smartcard functions while not suffering from the problems described earlier with respect to smartcard contact interfaces. Fox '624 at 3:23–26 RF interface 40, smartcard circuitry 42 and cellular telephone circuitry 46 may be fabricated on a single semiconductor integrated circuit 45 for achieving greater reliability and reducing overall cost. Fox '624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM)45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox '624 at 4:9–13 Cellular telephone circuitry 46 includes RF interface comprising a transmit/receive switch 136 to direct energy in RF interface 55 for receipt of calls via the antenna 18, or to direct energy out of RF interface 55 when transmitting from the phone.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	Fox '624 at 4:43–56 Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox '624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at 6:4–5 cellular telephone circuitry, including a main controller, for performing cellular telephone functions; Fox '624 at 6:6–10 smartcard circuitry, including a smartcard controller, for performing smartcard functions, said smartcard controller being coupled to said main controller of said cellular telephone circuitry for communicating therewith; Fox '624 at 6:11–13 an RF interface, coupled to said smartcard circuitry, for transmitting and receiving information associated with said smartcard functions; and Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox '624 at 6:45–48 5. The cellular telephone according to claim 1 wherein said smartcard circuitry, said cellular telephone circuitry and said RF interface are fabricated on a single semiconductor chip as an integrated circuit. Fox '624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox '624 at 8:1–9 smartcard circuitry, including a microprocessor unit (MPU), for performing smartcard functions, said smartcard functions including establishing a communications connection between the cellular telephone and an external smartcard reader via a direct radio frequency (RF) channel between the cellular telephone

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	and the external smartcard reader, said MPU being coupled to said cellular telephone circuitry for communicating therewith; and *See also* 1[c] and claim 5 above. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	Fox '624 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: *See* above at [1d]. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Fox '624 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Fox '624 at Fig. 3  45 FIG. 3 Fox '624 at 1:9–30 Smartcards are fast becoming the common media to transfer information of many types relative to banking, transportation, subscriber, health, identification, etc. Typically, smartcards are housed within a plastic card, taking the form and size, for example, of a plastic credit card. Such smartcards include a microcomputer having some form of memory for storing and processing data. When a transaction within the capability of the smartcard is to be performed, the smartcard interacts with an external system which may be, for example, an automated teller machine, a merchant's point of sale system, etc. In performing such a transaction, typically the smartcard is inserted into a card reader associated with the external

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	system through which electrical contact is made between the card reader and the smartcard. However, such systems requiring the smartcard to come into contact with the external system suffer from the disadvantages that the smartcard must be physically inserted into the external reader, the contacts between the smartcard and the external reader must be aligned for proper signal transfer, and the contacts may become worn or dirty thereby causing unreliability through signal degradation or signal interruption. Fox '624 at 1:62–64 FIG. 2 is a detailed block diagram illustrating the electronics for incorporating both a smartcard function and a cellular telephone function; Fox '624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox '624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox '624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox '624 at 6:58–67

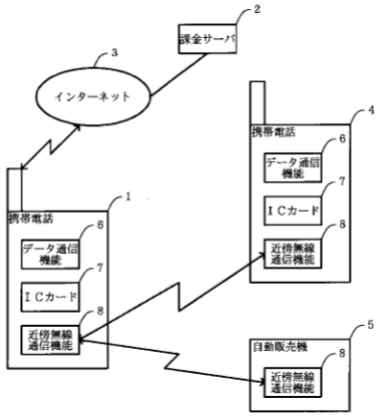
Claim Element	Exemplary Citations to US5943624A ("Fox '624")
	obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox '624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. *See also* claim 8 above. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Fox '624 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example: *See* above at claim 3. To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	To the extent this limitation is not disclosed by Fox '624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox '624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Haginiwa '847 and (b) under 35 U.S.C. § 103(a) as obvious over Haginiwa '847 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

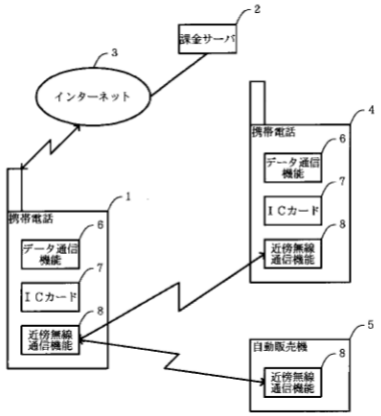
Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to JP2004240847A ("Haginiwa '847")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Haginiwa '847 discloses or renders obvious "[a] mobile device." For example: Haginiwa '847 at Abstract SOLUTION: An IC card is detachable for a personal digital assistant connectable to a radio network. This card is provided with a radio function for near communication to communicate with an apparatus existing at its periphery; a memory means to store information related to the radio function for near communication of the personal digital assistant; and a communication controlling means to determine whether to carry out communication by the radio function for near communication for the personal digital assistant, to accumulate communication volume of the radio for near communication, and to ask a server to collect money. Also, a charging method is provided in which the single IC card can carry out the accumulation of the communication volume and charging is carried out by the server by using the IC card. Haginiwa '847 at [0002] In recent years, research and development of a kind of IC card called UIM (User Identity Module), which stores various information and can be built into a mobile phone, an information home appliance, a PDA

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	(Personal Digital Assistant), or the like, has been developed. It is underway and is expected to spread in the future. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0020] A ninth aspect of the present invention is a charging method using an IC card that is detachable from a portable information terminal that has a data communication function and can be connected to a wireless network. Receiving a use identification number for identifying a use of communication by the wireless communication function; and searching a communication management area pre-stored in an IC card attached to the portable information terminal based on the received use identification number, and Judging whether or not to perform communication using the near field communication wireless function indicated by the number; and performing communication using the near field communication wireless function indicated by the application identification number. Adding the communication traffic of the communication to the communication traffic management area provided in the IC card, requesting the server to charge the communication traffic, and charging the communication traffic by the server. It is obtained to perform and performing. Haginiwa '847 at [0022] The billing system includes a mobile phone 1 and a billing server 2. In FIG. 1, a configuration including the Internet 3, a mobile phone 4, and a vending machine 5 will be further described. Haginiwa '847 at [0023] The mobile phone 1 includes a data communication function 6, an IC card 7, and a near field communication function 8, in order to function as a portable information terminal. Descriptions and

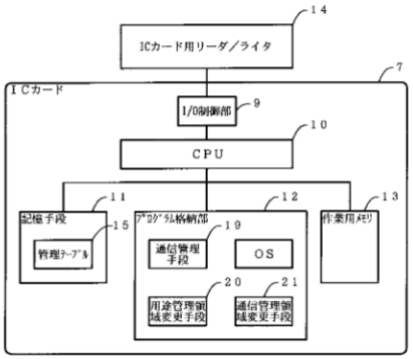
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	drawings of general mobile phone mechanisms and functions not related to the present invention are omitted. Haginiwa '847 at [0041] The charging server 2 is a computer system connected to the Internet 3 or the like and capable of communicating with the mobile phone 1. The charging server 2 receives the communication volume accumulated in the communication volume management area 16 from the mobile phone 1 and performs charging. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. Haginiwa '847 at Figure 1 【図１】  To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Haginiwa '847 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Haginiwa '847 at Abstract PROBLEM TO BE SOLVED: To provide an IC card and a charging method using an IC card in which, for near radiocommunication, whether or not receiving is possible and charging are controlled by exchanging use identification numbers for near radiocommunication. Haginiwa '847 at Abstract SOLUTION: An IC card is detachable for a personal digital assistant connectable to a radio network. This card is provided with a radio function for near communication to communicate with an apparatus existing at its periphery; a memory means to store information related to the radio function for near communication of the personal digital assistant; and a communication controlling means to determine whether to carry out communication by the radio function for near communication for the personal digital assistant, to accumulate communication volume of the radio for near communication, and to ask a server to collect money. Also, a charging method is provided in which the single IC card can carry out the accumulation of the communication volume and charging is carried out by the server by using the IC card. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0014] According to a third aspect of the present invention, there is provided the IC card according to the first or second aspect, wherein the storage means stores a communication use of the near field communication wireless function and an identification number of the communication use. An area is provided.

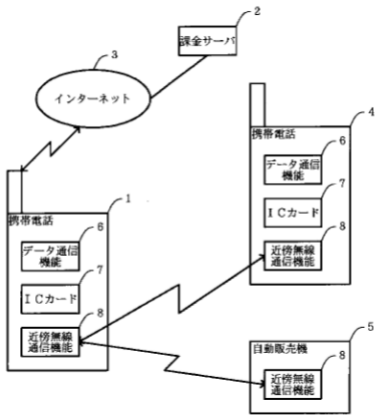
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. Haginiwa '847 at Figure 1 【図１】 

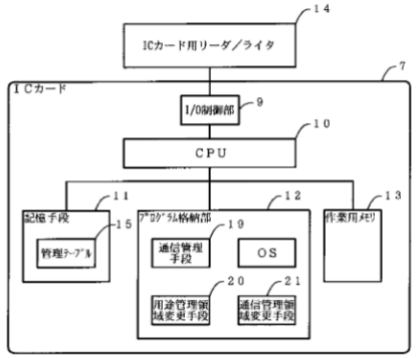
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a memory to hold transaction data; and	Haginiwa '847 discloses or renders obvious "a memory to hold transaction data." For example: Haginiwa '847 at Abstract SOLUTION: An IC card is detachable for a personal digital assistant connectable to a radio network. This card is provided with a radio function for near communication to communicate with an apparatus existing at its periphery; a memory means to store information related to the radio function for near communication of the personal digital assistant; and a communication controlling means to determine whether to carry out communication by the radio function for near communication for the personal digital assistant, to accumulate communication volume of the radio for near communication, and to ask a server to collect money. Also, a charging method is provided in which the single IC card can carry out the accumulation of the communication volume and charging is carried out by the server by using the IC card. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0013]–[0014] According to a second aspect of the present invention, in the IC card according to the first aspect, the storage means stores a communication amount management area for storing a communication amount by the near field communication wireless function with which the portable information terminal has communicated. A communication management area for storing communication enable / disable information as to whether or not to perform communication using the near field communication wireless

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	function for each use identification number for identifying the use of the near field communication wireless function. Haginiwa '847 at [0014] According to a third aspect of the present invention, there is provided the IC card according to the first or second aspect, wherein the storage means stores a communication use of the near field communication wireless function and an identification number of the communication use. An area is provided. Haginiwa '847 at [0026] FIG. 2 is a schematic configuration diagram of the inside of the IC card 7. The IC card 7 includes an I / O control unit 9, a CPU 10, a storage unit 11, a program storage unit 12, and a work memory 13. Haginiwa '847 at [0028] The CPU 10 executes various applications recorded in the program storage unit 12. When executing the application, the storage unit 11 and the working memory 13 are used as needed. Haginiwa '847 at [0029] The storage unit 11 is an electrically erasable programmable read-only memory (EEPROM) that is actually a nonvolatile memory, and is used to store and hold various data. Haginiwa '847 at [0030] The storage unit 11 includes, as a part thereof, an area for storing a management table 15 used by a function provided by the IC card 7. Haginiwa '847 at [0036] The program storage unit 12 stores applications such as the communication management unit 19, the use management area changing unit 20, and the communication management area changing unit 21 in addition to the OS. Only Memory) or an EEPROM in which an application can be loaded and used. Haginiwa '847 at [0038] When the storage unit 11 includes the use management area 17, the use management area change unit 20 stores a communication use name, a use identification number, and the like, which are stored in the use management area 17 in response to a user input of the mobile phone 1. Add, change, or delete content. Haginiwa '847 at [0073]

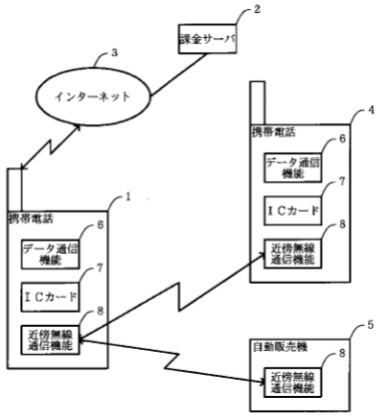
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	In addition, since the communication amount, the use identification number, and the availability of the near field communication are stored in the IC card mounted on the portable information terminal, the near field communication can be performed even when not connected to the mobile communication network or the billing server. It is possible to judge whether or not to perform communication according to, and to accumulate the communication amount. Haginiwa '847 at Figure 2 【図２】  To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Haginiwa '847 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Haginiwa '847 at Abstract PROBLEM TO BE SOLVED: To provide an IC card and a charging method using an IC card in which, for near radiocommunication, whether or not receiving is possible and charging are controlled by exchanging use identification numbers for near radiocommunication. Haginiwa '847 at Abstract SOLUTION: An IC card is detachable for a personal digital assistant connectable to a radio network. This card is provided with a radio function for near communication to communicate with an apparatus existing at its periphery; a memory means to store information related to the radio function for near communication of the personal digital assistant; and a communication controlling means to determine

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	whether to carry out communication by the radio function for near communication for the personal digital assistant, to accumulate communication volume of the radio for near communication, and to ask a server to collect money. Also, a charging method is provided in which the single IC card can carry out the accumulation of the communication volume and charging is carried out by the server by using the IC card. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0014] According to a third aspect of the present invention, there is provided the IC card according to the first or second aspect, wherein the storage means stores a communication use of the near field communication wireless function and an identification number of the communication use. An area is provided. Haginiwa '847 at [0026] FIG. 2 is a schematic configuration diagram of the inside of the IC card 7. The IC card 7 includes an I / O control unit 9, a CPU 10, a storage unit 11, a program storage unit 12, and a work memory 13. Haginiwa '847 at [0028] The CPU 10 executes various applications recorded in the program storage unit 12. When executing the application, the storage unit 11 and the working memory 13 are used as needed. Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. Haginiwa '847 at Figure 1 【図１】  Haginiwa '847 at Figure 2

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図２】  To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	Haginiwa '847 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: Haginiwa '847 at [0002] In recent years, research and development of a kind of IC card called UIM (User Identity Module), which stores various information and can be built into a mobile phone, an information home appliance, a PDA (Personal Digital Assistant), or the like, has been developed. It is underway and is expected to spread in the future. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at [0020] A ninth aspect of the present invention is a charging method using an IC card that is detachable from a portable information terminal that has a data communication function and can be connected to a wireless network. Receiving a use identification number for identifying a use of communication by the wireless communication function; and searching a communication management area pre-stored in an IC card attached to the portable information terminal based on the received use identification number, and Judging whether or not to perform communication using the near field communication wireless function indicated by the number; and performing communication using the near field communication wireless function indicated by the application identification number. Adding the communication traffic of the communication to the communication traffic management area provided in the IC card, requesting the server to charge the communication traffic, and charging the communication traffic by the server. It is obtained to perform and performing. Haginiwa '847 at [0022] The billing system includes a mobile phone 1 and a billing server 2. In FIG. 1, a configuration including the Internet 3, a mobile phone 4, and a vending machine 5 will be further described. Haginiwa '847 at [0023] The mobile phone 1 includes a data communication function 6, an IC card 7, and a near field communication function 8, in order to function as a portable information terminal. Descriptions and drawings of general mobile phone mechanisms and functions not related to the present invention are omitted. Haginiwa '847 at [0041] The charging server 2 is a computer system connected to the Internet 3 or the like and capable of communicating with the mobile phone 1. The charging server 2 receives the communication volume accumulated in the communication volume management area 16 from the mobile phone 1 and performs charging. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0050] When the power switch of the mobile phone 1 is turned on, the IC card 7 receives power supply from the mobile phone 1, activates the OS unit, and waits for a command to be received. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. Haginiwa '847 at Figure 1 【図１】  To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example:

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
field mimics a swipe of a magnetic credit card.	Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. *See also* 1[pre] above.

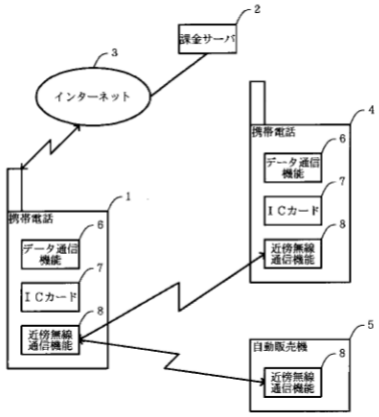
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.

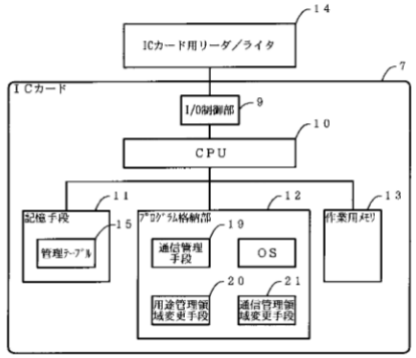
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Haginiwa '847 at Abstract PROBLEM TO BE SOLVED: To provide an IC card and a charging method using an IC card in which, for near radiocommunication, whether or not receiving is possible and charging are controlled by exchanging use identification numbers for near radiocommunication.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at Abstract SOLUTION: An IC card is detachable for a personal digital assistant connectable to a radio network. This card is provided with a radio function for near communication to communicate with an apparatus existing at its periphery; a memory means to store information related to the radio function for near communication of the personal digital assistant; and a communication controlling means to determine whether to carry out communication by the radio function for near communication for the personal digital assistant, to accumulate communication volume of the radio for near communication, and to ask a server to collect money. Also, a charging method is provided in which the single IC card can carry out the accumulation of the communication volume and charging is carried out by the server by using the IC card. Haginiwa '847 at [0001] The present invention relates to an IC card, and more particularly to an application for performing a billing process using an IC card. Haginiwa '847 at [0011] SUMMARY OF THE INVENTION The present invention has been made in view of the above-described problems, and uses an IC card and an IC card for controlling reception availability and charging by exchanging a use identification number of the proximity wireless communication in the proximity wireless communication. The purpose is to provide a billing method. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0013]–[0014]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	According to a second aspect of the present invention, in the IC card according to the first aspect, the storage means stores a communication amount management area for storing a communication amount by the near field communication wireless function with which the portable information terminal has communicated. A communication management area for storing communication enable / disable information as to whether or not to perform communication using the near field communication wireless function for each use identification number for identifying the use of the near field communication wireless function. Haginiwa '847 at [0014] According to a third aspect of the present invention, there is provided the IC card according to the first or second aspect, wherein the storage means stores a communication use of the near field communication wireless function and an identification number of the communication use. An area is provided. Haginiwa '847 at [0020] A ninth aspect of the present invention is a charging method using an IC card that is detachable from a portable information terminal that has a data communication function and can be connected to a wireless network. Receiving a use identification number for identifying a use of communication by the wireless communication function; and searching a communication management area pre-stored in an IC card attached to the portable information terminal based on the received use identification number, and Judging whether or not to perform communication using the near field communication wireless function indicated by the number; and performing communication using the near field communication wireless function indicated by the application identification number. Adding the communication traffic of the communication to the communication traffic management area provided in the IC card, requesting the server to charge the communication traffic, and charging the communication traffic by the server. It is obtained to perform and performing. Haginiwa '847 at [0025] The IC card 7 is actually a JavaCard (registered trademark) UIM in a plug-in shape and capable of mounting a plurality of applications. Haginiwa '847 at [0026] FIG. 2 is a schematic configuration diagram of the inside of the IC card 7. The IC card 7 includes an I / O control unit 9, a CPU 10, a storage unit 11, a program storage unit 12, and a work memory 13. Haginiwa '847 at [0028]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	The CPU 10 executes various applications recorded in the program storage unit 12. When executing the application, the storage unit 11 and the working memory 13 are used as needed. Haginiwa '847 at [0029] The storage unit 11 is an electrically erasable programmable read-only memory (EEPROM) that is actually a nonvolatile memory, and is used to store and hold various data. Haginiwa '847 at [0030] The storage unit 11 includes, as a part thereof, an area for storing a management table 15 used by a function provided by the IC card 7. Haginiwa '847 at [0036] The program storage unit 12 stores applications such as the communication management unit 19, the use management area changing unit 20, and the communication management area changing unit 21 in addition to the OS. Only Memory) or an EEPROM in which an application can be loaded and used. Haginiwa '847 at [0038] When the storage unit 11 includes the use management area 17, the use management area change unit 20 stores a communication use name, a use identification number, and the like, which are stored in the use management area 17 in response to a user input of the mobile phone 1. Add, change, or delete content. Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0050] When the power switch of the mobile phone 1 is turned on, the IC card 7 receives power supply from the mobile phone 1, activates the OS unit, and waits for a command to be received. Haginiwa '847 at [0073]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	In addition, since the communication amount, the use identification number, and the availability of the near field communication are stored in the IC card mounted on the portable information terminal, the near field communication can be performed even when not connected to the mobile communication network or the billing server. It is possible to judge whether or not to perform communication according to, and to accumulate the communication amount. Haginiwa '847 at [citation unavailable] FIG. 2 is a schematic configuration diagram of the inside of an IC card (UIM) of the present invention. Haginiwa '847 at claim 2 An IC card comprising: The IC card according to claim 1, Haginiwa '847 at Figure 1 【図１】  Haginiwa '847 at Figure 2

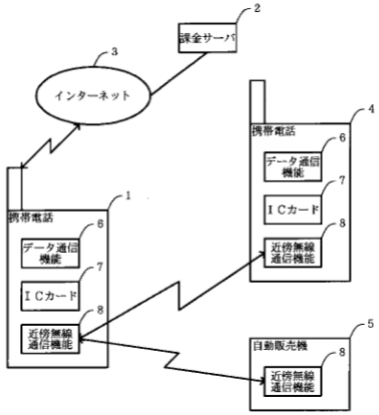
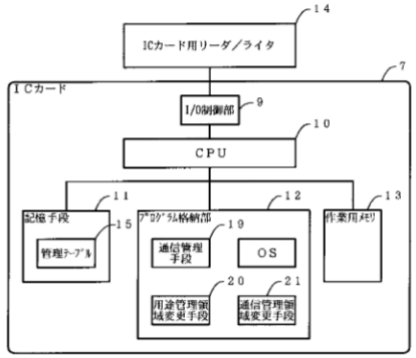
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図２】  To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Haginiwa '847 discloses or renders obvious "[a] mobile device." For example: *See* above at 1[pre]. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Haginiwa '847 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a]. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Haginiwa '847 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Haginiwa '847 at Abstract PROBLEM TO BE SOLVED: To provide an IC card and a charging method using an IC card in which, for near radiocommunication, whether or not receiving is possible and charging are controlled by exchanging use identification numbers for near radiocommunication. Haginiwa '847 at Abstract SOLUTION: An IC card is detachable for a personal digital assistant connectable to a radio network. This card is provided with a radio function for near communication to communicate with an apparatus existing

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	at its periphery; a memory means to store information related to the radio function for near communication of the personal digital assistant; and a communication controlling means to determine whether to carry out communication by the radio function for near communication for the personal digital assistant, to accumulate communication volume of the radio for near communication, and to ask a server to collect money. Also, a charging method is provided in which the single IC card can carry out the accumulation of the communication volume and charging is carried out by the server by using the IC card. Haginiwa '847 at [0001] The present invention relates to an IC card, and more particularly to an application for performing a billing process using an IC card. Haginiwa '847 at [0011] SUMMARY OF THE INVENTION The present invention has been made in view of the above-described problems, and uses an IC card and an IC card for controlling reception availability and charging by exchanging a use identification number of the proximity wireless communication in the proximity wireless communication. The purpose is to provide a billing method. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0013]–[0014] According to a second aspect of the present invention, in the IC card according to the first aspect, the storage means stores a communication amount management area for storing a communication amount by the near field communication wireless function with which the portable information terminal has communicated. A communication management area for storing communication enable / disable information as to whether or not to perform communication using the near field communication wireless

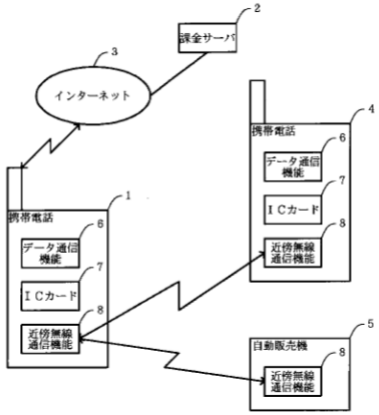
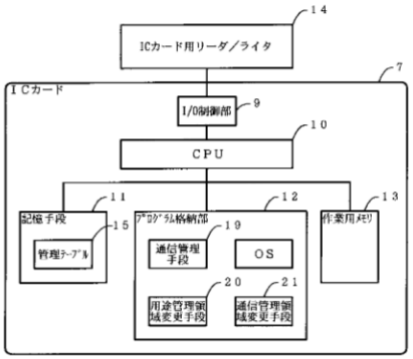
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	function for each use identification number for identifying the use of the near field communication wireless function. Haginiwa '847 at [0014] According to a third aspect of the present invention, there is provided the IC card according to the first or second aspect, wherein the storage means stores a communication use of the near field communication wireless function and an identification number of the communication use. An area is provided. Haginiwa '847 at [0020] A ninth aspect of the present invention is a charging method using an IC card that is detachable from a portable information terminal that has a data communication function and can be connected to a wireless network. Receiving a use identification number for identifying a use of communication by the wireless communication function; and searching a communication management area pre-stored in an IC card attached to the portable information terminal based on the received use identification number, and Judging whether or not to perform communication using the near field communication wireless function indicated by the number; and performing communication using the near field communication wireless function indicated by the application identification number. Adding the communication traffic of the communication to the communication traffic management area provided in the IC card, requesting the server to charge the communication traffic, and charging the communication traffic by the server. It is obtained to perform and performing. Haginiwa '847 at [0022] The billing system includes a mobile phone 1 and a billing server 2. In FIG. 1, a configuration including the Internet 3, a mobile phone 4, and a vending machine 5 will be further described. Haginiwa '847 at [0025] The IC card 7 is actually a JavaCard (registered trademark) UIM in a plug-in shape and capable of mounting a plurality of applications. Haginiwa '847 at [0026] FIG. 2 is a schematic configuration diagram of the inside of the IC card 7. The IC card 7 includes an I / O control unit 9, a CPU 10, a storage unit 11, a program storage unit 12, and a work memory 13. Haginiwa '847 at [0028]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	The CPU 10 executes various applications recorded in the program storage unit 12. When executing the application, the storage unit 11 and the working memory 13 are used as needed. Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0050] When the power switch of the mobile phone 1 is turned on, the IC card 7 receives power supply from the mobile phone 1, activates the OS unit, and waits for a command to be received. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. Haginiwa '847 at [citation unavailable] FIG. 1 is an overall configuration diagram of a billing system using a mobile phone in which an IC card according to the present invention is detachable. Haginiwa '847 at [citation unavailable] FIG. 2 is a schematic configuration diagram of the inside of an IC card (UIM) of the present invention. Haginiwa '847 at claim 2

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	An IC card comprising: The IC card according to claim 1, Haginiwa '847 at Figure 1 【図１】  Haginiwa '847 at Figure 2 【図２】  *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

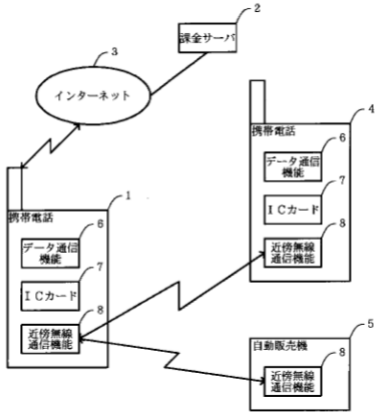
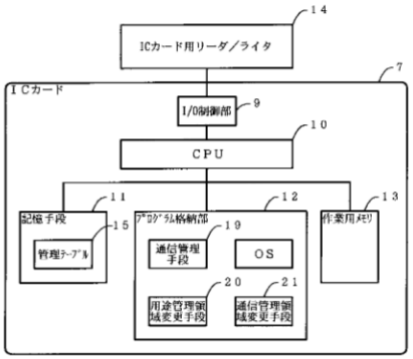
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Haginiwa '847 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Haginiwa '847 at Abstract PROBLEM TO BE SOLVED: To provide an IC card and a charging method using an IC card in which, for near radiocommunication, whether or not receiving is possible and charging are controlled by exchanging use identification numbers for near radiocommunication. Haginiwa '847 at Abstract SOLUTION: An IC card is detachable for a personal digital assistant connectable to a radio network. This card is provided with a radio function for near communication to communicate with an apparatus existing at its periphery; a memory means to store information related to the radio function for near communication of the personal digital assistant; and a communication controlling means to determine whether to carry out communication by the radio function for near communication for the personal digital assistant, to accumulate communication volume of the radio for near communication, and to ask a server to collect money. Also, a charging method is provided in which the single IC card can carry out the accumulation of the communication volume and charging is carried out by the server by using the IC card. Haginiwa '847 at [0012] [Means for Solving the Problems] In order to achieve the above object, a first aspect of the present invention is an IC card having a data communication function and detachable from a portable information terminal that can be connected to a wireless network, wherein the portable information terminal is located around the IC card. Wireless communication function for communicating with the portable information terminal, storage means for storing information related to the wireless communication function for the near field communication of the portable information terminal, and whether or not to perform communication using the wireless function for near field communication in the portable information terminal. And a communication management means for accumulating the communication amount of the short range communication wireless communication and requesting the server to charge the communication amount. Haginiwa '847 at [0014] According to a third aspect of the present invention, there is provided the IC card according to the first or second aspect, wherein the storage means stores a communication use of the near field communication wireless function and an identification number of the communication use. An area is provided.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at [0026] FIG. 2 is a schematic configuration diagram of the inside of the IC card 7. The IC card 7 includes an I / O control unit 9, a CPU 10, a storage unit 11, a program storage unit 12, and a work memory 13. Haginiwa '847 at [0028] The CPU 10 executes various applications recorded in the program storage unit 12. When executing the application, the storage unit 11 and the working memory 13 are used as needed. Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. Haginiwa '847 at Figure 1

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図１】  Haginiwa '847 at Figure 2 【図２】  *See also* 1[c] and claim 5 above. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	Haginiwa '847 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: *See* above at [1d].

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Haginiwa '847 at [0001] The present invention relates to an IC card, and more particularly to an application for performing a billing process using an IC card. Haginiwa '847 at [0011] SUMMARY OF THE INVENTION The present invention has been made in view of the above-described problems, and uses an IC card and an IC card for controlling reception availability and charging by exchanging a use identification number of the proximity wireless communication in the proximity wireless communication. The purpose is to provide a billing method. Haginiwa '847 at [0022] The billing system includes a mobile phone 1 and a billing server 2. In FIG. 1, a configuration including the Internet 3, a mobile phone 4, and a vending machine 5 will be further described. Haginiwa '847 at [0027] The I / O control unit 9 is an interface for the IC card 7 to communicate with the IC card reader / writer 14. Haginiwa '847 at [0037] The communication management unit 19 searches the communication management area 18 based on the application identification number received from the nearby wireless communication function 8 of the peripheral device (for example, the mobile phone 4 or the vending machine 5) and determines whether communication is possible. It is determined whether or not to perform near field communication indicated by the use identification number based on the information. If the near field communication has been performed, the total communication amount is stored, and the charging server 2 is requested to charge the communication amount. is there. Haginiwa '847 at [0040]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field communication function 8 such as the mobile phone 4 and the vending machine 5. It communicates with. Haginiwa '847 at [0044] The vending machine 5 is provided with a near field communication function 8, and is capable of performing data communication with a device having the near field communication function 8, such as the mobile phone 1 or the mobile phone 4, when selling a product. It is. Haginiwa '847 at [0047] Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 5 receives a product purchase instruction from the mobile phone 1 via near field communication and sells the product. At that time, the vending machine 5 transmits the use identification number of "9999" with the communication use of "other" to the mobile phone 1 by near field communication. Haginiwa '847 at [citation unavailable] FIG. 1 is an overall configuration diagram of a billing system using a mobile phone in which an IC card according to the present invention is detachable. Haginiwa '847 at Figure 1

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図１】  Haginiwa '847 at Figure 2 【図２】  *See also* claim 8 above. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example:

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	See above at claim 3. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Haginiwa '847 discloses or renders obvious "[t]he mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: *See* above at claim 2. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

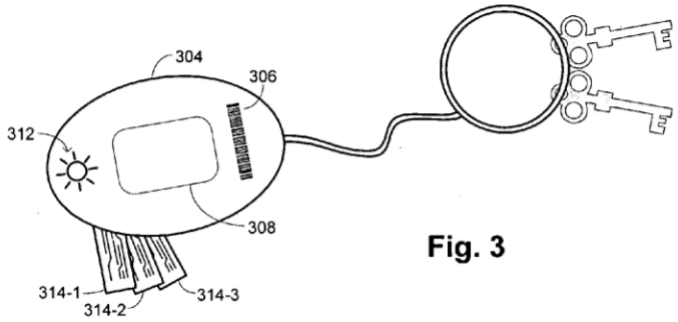
DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,202,156

EXHIBIT E7: US20050137986A1 ("Kean '986")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Kean '986 and (b) under 35 U.S.C. § 103(a) as obvious over Kean '986 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to US20050137986A1 ("Kean '986")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Kean '986 discloses or renders obvious "[a] mobile device." For example: Kean '986 at Abstract Methods and systems are provided for processing secure transactions. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at Fig. 3

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	 Fig. 3 Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch. Kean '986 at [0018] FIG. 3 provides an illustration of a structure for a portable device used in processing secure transactions in an embodiment of the invention; Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks,

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at [0033] The portable device 304 shown in FIG. 3 may include a variety of mechanisms that enhance the security of the transactions even beyond the use of encryption. For instance, a switch 308 may be used to prevent "pocket surfing," in which electromagnetic transmissions from the portable device are captured with the intention of using the received information fraudulently. The switch 308 acts as a physical security measure that may be implemented so that useable electromagnetic signals are only transmitted when the switch is activated. A light-emitting device ("LED") 312 or other indicator may be provided on the portable device to indicate activation by the switch. In one embodiment, the switch 308 comprises a membrane switch, although other switch configurations may alternatively be used. Kean '986 at claim 24 24. A portable device for use in processing a secure transaction, the portable device comprising: To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Kean '986 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Kean '986 at Abstract Methods and systems are provided for processing secure transactions. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0006] Embodiments of the invention thus provide methods and systems for processing secure transactions that make use of electromagnetic initiation of the transactions. In a first set of embodiments, a method is provided for processing a secure transaction. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0007] In some instances, the electromagnetic transmission packet is received at a radio frequency. Further, in some embodiments, a barcode scan of a barcode may also be received, with a barcode value that corresponds to the barcode being transmitted with the decryption of the encrypted magnetic-stripe image. The validity of the barcode may also be verified, such as by calculating a check digit from characters comprised by the scanned barcode and comparing the calculated check digit with a comparison check digit comprised by the scanned barcode. In one embodiment, an antenna is activated to receive the electromagnetic transmission packet only after verifying the validity of the barcode, with the antenna being deactivated after receiving the electromagnetic transmission packet, thereby providing electrical savings and reducing signal-pollution radiation. In other embodiments, the alphanumerical identifier may be transmitted with the decryption of the encrypted magnetic-stripe image. Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch.

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0026] An example of a structure that may conveniently be used for the processing devices 200 is shown for one embodiment in FIGS. 2A and 2B. While FIG. 2A provides an illustration of an external physical structure for the processing device 200, FIG. 2B provides an illustration of components that are usually included internal to the device. The external structure shown in FIG. 2A provides a number of elements that conveniently allow the customer to interface with the device. An antenna 224, which may be optimized for operation at radio frequencies in some instances, allows the processing device 200 to interact with the portable device as described in greater detail below. In addition to the electromagnetic interactions enabled by the antenna 224, the processing device includes a keypad 216 that allows entry of a nonencrypted version of an alphanumerical identifier. As used herein, an "alphanumerical identifier" may have only alphabetic components, may have only numerical components, or may have a combination of alphabetic and numerical components. The illustration in FIG. 2A provides an example where the keypad 216 is equipped to permit entry of an alphanumerical identifier consisting of numerical components. A display 208 permits instructions to be communicated to the customer and a status bar 212 provides an indication that processing steps are being taken. The status bar 212 may be adapted for display in different colors, such as red and green, depending on operations that are being performed and to indicate the successful completion of those operations, progressively illuminating more of the status bar as the terminal completes each phase of the transaction. A set of transaction-selection buttons 204 may be used to select among a number of different services accommodated by the processing device, one of which, i.e. button 204-1, corresponds to the specific service described herein. A terminal interface cable 220 may be

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	used to provide a mechanism for exchange of information between the processing device 200 and a point-of-sale terminal 120, although other mechanisms may alternatively be used, including wireless mechanisms. Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at [0034] here are a number of different ways in which such a switch may function, as illustrated with FIGS. 4A and 4B for different embodiments. For example, in the embodiment illustrated in FIG. 4A, the switch 406 may be configured so that no signal is provided from a processor 410 comprised by the portable device 304 to an antenna 402 comprised by the portable device 304 unless activated. In such an embodiment, no electromagnetic signal is thus transmitted, and therefore cannot be pocket surfed, unless the customer is activating the switch at the time of the transaction. In the embodiment illustrated in FIG. 4B, the switch 414 may instead be configured so that a magnetic-stripe image associated with different accounts is transmitted depending on a state of the switch 414. For example, the default account 418 might correspond to an account that requires a PIN in order to effect transactions so that the magnetic-stripe image alone is insufficient. Protection against pocket surfing is thereby provided by assigning such an account as the default, and by requiring activation of the switch 414 to access the magnetic-stripe image

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	for a different account 418′ or 418″. In some cases, as FIG. 4B illustrates, the switch may comprise a multiposition switch so that more than two states may be accommodated, permitting access to a greater number of accounts with a single portable device 304. Kean '986 at claim 2 The method recited in claim 1 wherein the electromagnetic transmission packet is received at a radio frequency. Kean '986 at claim 23 23. The processing device recited in claim 17 further comprising an interface with a point-of-sale terminal equipped for processing the secure transaction with the magnetic-stripe image. Kean '986 at claim 24 a processor in communication with the radio-frequency antenna, the memory device, and the activation switch, the memory device having a computer-readable program embodied therein for transmitting to a processing device, with the radio-frequency antenna and in accordance with a state of the activation switch, a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a memory to hold transaction data; and	Kean '986 discloses or renders obvious "a memory to hold transaction data." For example: Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch. Kean '986 at [0027]

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	FIG. 2B provides one example of a functional arrangement of components that may be embodied by the processing device 200 to implement the functions described herein, although other functional arrangements may be used in alternative embodiments. FIG. 2B broadly illustrates how individual system elements for the processing device 200 may be implemented in a separated or more integrated manner. The processing device 200 is shown comprised of hardware elements that are electrically coupled via bus 258, including a processor 250, one or more input devices 254, one or more storage devices 256, and the antenna system 224. Information used in implementing the methods described below, such as encryption-key information, is stored on the storage devices 256, which may, for instance, comprise secure-access memory ("SAM") 257. In addition to the keypad 216, for example, the input devices 254 might comprise a smart-card reader slot to allow injection of data to the processing device 200, such as the encryption keys, software upgrades, and the like. Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Kean '986 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Kean '986 at Abstract Methods and systems are provided for processing secure transactions. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0006] Embodiments of the invention thus provide methods and systems for processing secure transactions that make use of electromagnetic initiation of the transactions. In a first set of embodiments, a method is provided for processing a secure transaction. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0007] In some instances, the electromagnetic transmission packet is received at a radio frequency. Further, in some embodiments, a barcode scan of a barcode may also be received, with a barcode value that corresponds to the barcode being transmitted with the decryption of the encrypted magnetic-stripe image. The validity of the barcode may also be verified, such as by calculating a check digit from characters comprised by the scanned barcode and comparing the calculated check digit with a comparison check digit comprised by the scanned barcode. In one embodiment, an antenna is activated to receive the electromagnetic transmission packet only after verifying the validity of the barcode, with the antenna being deactivated after receiving the electromagnetic transmission packet, thereby providing electrical

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	savings and reducing signal-pollution radiation. In other embodiments, the alphanumerical identifier may be transmitted with the decryption of the encrypted magnetic-stripe image. Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch. Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0026] An example of a structure that may conveniently be used for the processing devices 200 is shown for one embodiment in FIGS. 2A and 2B. While FIG. 2A provides an illustration of an external physical structure for the processing device 200, FIG. 2B provides an illustration of components that are usually included internal to the device. The external structure shown in FIG. 2A provides a number of elements that conveniently allow the customer to interface with the device. An antenna 224, which may be optimized for operation at radio frequencies in some instances, allows the processing device 200 to interact with the portable device as described in greater detail below. In addition to the electromagnetic interactions enabled by the antenna 224, the processing device includes a keypad 216 that allows entry of a

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	nonencrypted version of an alphanumerical identifier. As used herein, an "alphanumerical identifier" may have only alphabetic components, may have only numerical components, or may have a combination of alphabetic and numerical components. The illustration in FIG. 2A provides an example where the keypad 216 is equipped to permit entry of an alphanumerical identifier consisting of numerical components. A display 208 permits instructions to be communicated to the customer and a status bar 212 provides an indication that processing steps are being taken. The status bar 212 may be adapted for display in different colors, such as red and green, depending on operations that are being performed and to indicate the successful completion of those operations, progressively illuminating more of the status bar as the terminal completes each phase of the transaction. A set of transaction-selection buttons 204 may be used to select among a number of different services accommodated by the processing device, one of which, i.e. button 204-1, corresponds to the specific service described herein. A terminal interface cable 220 may be used to provide a mechanism for exchange of information between the processing device 200 and a point-of-sale terminal 120, although other mechanisms may alternatively be used, including wireless mechanisms. Kean '986 at [0027] FIG. 2B provides one example of a functional arrangement of components that may be embodied by the processing device 200 to implement the functions described herein, although other functional arrangements may be used in alternative embodiments. FIG. 2B broadly illustrates how individual system elements for the processing device 200 may be implemented in a separated or more integrated manner. The processing device 200 is shown comprised of hardware elements that are electrically coupled via bus 258, including a processor 250, one or more input devices 254, one or more storage devices 256, and the antenna system 224. Information used in implementing the methods described below, such as encryption-key information, is stored on the storage devices 256, which may, for instance, comprise secure-access memory ("SAM") 257. In addition to the keypad 216, for example, the input devices 254 might comprise a smart-card reader slot to allow injection of data to the processing device 200, such as the encryption keys, software upgrades, and the like. Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For

Claim Element	Exemplary Citations to US20050137986A1 (“Kean ’986”)
	example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number (“BIN”). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean ’986 at [0034] here are a number of different ways in which such a switch may function, as illustrated with FIGS. 4A and 4B for different embodiments. For example, in the embodiment illustrated in FIG. 4A, the switch 406 may be configured so that no signal is provided from a processor 410 comprised by the portable device 304 to an antenna 402 comprised by the portable device 304 unless activated. In such an embodiment, no electromagnetic signal is thus transmitted, and therefore cannot be pocket surfed, unless the customer is activating the switch at the time of the transaction. In the embodiment illustrated in FIG. 4B, the switch 414 may instead be configured so that a magnetic-stripe image associated with different accounts is transmitted depending on a state of the switch 414. For example, the default account 418 might correspond to an account that requires a PIN in order to effect transactions so that the magnetic-stripe image alone is insufficient. Protection against pocket surfing is thereby provided by assigning such an account as the default, and by requiring activation of the switch 414 to access the magnetic-stripe image for a different account 418′ or 418″. In some cases, as FIG. 4B illustrates, the switch may comprise a multiposition switch so that more than two states may be accommodated, permitting access to a greater number of accounts with a single portable device 304. Kean ’986 at claim 2 The method recited in claim 1 wherein the electromagnetic transmission packet is received at a radio frequency. Kean ’986 at claim 24 a processor in communication with the radio-frequency antenna, the memory device, and the activation switch, the memory device having a computer-readable program embodied therein for transmitting to a

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	processing device, with the radio-frequency antenna and in accordance with a state of the activation switch, a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	*See* 1[pre] above. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: Kean '986 at Abstract Methods and systems are provided for processing secure transactions. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0006] Embodiments of the invention thus provide methods and systems for processing secure transactions that make use of electromagnetic initiation of the transactions. In a first set of embodiments, a method is provided for processing a secure transaction. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0007] In some instances, the electromagnetic transmission packet is received at a radio frequency. Further, in some embodiments, a barcode scan of a barcode may also be received, with a barcode value that corresponds to the barcode being transmitted with the decryption of the encrypted magnetic-stripe image. The validity of the barcode may also be verified, such as by calculating a check digit from characters comprised by the scanned barcode and comparing the calculated check digit with a comparison check digit comprised by the scanned barcode. In one embodiment, an antenna is activated to receive the electromagnetic transmission packet only after verifying the validity of the barcode, with the antenna being deactivated after receiving the electromagnetic transmission packet, thereby providing electrical savings and reducing signal-pollution radiation. In other embodiments, the alphanumerical identifier may be transmitted with the decryption of the encrypted magnetic-stripe image. Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch. Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with

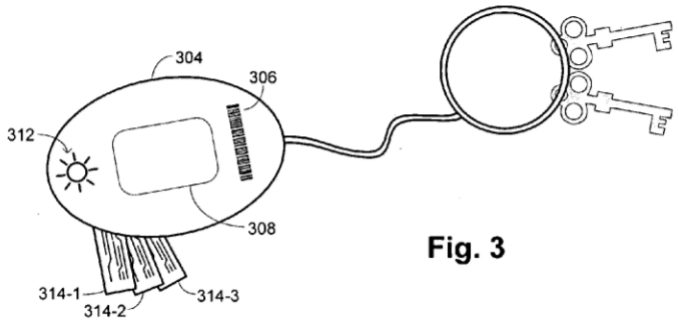
Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at [0034] here are a number of different ways in which such a switch may function, as illustrated with FIGS. 4A and 4B for different embodiments. For example, in the embodiment illustrated in FIG. 4A, the switch 406 may be configured so that no signal is provided from a processor 410 comprised by the portable device 304 to an antenna 402 comprised by the portable device 304 unless activated. In such an embodiment, no electromagnetic signal is thus transmitted, and therefore cannot be pocket surfed, unless the customer is activating the switch at the time of the transaction. In the embodiment illustrated in FIG. 4B, the switch 414 may instead be configured so that a magnetic-stripe image associated with different accounts is transmitted depending on a state of the switch 414. For example, the default account 418 might correspond to an account that requires a PIN in order to effect transactions so that the magnetic-stripe image alone is insufficient. Protection against pocket surfing is thereby provided by assigning such an account as the default, and by requiring activation of the switch 414 to access the magnetic-stripe image

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	for a different account 418′ or 418″. In some cases, as FIG. 4B illustrates, the switch may comprise a multiposition switch so that more than two states may be accommodated, permitting access to a greater number of accounts with a single portable device 304. Kean '986 at claim 23 23. The processing device recited in claim 17 further comprising an interface with a point-of-sale terminal equipped for processing the secure transaction with the magnetic-stripe image. Kean '986 at claim 24 a processor in communication with the radio-frequency antenna, the memory device, and the activation switch, the memory device having a computer-readable program embodied therein for transmitting to a processing device, with the radio-frequency antenna and in accordance with a state of the activation switch, a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Kean '986 at [0025] In processing transactions, the host system 104 is provided in communication with one or more financial institutions 112, usually through a private financial network 108 that so that it is less likely to be compromised than a public network. The financial institutions 112 usually maintain or have access to maintenance information for financial accounts identified in information transmitted to the host system 104 from the transaction-point devices. For example, in the case of a debit transaction, the financial institution 112 may comprise a bank that maintains a demand-deposit account to be debited in accordance with the terms of the transaction. In the case of a credit transaction, the financial institution 112 may comprise a credit-card company that provides funds on a credit basis to customers in accordance with preset credit limits. In the case of a stored-value transaction, the financial institution may be a company that maintains records of stored-value balances for a variety of different merchant labels, perhaps providing mechanisms for reloading value and performing other maintenance functions.

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at [0034] here are a number of different ways in which such a switch may function, as illustrated with FIGS. 4A and 4B for different embodiments. For example, in the embodiment illustrated in FIG. 4A, the switch 406 may be configured so that no signal is provided from a processor 410 comprised by the portable device 304 to an antenna 402 comprised by the portable device 304 unless activated. In such an embodiment, no electromagnetic signal is thus transmitted, and therefore cannot be pocket surfed, unless the customer is activating the switch at the time of the transaction. In the embodiment illustrated in FIG. 4B, the switch 414 may instead be configured so that a magnetic-stripe image associated with different accounts is transmitted depending on a state of the switch 414. For example, the default account 418 might correspond to an account that requires a PIN in order to effect transactions so that the magnetic-stripe image alone is insufficient. Protection against pocket surfing is thereby provided by assigning such an account as the default, and by requiring activation of the switch 414 to access the magnetic-stripe image for a different account 418′ or 418″. In some cases, as FIG. 4B illustrates, the switch may comprise a multiposition switch so that more than two states may be accommodated, permitting access to a greater number of accounts with a single portable device 304.

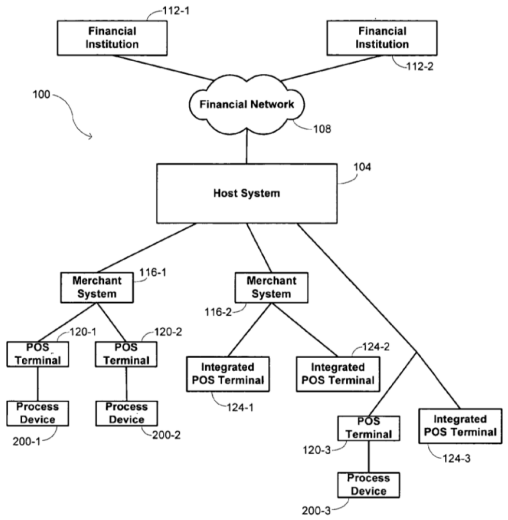
Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0025] In processing transactions, the host system 104 is provided in communication with one or more financial institutions 112, usually through a private financial network 108 that so that it is less likely to be compromised than a public network. The financial institutions 112 usually maintain or have access to maintenance information for financial accounts identified in information transmitted to the host system 104 from the transaction-point devices. For example, in the case of a debit transaction, the financial institution 112 may comprise a bank that maintains a demand-deposit account to be debited in accordance with the terms of the transaction. In the case of a credit transaction, the financial institution 112 may comprise a credit-card company that provides funds on a credit basis to customers in accordance with preset credit limits. In the case of a stored-value transaction, the financial institution may be a company that maintains records of stored-value balances for a variety of different merchant labels, perhaps providing mechanisms for reloading value and performing other maintenance functions.

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at [0034] here are a number of different ways in which such a switch may function, as illustrated with FIGS. 4A and 4B for different embodiments. For example, in the embodiment illustrated in FIG. 4A, the switch 406 may be configured so that no signal is provided from a processor 410 comprised by the portable device 304 to an antenna 402 comprised by the portable device 304 unless activated. In such an embodiment, no electromagnetic signal is thus transmitted, and therefore cannot be pocket surfed, unless the customer is activating the switch at the time of the transaction. In the embodiment illustrated in FIG. 4B, the switch 414 may instead be configured so that a magnetic-stripe image associated with different accounts is transmitted depending on a state of the switch 414. For example, the default account 418 might correspond to an account that requires a PIN in order to effect transactions so that the magnetic-stripe image alone is insufficient. Protection against pocket surfing is thereby provided by assigning such an account as the default, and by requiring activation of the switch 414 to access the magnetic-stripe image for a different account 418′ or 418″. In some cases, as FIG. 4B illustrates, the switch may comprise a multiposition switch so that more than two states may be accommodated, permitting access to a greater number of accounts with a single portable device 304.

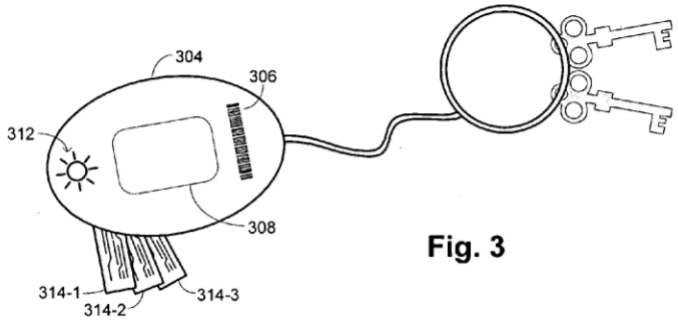
Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Kean '986 at Fig. 3  Fig. 3 Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch. Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet.

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0027] FIG. 2B provides one example of a functional arrangement of components that may be embodied by the processing device 200 to implement the functions described herein, although other functional arrangements may be used in alternative embodiments. FIG. 2B broadly illustrates how individual system elements for the processing device 200 may be implemented in a separated or more integrated manner. The processing device 200 is shown comprised of hardware elements that are electrically coupled via bus 258, including a processor 250, one or more input devices 254, one or more storage devices 256, and the antenna system 224. Information used in implementing the methods described below, such as encryption-key information, is stored on the storage devices 256, which may, for instance, comprise secure-access memory ("SAM") 257. In addition to the keypad 216, for example, the input devices 254 might comprise a smart-card reader slot to allow injection of data to the processing device 200, such as the encryption keys, software upgrades, and the like. Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at claim 22 22. The processing device recited in claim 21 wherein the input device comprises a smart-card reader. Kean '986 at claim 24 a processor in communication with the radio-frequency antenna, the memory device, and the activation switch, the memory device having a computer-readable program embodied therein for transmitting to a processing device, with the radio-frequency antenna and in accordance with a state of the activation switch, a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Kean '986 at Figure 1

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	 Fig. 1 Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Kean '986 discloses or renders obvious "[a] mobile device." For example: *See* above at 1[pre]. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Kean '986 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a].

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Kean '986 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Kean '986 at Fig. 3  Fig. 3 Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch. Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct

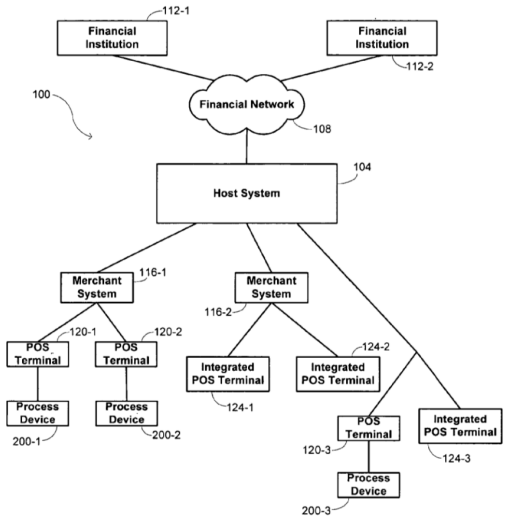
Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at claim 22 22. The processing device recited in claim 21 wherein the input device comprises a smart-card reader. *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Kean '986 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Kean '986 at Abstract Methods and systems are provided for processing secure transactions. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0006] Embodiments of the invention thus provide methods and systems for processing secure transactions that make use of electromagnetic initiation of the transactions. In a first set of embodiments, a method is provided for processing a secure transaction. An electromagnetic transmission packet is received from a portable device at a processing device. The electromagnetic transmission packet includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. A keyed nonencrypted version of the alphanumerical identifier is received at the processing device, and the encrypted version of

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	the alphanumerical identifier is decrypted. The decryption of the encrypted version of the alphanumerical identifier is compared with the nonencrypted version of the alphanumerical identifier. Thereafter, a decryption of the encrypted magnetic-stripe image is transmitted to a host system for processing the secure transaction using an account identified by the decryption of the magnetic-stripe image. Kean '986 at [0007] In some instances, the electromagnetic transmission packet is received at a radio frequency. Further, in some embodiments, a barcode scan of a barcode may also be received, with a barcode value that corresponds to the barcode being transmitted with the decryption of the encrypted magnetic-stripe image. The validity of the barcode may also be verified, such as by calculating a check digit from characters comprised by the scanned barcode and comparing the calculated check digit with a comparison check digit comprised by the scanned barcode. In one embodiment, an antenna is activated to receive the electromagnetic transmission packet only after verifying the validity of the barcode, with the antenna being deactivated after receiving the electromagnetic transmission packet, thereby providing electrical savings and reducing signal-pollution radiation. In other embodiments, the alphanumerical identifier may be transmitted with the decryption of the encrypted magnetic-stripe image. Kean '986 at [0011] In a third set of embodiments, a portable device is provided for use in processing a secure transaction. The portable device comprises a radio-frequency antenna, a memory device, an activation switch, and a processor. The processor is provided in communication with the radio-frequency antenna, the memory device, and the activation switch. The memory device has a computer-readable program embodied therein for transmitting a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier to a processing device. The transmission is performed with the radio-frequency antenna and in accordance with a state of the activation switch. Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0026] An example of a structure that may conveniently be used for the processing devices 200 is shown for one embodiment in FIGS. 2A and 2B. While FIG. 2A provides an illustration of an external physical structure for the processing device 200, FIG. 2B provides an illustration of components that are usually included internal to the device. The external structure shown in FIG. 2A provides a number of elements that conveniently allow the customer to interface with the device. An antenna 224, which may be optimized for operation at radio frequencies in some instances, allows the processing device 200 to interact with the portable device as described in greater detail below. In addition to the electromagnetic interactions enabled by the antenna 224, the processing device includes a keypad 216 that allows entry of a nonencrypted version of an alphanumerical identifier. As used herein, an "alphanumerical identifier" may have only alphabetic components, may have only numerical components, or may have a combination of alphabetic and numerical components. The illustration in FIG. 2A provides an example where the keypad 216 is equipped to permit entry of an alphanumerical identifier consisting of numerical components. A display 208 permits instructions to be communicated to the customer and a status bar 212 provides an indication that processing steps are being taken. The status bar 212 may be adapted for display in different colors, such as red and green, depending on operations that are being performed and to indicate the successful completion of those operations, progressively illuminating more of the status bar as the terminal completes each phase of the transaction. A set of transaction-selection buttons 204 may be used to select among a number of different services accommodated by the processing device, one of which, i.e. button 204-1, corresponds to the specific service described herein. A terminal interface cable 220 may be used to provide a mechanism for exchange of information between the processing device 200 and a point-of-sale terminal 120, although other mechanisms may alternatively be used, including wireless mechanisms. Kean '986 at [0027] FIG. 2B provides one example of a functional arrangement of components that may be embodied by the processing device 200 to implement the functions described herein, although other functional arrangements may be used in alternative embodiments. FIG. 2B broadly illustrates how individual system elements for the processing device 200 may be implemented in a separated or more integrated manner. The processing device 200 is shown comprised of hardware elements that are electrically coupled via bus

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	258, including a processor 250, one or more input devices 254, one or more storage devices 256, and the antenna system 224. Information used in implementing the methods described below, such as encryption-key information, is stored on the storage devices 256, which may, for instance, comprise secure-access memory ("SAM") 257. In addition to the keypad 216, for example, the input devices 254 might comprise a smart-card reader slot to allow injection of data to the processing device 200, such as the encryption keys, software upgrades, and the like. Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at [0034] here are a number of different ways in which such a switch may function, as illustrated with FIGS. 4A and 4B for different embodiments. For example, in the embodiment illustrated in FIG. 4A, the switch 406 may be configured so that no signal is provided from a processor 410 comprised by the portable device 304 to an antenna 402 comprised by the portable device 304 unless activated. In such an embodiment, no electromagnetic signal is thus transmitted, and therefore cannot be pocket surfed, unless the customer is activating the switch at the time of the transaction. In the embodiment illustrated in FIG. 4B, the switch 414 may instead be configured so that a magnetic-stripe image associated with different accounts is transmitted depending on a state of the switch 414. For example, the default account 418 might

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	correspond to an account that requires a PIN in order to effect transactions so that the magnetic-stripe image alone is insufficient. Protection against pocket surfing is thereby provided by assigning such an account as the default, and by requiring activation of the switch 414 to access the magnetic-stripe image for a different account 418′ or 418″. In some cases, as FIG. 4B illustrates, the switch may comprise a multiposition switch so that more than two states may be accommodated, permitting access to a greater number of accounts with a single portable device 304. Kean '986 at claim 2 The method recited in claim 1 wherein the electromagnetic transmission packet is received at a radio frequency. Kean '986 at claim 24 a processor in communication with the radio-frequency antenna, the memory device, and the activation switch, the memory device having a computer-readable program embodied therein for transmitting to a processing device, with the radio-frequency antenna and in accordance with a state of the activation switch, a radio-frequency transmission packet that includes an encrypted magnetic-stripe image and an encrypted version of an alphanumerical identifier. *See also* 1[c] and claim 5 above. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Kean '986 at Figure 1

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	 Fig. 1 Kean '986 at [0012] In some such embodiments, the computer-readable program further includes instruction for receiving, with the radio-frequency antenna, an identification of the processing device and a transaction identifier. The identification of the processing device and the transaction identifier are encrypted, with the encrypted versions being transmitted to the processing device as part of the radio-frequency transmission packet. The states of the activation switch may define on and off states of the portable device in some embodiments. In other embodiments, the states of the activation switch define which of a plurality of accounts is to be used for the secure transaction. A default of the plurality of accounts may require correct identification of the alphanumerical identifier. The activation switch may comprise a membrane switch. In some cases, the portable device may also comprise a plurality of input ports for payment modules, with the encrypted magnetic-stripe image defining at least one of the payment modules. The payment modules may comprise stored-value modules, debit modules, credit modules, and the like, and may be provided in the form of support interface modules ("SIMs"). Kean '986 at [0023] In FIG. 1, there are three examples where the process device 200 is provided as a satellite device in communication with an existing point-of-sale terminal 120, i.e. in the case of process devices 200-1, 200-

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	2, and 200-3. In each of these instances, the point-of-sale terminal 120 may have the structure and functionality of existing equipment configured for communication with a host system 104 in processing transactions. In some cases, such existing equipment may already be configured to accommodate a variety of different transaction instruments by including, for example, payment-information-entry components, signature-capture components, keypads, keyboards, display screens, biometric-data-capture components, speakers, printers, processors, software, memory, communication devices, and the like. Examples of such multifunction point-of-sale terminals are provided in the following commonly assigned applications, the entire disclosures of which are incorporated herein by reference for all purposes: U.S. Prov. Pat. Appl. No. 60/147,889, entitled "INTEGRATED POINT OF SALE DEVICE," filed Aug. 9, 1999 by Randy J. Templeton et al.; U.S. patent application Ser. No. 09/634,901, entitled "POINT OF SALE PAYMENT SYSTEM," filed Aug. 9, 2000 by Randy J. Templeton et al.; U.S. patent application Ser. No. 10/116,689, entitled "SYSTEMS AND METHODS FOR PERFORMING TRANSACTIONS AT A POINT-OF-SALE," filed Apr. 3, 2002 by Earney Stoutenburg et al.; U.S. patent application Ser. No. 10/116,733, entitled "SYSTEMS AND METHODS FOR DEPLOYING A POINT-OF-SALE SYSTEM," filed Apr. 3, 2002 by Earney Stoutenburg et al.; U.S. patent application Ser. No. 10/116,686, entitled "SYSTEMS AND METHODS FOR UTILIZING A POINT-OF-SALE SYSTEM," filed Apr. 3, 2002 by Earney Stoutenburg et al.; and U.S. patent application Ser. No. 10/116,735, entitled "SYSTEMS AND METHODS FOR CONFIGURING A POINT-OF-SALE SYSTEM," filed Apr. 3, 2002 by Earney Stoutenburg. FIG. 1 also provides three examples where the process device is integrated as part of a multifunction point-of-sale terminal 124, i.e. in the case of integrated point-of-sale terminals 124-1, 124-2, and 124-3. The point-of-sale terminals 120 and integrated point-of-sale terminals 124 are sometimes referred to collectively herein as "transaction-point devices." Kean '986 at [0030] An example of the portable device is provided in FIG. 3 in the form of a key fob 304, which may conveniently be carried by customers. The portable device includes memory that may be used to hold encrypted versions of the magnetic-stripe image and alphanumerical identifier. The magnetic-stripe image and alphanumerical identifier may conveniently be encrypted using the same key, although this is not required. As used herein, the "magnetic-stripe image" that is stored in memory by the portable device is intended to refer to account information of the type that is commonly stored on magnetic-stripe tracks. For example, the information may be stored in a format that has a correspondence to the ISO/IEC 7810, 11, 12, and 13 series of standards, which specify a three-track format, storage scheme, and bit density for all financial card applications. While the information may conveniently be stored in a format that mimics the magnetic-stripe organization, with different types of information being associated with different tracks, references to such a magnetic-stripe image are intended more broadly to encompass any organization of

Claim Element	Exemplary Citations to US20050137986A1 ("Kean '986")
	the information. For example, the magnetic-stripe image may comprise an identification of a financial account and of a financial institution that holds the financial account in the form of an account number coupled with a bank identification number ("BIN"). In addition, information identifying the customer by name, an expiration date, and various check characters may be included, although the specific information content of the magnetic-stripe image may vary according to such factors as the issuer, the type of accounts accommodated, the status of the customer, and the like. Kean '986 at claim 23 23. The processing device recited in claim 17 further comprising an interface with a point-of-sale terminal equipped for processing the secure transaction with the magnetic-stripe image. *See also* claim 8 above. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example: *See* above at claim 3. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Kean '986 discloses or renders obvious "[t]he mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: *See* above at claim 2. To the extent this limitation is not disclosed by Kean '986, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Kean '986, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

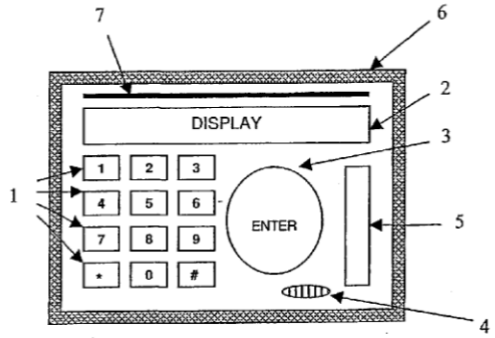
Patent Owner's Ex. 2020
Page 439

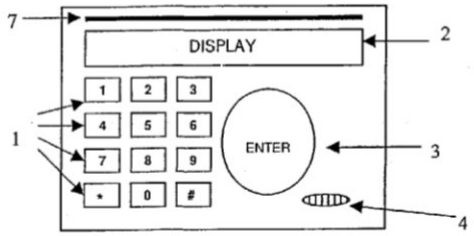
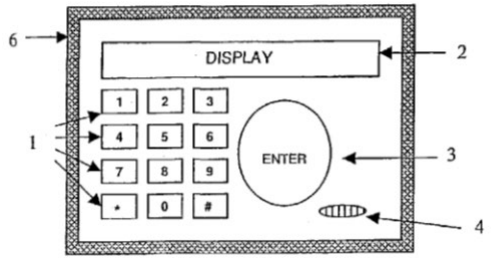
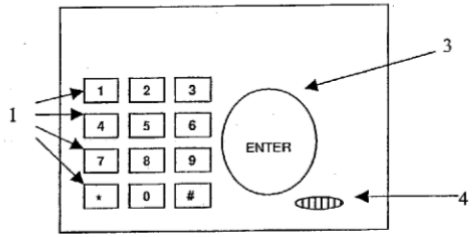
EXHIBIT E8: US20030075610A1 ("Ong '610")

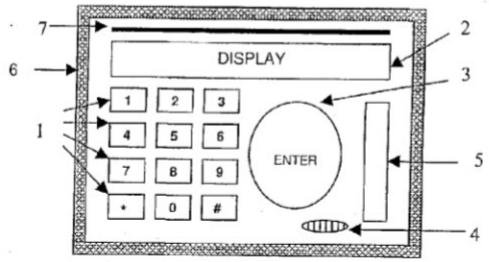
As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Ong '610 and (b) under 35 U.S.C. § 103(a) as obvious over Ong '610 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to US20030075610A1 ("Ong '610")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Ong '610 discloses or renders obvious "[a] mobile device." For example: Ong '610 at Abstract Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at Figure 1 Figure 1: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong '610 at [0058]–[0059] The electronic credit card financial limit can be verified by the transaction station with a link to a remote site system. This will prevent the electronic credit card from generating further transactions once the financial limit is reached. The funds limiting function is optional and may be activated by either the financial institution issuing the electronic credit card or by the holder to cross-check and either alert him or her of his or her account balance. The electronic credit card may transact electronic cash which can be used as a currency exchange device. A traveller going abroad can choose to have a set amount for a specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Ong '610 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Ong '610 at Figure 5.

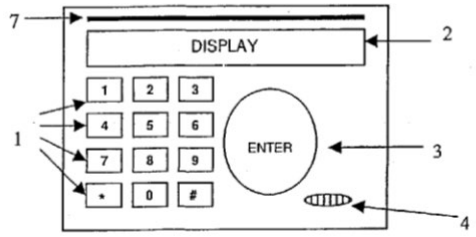
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong '610 at Figure 6 Figure 6: A drawing of ECC physical form covering SAC with PIN control using magnetic induction telecommunication device. Drawing is not to scale.  Ong '610 at Figure 8 Figure 8: A front view drawing of ECC physical form covering SAC with PIN control using magnetic strip telecommunication device. Drawing is not to scale.  Ong '610 at Figure 10

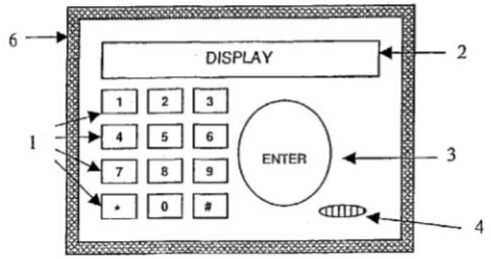
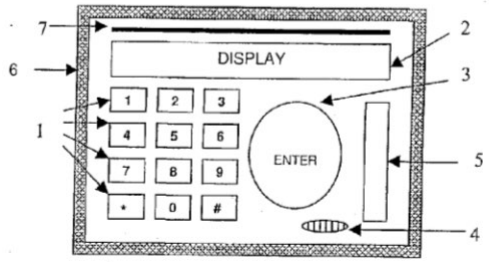
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 10: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong '610 at [0041] Referring to FIG. 1, there is shown an electronic credit card including a user verification means; a means for generating a unique code (not shown); a storage means for storing the user's account details (not shown); and a communication means. In this embodiment the user verification means includes a keypad for entry of a personal identification number (PIN) and the communication means includes a infra red communication device 5, a magnetic induction telecommunication device 6, radio frequency telecommunication device in the form of an antenna 7. The electronic credit card also includes a display 2, an enter/confirmation button and an audio transducer 4 for providing an audible sound. Ong '610 at [0042] The electronic code also includes a processor means for receiving input from the keypad 1 and the button 3. The processor means is also arranged to control output of the display 2 and output of the audio transducer 4. The processor means is further arranged to control communication via the communication means 5, 6, 7. Ong '610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong '610 at [0044] The electronic credit card operates by a user entering a PIN number into the keypad 1 whereby the user verification means verifies that the PIN number is correct and thus the identity of the user is verified. The

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	means for generating unique authorisation code then generates the authorisation code which is provided along with the user's account details, to the communication means which communicates these to a transaction station to facilitate an electronic funds transfer transaction. Ong '610 at [0047] Referring to FIG. 3, the electronic credit card communicates by it's communication means with an automatic teller machine (ATM) or an electronic funds transfer point of sale (EFTPOS) machine, which in turn communicates via standard methods to a host computer to perform electronic funds transfer, cash withdrawal or other transaction. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at [0050] FIG. 6 shows a version of the electronic credit card with a keypad forming part of the user verification means and magnetic induction communication device 6 forming part of the communication means. Ong '610 at [0052] FIG. 8 shows a version of the electronic credit card with a keypad acting as part of the user verification means and a magnetic strip 9 shown in FIG. 9 providing coded information as part of the communication means Ong '610 at [0053] FIG. 10 shows a version of the electronic credit card with a keypad 1 forming part of the user verification means, a combination of infra red transmitter receiver 5, radio frequency antenna 7 and induction 6 forming part of the communication means. Ong '610 at [0063] The electronic credit card can store more than one credit card/debit card accounts. These can be cards distributed from different financial institutions, organisations or companies. The electronic credit card can retain amounts of transactions conducted by the user, with information regarding his or her financial balance in relation to the account limit. This may be available for one or more credit card accounts. Ong '610 at claim 1

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at claim 16 An electronic credit card in accordance with claim 1, wherein the communication means includes a radio frequency transfer means. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a memory to hold transaction data; and	Ong '610 discloses or renders obvious "a memory to hold transaction data." For example: Ong '610 at Abstract Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong '610 at [0014] a storage means for storing the user's account details for use in an electronic funds transfer transaction; and

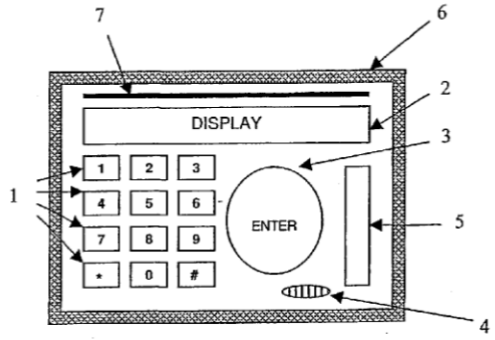
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at [0019] Preferably the storage means is arranged to store a financial limit for transactions that the electronic credit card may be used for. Preferably the financial limit is provided to the transaction station by the communication means. Alternatively the electronic credit card including a processor means for keeping track of the use of the electronic credit card and will not generate or provide the authorisation code if the financial limit is exceeded. Alternatively the financial limit may be retrieved via the transaction station from a financial institution. Ong '610 at [0019]–[0020] Preferably the storage means is arranged to store more than one set of account details. Ong '610 at [0021] Preferably the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at [0026] Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available. Ong '610 at [0041] Referring to FIG. 1, there is shown an electronic credit card including a user verification means; a means for generating a unique code (not shown); a storage means for storing the user's account details (not shown); and a communication means. In this embodiment the user verification means includes a keypad for entry of a personal identification number (PIN) and the communication means includes a infra red communication device 5, a magnetic induction telecommunication device 6, radio frequency telecommunication device in the form of an antenna 7. The electronic credit card also includes a display 2, an enter/confirmation button and an audio transducer 4 for providing an audible sound. Ong '610 at [0063] The electronic credit card can store more than one credit card/debit card accounts. These can be cards distributed from different financial institutions, organisations or companies. The electronic credit card can retain amounts of transactions conducted by the user, with information regarding his or her financial balance in relation to the account limit. This may be available for one or more credit card accounts.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at claim 1 a storage means for storing the user's account details for use in an electronic funds transfer transaction; and Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at claim 21 . An electronic credit card in accordance with claim 6, wherein the storage means stores transaction details and a processor means is provided to calculate the funds available from the financial limit. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Ong '610 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Ong '610 at Figure 5. Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong '610 at Figure 6

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	Figure 6: A drawing of ECC physical form covering SAC with PIN control using magnetic induction telecommunication device. Drawing is not to scale.  Ong ’610 at Figure 10 Figure 10: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong ’610 at [0026] Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available. Ong ’610 at [0041] Referring to FIG. 1, there is shown an electronic credit card including a user verification means; a means for generating a unique code (not shown); a storage means for storing the user's account details (not shown); and a communication means. In this embodiment the user verification means includes a keypad for entry of a personal identification number (PIN) and the communication means includes a infra red communication device 5, a magnetic induction telecommunication device 6, radio frequency telecommunication device in the form of an antenna 7. The electronic credit card also includes a display 2, an enter/confirmation button and an audio transducer 4 for providing an audible sound. Ong ’610 at [0042]

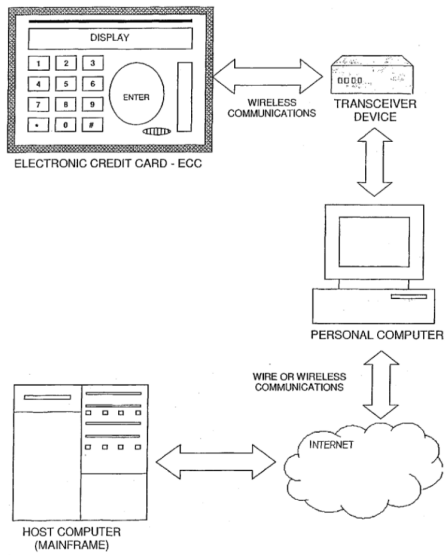
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	The electronic code also includes a processor means for receiving input from the keypad 1 and the button 3. The processor means is also arranged to control output of the display 2 and output of the audio transducer 4. The processor means is further arranged to control communication via the communication means 5, 6, 7. Ong '610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at [0050] FIG. 6 shows a version of the electronic credit card with a keypad forming part of the user verification means and magnetic induction communication device 6 forming part of the communication means. Ong '610 at [0053] FIG. 10 shows a version of the electronic credit card with a keypad 1 forming part of the user verification means, a combination of infra red transmitter receiver 5, radio frequency antenna 7 and induction 6 forming part of the communication means. Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at claim 16 An electronic credit card in accordance with claim 1, wherein the communication means includes a radio frequency transfer means. Ong '610 at claim 21 . An electronic credit card in accordance with claim 6, wherein the storage means stores transaction details and a processor means is provided to calculate the funds available from the financial limit. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	Ong '610 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: Ong '610 at [0027] Preferably the electronic credit card is incorporated into another device. Ong '610 at [0058]–[0059] The electronic credit card financial limit can be verified by the transaction station with a link to a remote site system. This will prevent the electronic credit card from generating further transactions once the financial limit is reached. The funds limiting function is optional and may be activated by either the financial institution issuing the electronic credit card or by the holder to cross-check and either alert him or her of his or her account balance. The electronic credit card may transact electronic cash which can be used as a currency exchange device. A traveller going abroad can choose to have a set amount for a specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone. *See also* 1[pre] above. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic	Ong '610 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example:

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
field mimics a swipe of a magnetic credit card.	Ong '610 at Abstract Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong '610 at Figure 1 Figure 1: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong '610 at Figure 2

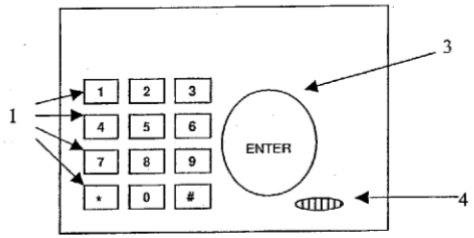
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")

Figure 2: A drawing of ECC communications link to PC and Mainframe Computer. Drawing is not to scale.



Ong '610 at Figure 8

Figure 8: A front view drawing of ECC physical form covering SAC with PIN control using magnetic strip telecommunication device. Drawing is not to scale.



Ong '610 at [0001]

> The present invention relates to an electronic credit card providing secure controlled and reliable transaction of funds.

Ong '610 at [0011]

> In accordance with the present invention there is provided an electronic credit card comprising at least:

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at [0019] Preferably the storage means is arranged to store a financial limit for transactions that the electronic credit card may be used for. Preferably the financial limit is provided to the transaction station by the communication means. Alternatively the electronic credit card including a processor means for keeping track of the use of the electronic credit card and will not generate or provide the authorisation code if the financial limit is exceeded. Alternatively the financial limit may be retrieved via the transaction station from a financial institution. Ong '610 at [0029] FIG. 1 is a schematic representation of an electronic credit card in accordance with the present invention; Ong '610 at [0031] FIG. 3 is a schematic representation between electronic credit card of FIG. 1 and an ATM or EFTPOS terminal and a host computer; Ong '610 at [0032] FIG. 4 is an alternative embodiment of an electronic credit card in accordance with the present invention; Ong '610 at [0033] FIG. 5 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong '610 at [0034] FIG. 6 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong '610 at [0035] FIG. 7 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong '610 at [0036] FIG. 8 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong '610 at [0037]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	FIG. 9 is a rear view of an electronic credit card in accordance with the present invention having a magnetic strip communication device; Ong '610 at [0038] FIG. 10 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong '610 at [0039] FIG. 11 is a further alternative embodiment of an electronic credit card in accordance with the present invention; and Ong '610 at [0040] FIG. 12 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong '610 at [0041] Referring to FIG. 1, there is shown an electronic credit card including a user verification means; a means for generating a unique code (not shown); a storage means for storing the user's account details (not shown); and a communication means. In this embodiment the user verification means includes a keypad for entry of a personal identification number (PIN) and the communication means includes a infra red communication device 5, a magnetic induction telecommunication device 6, radio frequency telecommunication device in the form of an antenna 7. The electronic credit card also includes a display 2, an enter/confirmation button and an audio transducer 4 for providing an audible sound. Ong '610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong '610 at [0044] The electronic credit card operates by a user entering a PIN number into the keypad 1 whereby the user verification means verifies that the PIN number is correct and thus the identity of the user is verified. The means for generating unique authorisation code then generates the authorisation code which is provided

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	along with the user's account details, to the communication means which communicates these to a transaction station to facilitate an electronic funds transfer transaction. Ong '610 at [0047] Referring to FIG. 3, the electronic credit card communicates by it's communication means with an automatic teller machine (ATM) or an electronic funds transfer point of sale (EFTPOS) machine, which in turn communicates via standard methods to a host computer to perform electronic funds transfer, cash withdrawal or other transaction. Ong '610 at [0048] FIG. 4 shows a typical physical form of an electronic credit card with a keypad as the user verification means, and infra red receiver as part of the communication means. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at [0050] FIG. 6 shows a version of the electronic credit card with a keypad forming part of the user verification means and magnetic induction communication device 6 forming part of the communication means. Ong '610 at [0052] FIG. 8 shows a version of the electronic credit card with a keypad acting as part of the user verification means and a magnetic strip 9 shown in FIG. 9 providing coded information as part of the communication means Ong '610 at [0058] The electronic credit card may generate its transaction number either in synchronisation with the transfer station link to a remote site system control function. The transaction station may be an Internet site with this capability. Ong '610 at [0058]–[0059] The electronic credit card financial limit can be verified by the transaction station with a link to a remote site system. This will prevent the electronic credit card from generating further transactions once the financial limit is reached. The funds limiting function is optional and may be activated by either the

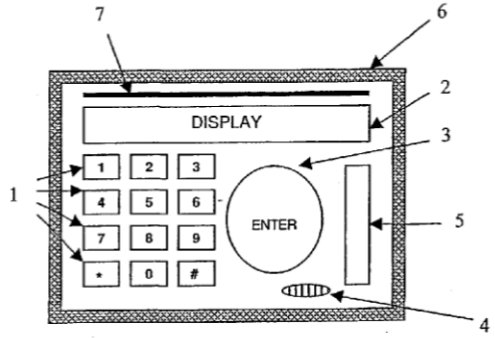
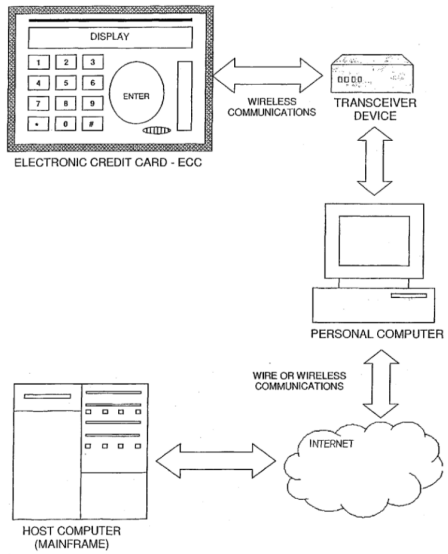
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	financial institution issuing the electronic credit card or by the holder to cross-check and either alert him or her of his or her account balance. The electronic credit card may transact electronic cash which can be used as a currency exchange device. A traveller going abroad can choose to have a set amount for a specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone. Ong '610 at [0063] The electronic credit card can store more than one credit card/debit card accounts. These can be cards distributed from different financial institutions, organisations or companies. The electronic credit card can retain amounts of transactions conducted by the user, with information regarding his or her financial balance in relation to the account limit. This may be available for one or more credit card accounts. Ong '610 at claim 1 An electronic credit card comprising at least: Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at claim 16 An electronic credit card in accordance with claim 1, wherein the communication means includes a radio frequency transfer means. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.

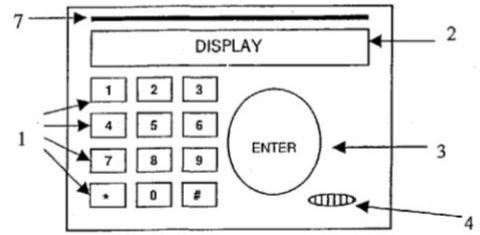
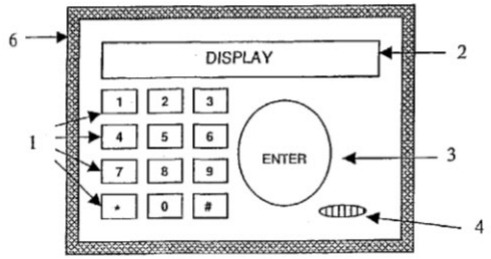
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Ong '610 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Ong '610 at Abstract Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong '610 at [0001] The present invention relates to an electronic credit card providing secure controlled and reliable transaction of funds. Ong '610 at [0021] Preferably the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at [0026] Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available. Ong '610 at [0063] The electronic credit card can store more than one credit card/debit card accounts. These can be cards distributed from different financial institutions, organisations or companies. The electronic credit card can retain amounts of transactions conducted by the user, with information regarding his or her financial balance in relation to the account limit. This may be available for one or more credit card accounts.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Ong '610 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Ong '610 at Abstract Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong '610 at [0001] The present invention relates to an electronic credit card providing secure controlled and reliable transaction of funds. Ong '610 at [0011] In accordance with the present invention there is provided an electronic credit card comprising at least: Ong '610 at [0021]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Preferably the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at [0026] Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available. Ong '610 at [0029] FIG. 1 is a schematic representation of an electronic credit card in accordance with the present invention; Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at [0058] The electronic credit card may generate its transaction number either in synchronisation with the transfer station link to a remote site system control function. The transaction station may be an Internet site with this capability. Ong '610 at [0058]–[0059] The electronic credit card financial limit can be verified by the transaction station with a link to a remote site system. This will prevent the electronic credit card from generating further transactions once the financial limit is reached. The funds limiting function is optional and may be activated by either the financial institution issuing the electronic credit card or by the holder to cross-check and either alert him or her of his or her account balance. The electronic credit card may transact electronic cash which can be used as a currency exchange device. A traveller going abroad can choose to have a set amount for a specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone. Ong '610 at [0063] The electronic credit card can store more than one credit card/debit card accounts. These can be cards distributed from different financial institutions, organisations or companies. The electronic credit card can

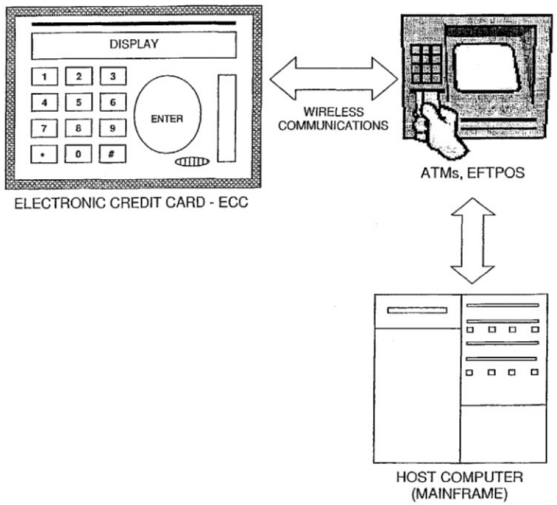
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	retain amounts of transactions conducted by the user, with information regarding his or her financial balance in relation to the account limit. This may be available for one or more credit card accounts. Ong '610 at claim 1 An electronic credit card comprising at least: Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Ong '610 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Ong '610 at Abstract Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via

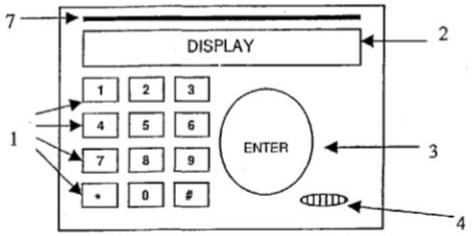
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong '610 at Figure 1 Figure 1: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong '610 at Figure 2 Figure 2: A drawing of ECC communications link to PC and Mainframe Computer. Drawing is not to scale. 

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at Figure 5. Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong '610 at Figure 6 Figure 6: A drawing of ECC physical form covering SAC with PIN control using magnetic induction telecommunication device. Drawing is not to scale.  Ong '610 at [0019] Preferably the storage means is arranged to store a financial limit for transactions that the electronic credit card may be used for. Preferably the financial limit is provided to the transaction station by the communication means. Alternatively the electronic credit card including a processor means for keeping track of the use of the electronic credit card and will not generate or provide the authorisation code if the financial limit is exceeded. Alternatively the financial limit may be retrieved via the transaction station from a financial institution. Ong '610 at [0021] Preferably the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified.

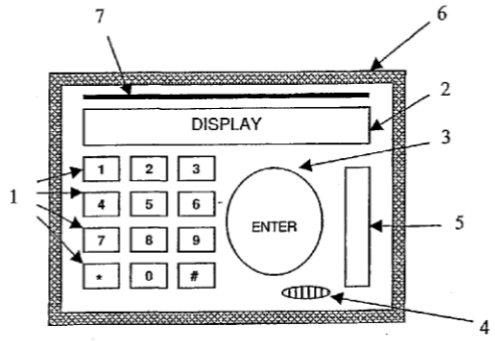
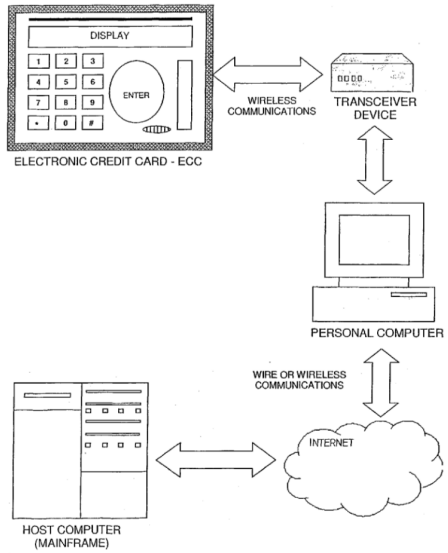
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at [0026] Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available. Ong '610 at [0041] Referring to FIG. 1, there is shown an electronic credit card including a user verification means; a means for generating a unique code (not shown); a storage means for storing the user's account details (not shown); and a communication means. In this embodiment the user verification means includes a keypad for entry of a personal identification number (PIN) and the communication means includes a infra red communication device 5, a magnetic induction telecommunication device 6, radio frequency telecommunication device in the form of an antenna 7. The electronic credit card also includes a display 2, an enter/confirmation button and an audio transducer 4 for providing an audible sound. Ong '610 at [0042] The electronic code also includes a processor means for receiving input from the keypad 1 and the button 3. The processor means is also arranged to control output of the display 2 and output of the audio transducer 4. The processor means is further arranged to control communication via the communication means 5, 6, 7. Ong '610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong '610 at [0048] FIG. 4 shows a typical physical form of an electronic credit card with a keypad as the user verification means, and infra red receiver as part of the communication means. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means.

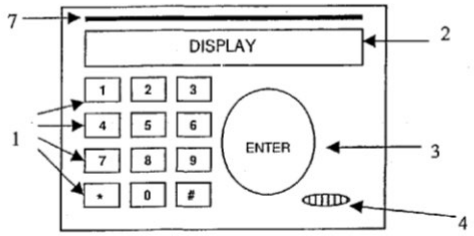
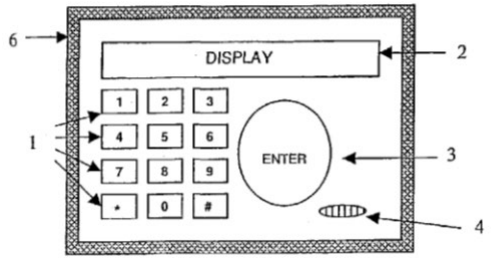
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at [0058]–[0059] The electronic credit card financial limit can be verified by the transaction station with a link to a remote site system. This will prevent the electronic credit card from generating further transactions once the financial limit is reached. The funds limiting function is optional and may be activated by either the financial institution issuing the electronic credit card or by the holder to cross-check and either alert him or her of his or her account balance. The electronic credit card may transact electronic cash which can be used as a currency exchange device. A traveller going abroad can choose to have a set amount for a specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone. Ong '610 at claim 1 An electronic credit card comprising at least: Ong '610 at claim 1 a storage means for storing the user's account details for use in an electronic funds transfer transaction; and Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at claim 16 An electronic credit card in accordance with claim 1, wherein the communication means includes a radio frequency transfer means. Ong '610 at claim 21

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	. An electronic credit card in accordance with claim 6, wherein the storage means stores transaction details and a processor means is provided to calculate the funds available from the financial limit. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Ong '610 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Ong '610 at Figure 3 Figure 3: A drawing of ECC communications link to Teller Machines, ATMs, EFTPOS and Host Computer. Drawing is not to scale.  Ong '610 at Figure 5.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong '610 at [0047] Referring to FIG. 3, the electronic credit card communicates by it's communication means with an automatic teller machine (ATM) or an electronic funds transfer point of sale (EFTPOS) machine, which in turn communicates via standard methods to a host computer to perform electronic funds transfer, cash withdrawal or other transaction. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 16 An electronic credit card in accordance with claim 1, wherein the communication means includes a radio frequency transfer means. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Ong '610 discloses or renders obvious "[a] mobile device." For example:

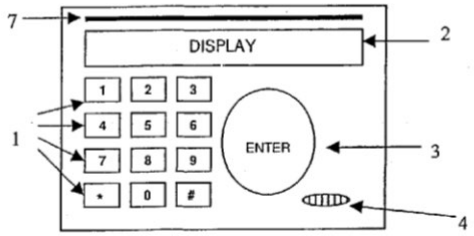
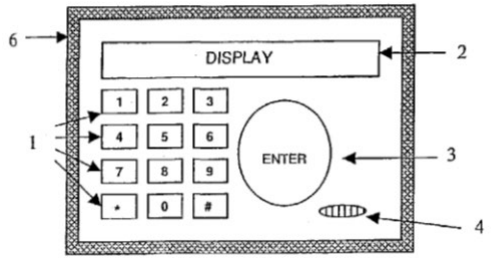
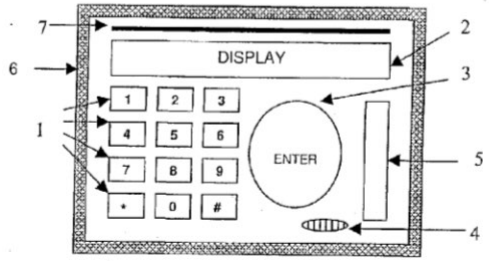
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	See above at 1[pre]. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Ong '610 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a]. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Ong '610 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Ong '610 at Abstract Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong '610 at Figure 1

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 1: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong '610 at Figure 2 Figure 2: A drawing of ECC communications link to PC and Mainframe Computer. Drawing is not to scale.  Ong '610 at Figure 5.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong '610 at Figure 6 Figure 6: A drawing of ECC physical form covering SAC with PIN control using magnetic induction telecommunication device. Drawing is not to scale.  Ong '610 at [0019] Preferably the storage means is arranged to store a financial limit for transactions that the electronic credit card may be used for. Preferably the financial limit is provided to the transaction station by the communication means. Alternatively the electronic credit card including a processor means for keeping track of the use of the electronic credit card and will not generate or provide the authorisation code if the financial limit is exceeded. Alternatively the financial limit may be retrieved via the transaction station from a financial institution. Ong '610 at [0021] Preferably the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at [0026]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available. Ong '610 at [0042] The electronic code also includes a processor means for receiving input from the keypad 1 and the button 3. The processor means is also arranged to control output of the display 2 and output of the audio transducer 4. The processor means is further arranged to control communication via the communication means 5, 6, 7. Ong '610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong '610 at [0048] FIG. 4 shows a typical physical form of an electronic credit card with a keypad as the user verification means, and infra red receiver as part of the communication means. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at [0058]–[0059] The electronic credit card financial limit can be verified by the transaction station with a link to a remote site system. This will prevent the electronic credit card from generating further transactions once the financial limit is reached. The funds limiting function is optional and may be activated by either the financial institution issuing the electronic credit card or by the holder to cross-check and either alert him or her of his or her account balance. The electronic credit card may transact electronic cash which can be used as a currency exchange device. A traveller going abroad can choose to have a set amount for a specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at claim 1 An electronic credit card comprising at least: Ong '610 at claim 1 a storage means for storing the user's account details for use in an electronic funds transfer transaction; and Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at claim 16 An electronic credit card in accordance with claim 1, wherein the communication means includes a radio frequency transfer means. Ong '610 at claim 21 . An electronic credit card in accordance with claim 6, wherein the storage means stores transaction details and a processor means is provided to calculate the funds available from the financial limit. *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Ong '610 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Ong '610 at Figure 5.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong '610 at Figure 6 Figure 6: A drawing of ECC physical form covering SAC with PIN control using magnetic induction telecommunication device. Drawing is not to scale.  Ong '610 at Figure 10 Figure 10: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong '610 at [0026] Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at [0041] Referring to FIG. 1, there is shown an electronic credit card including a user verification means; a means for generating a unique code (not shown); a storage means for storing the user's account details (not shown); and a communication means. In this embodiment the user verification means includes a keypad for entry of a personal identification number (PIN) and the communication means includes a infra red communication device 5, a magnetic induction telecommunication device 6, radio frequency telecommunication device in the form of an antenna 7. The electronic credit card also includes a display 2, an enter/confirmation button and an audio transducer 4 for providing an audible sound. Ong '610 at [0042] The electronic code also includes a processor means for receiving input from the keypad 1 and the button 3. The processor means is also arranged to control output of the display 2 and output of the audio transducer 4. The processor means is further arranged to control communication via the communication means 5, 6, 7. Ong '610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at [0050] FIG. 6 shows a version of the electronic credit card with a keypad forming part of the user verification means and magnetic induction communication device 6 forming part of the communication means. Ong '610 at [0053] FIG. 10 shows a version of the electronic credit card with a keypad 1 forming part of the user verification means, a combination of infra red transmitter receiver 5, radio frequency antenna 7 and induction 6 forming part of the communication means.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at claim 16 An electronic credit card in accordance with claim 1, wherein the communication means includes a radio frequency transfer means. Ong '610 at claim 21 . An electronic credit card in accordance with claim 6, wherein the storage means stores transaction details and a processor means is provided to calculate the funds available from the financial limit. *See also* 1[c] and claim 5 above. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	Ong '610 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: *See* above at [1d]. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Ong '610 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Ong '610 at Abstract

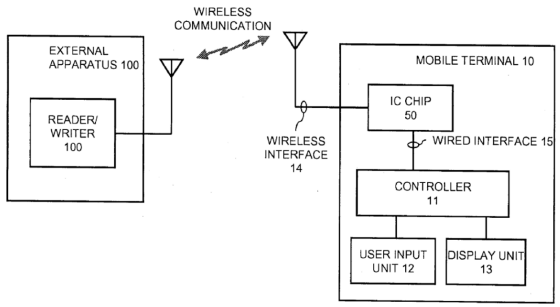
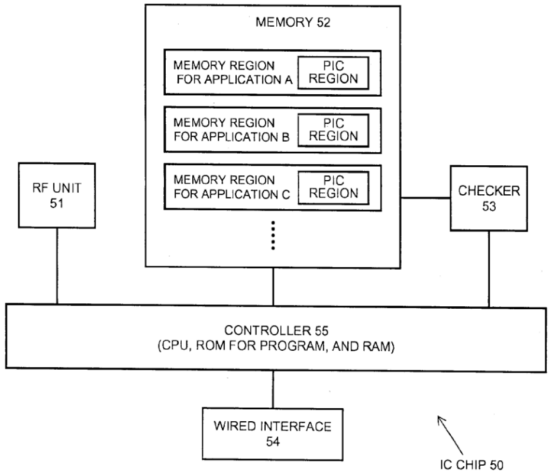
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Electronic Credit Card (ECC) is an electronic device that enables transmission/reception of data and/or digital information to/from a host computer via a Terminal Station (TS). TS includes Teller Machines in supermarkets/shopping complex, Automatic Teller Machines (ATM), EFTPOS devices and proprietary transceiver devices developed by Creative On-Line Technologies Limited for PC interface. It provides latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong '610 at [0019] Preferably the storage means is arranged to store a financial limit for transactions that the electronic credit card may be used for. Preferably the financial limit is provided to the transaction station by the communication means. Alternatively the electronic credit card including a processor means for keeping track of the use of the electronic credit card and will not generate or provide the authorisation code if the financial limit is exceeded. Alternatively the financial limit may be retrieved via the transaction station from a financial institution. Ong '610 at [0021] Preferably the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong '610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong '610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Ong '610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 21 . An electronic credit card in accordance with claim 6, wherein the storage means stores transaction details and a processor means is provided to calculate the funds available from the financial limit. *See also* claim 8 above. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Ong '610 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example: *See* above at claim 3. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Ong '610 discloses or renders obvious "[t]he mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: *See* above at row 2. To the extent this limitation is not disclosed by Ong '610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong '610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,202,156 ("the '156 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Yamagata '839 and (b) under 35 U.S.C. § 103(a) as obvious over Yamagata '839 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit E and Exhibits E1–E9, the contents of which are hereby incorporated by reference into this chart. One of ordinary skill in the art, as of the priority date of the '156 patent, would have known to combine the prior art elements disclosed by the foregoing references using known methods, and to use these elements according to their established functions in order to achieve a known and predictable result.

Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '156 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	**Exemplary Citations to US20030174839A1 ("Yamagata '839")**
1[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Yamagata '839 discloses or renders obvious "[a] mobile device." For example: Yamagata '839 at Abstract A memory region on an IC card has a hierarchical structure. Each application allocated on the memory region is registered in a directory, and the memory region is managed in directory units. A personal identification code is set for each application and directory, and the access right is controlled in application units or directory units. If a mobile terminal is lost, the right to access each application in the IC card automatically disappears. Therefore, the right to access each application allocated to the memory region on the IC card is efficiently controlled. Yamagata '839 at Fig. 1

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 Yamagata '839 at Figure 11  FIG. 11 Yamagata '839 at Figure 16

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")

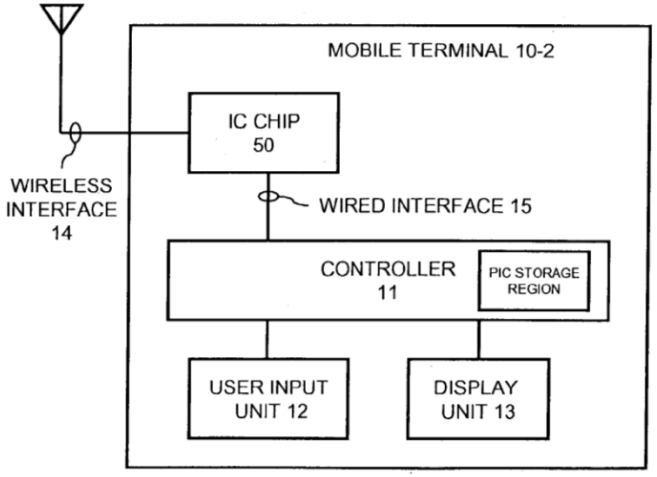


FIG. 16

Yamagata '839 at [0001]

> The present invention relates to information storage media with memory regions, IC chips with memory regions, information processing apparatuses having the IC chips with the memory regions, and memory management methods for the information storage media, and particularly relates to an information storage medium for use by being placed in an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium.

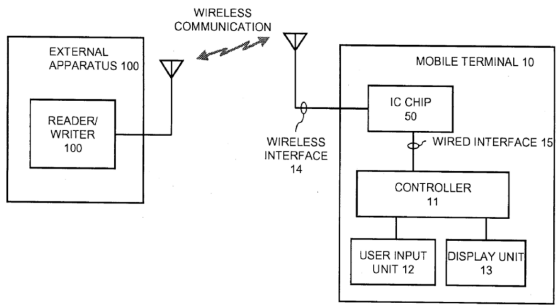
Yamagata '839 at [0002]–[0003]

> The present invention also relates to a mobile terminal having an IC chip placed therein, which is driven by receiving power using wireless communication with an external apparatus, and to an IC card for use in conjunction with the mobile terminal, and more particularly relates to a mobile terminal having an IC chip placed therein, which is driven by receiving power using wireless communication with an external apparatus and which has a memory function, a control method therefor, and an IC card with a memory function.

Yamagata '839 at [0004]

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	More particularly, the present invention relates to a mobile terminal in which one or more applications are allocated to a memory region on an IC chip, a control method therefor, and an IC card in which one or more applications are allocated to a memory region, and more particularly relates to a mobile terminal for controlling the right to access each application allocated to a memory region on an IC chip in application units, a control method therefor, and an IC card for controlling the right to access each application allocated to a memory region in application units. Yamagata '839 at [0017] It is another object of the present invention to provide an improved information storage medium for use by being placed on an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0025] The integrated circuit device according to the first aspect of the present invention is provided in the form of, for example, an IC chip. A cartridge which has the IC chip with an antenna and which is formed in the size of a credit card is generally referred to as an "IC card". The IC chip is used by being embedded in a mobile terminal such as a cellular phone or a PDA or in other information processing apparatuses. The IC card may be used by being inserted into an information processing apparatus. Applications for the IC chip or IC card include functions related to value information, such as prepaid electronic money or an electronic ticket. In the following description, the functions provided by the IC chip or IC card may also be referred to "applications". Yamagata '839 at [0039] According to a second aspect of the present invention, a mobile terminal apparatus is provided including: Yamagata '839 at [0064] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention is formed of, for example, an IC chip. The IC chip includes a wireless interface for establishing a wireless link with an external apparatus such as a reader/writer and a wired interface for establishing an internal connection with a controller of the mobile terminal apparatus having the IC chip. In response to establishment of a wireless link with the reader/writer, the IC chip is activated by electromagnetic waves sent from the reader/writer. Yamagata '839 at [0074]

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	FIG. 1 is a diagram schematically showing the hardware configuration of a mobile terminal 10 according to an embodiment of the present invention. Yamagata '839 at [0093] FIG. 1 schematically shows the hardware configuration of a mobile terminal 10 according to an embodiment of the present invention. The mobile terminal 10 is an information processing terminal, such as a cellular phone or a PDA (Personal Digital Assistant), which is small and light enough to be carried by a user. Yamagata '839 at [0094] The mobile terminal 10 shown in the diagram includes an IC chip 50 which is driven by receiving power using wireless communication with an external apparatus and which has a memory function, a controller 11 for controlling the overall internal operation of the mobile terminal 10, a user input unit 12 formed of keys/buttons for inputting by the user various character strings and commands, such as a personal identification number or password, and a display unit 13, such as an LCD (liquid Crystal Display), for displaying the processing result. Needless to say, the mobile terminal 10 may include peripheral units and circuit components other than those shown in the diagram in order to implement the primary function of the mobile terminal 10 Yamagata '839 at [0095] A cartridge which has an IC chip with an antenna and which is formed in the size of a credit card is generally referred to as an "IC card". Yamagata '839 at [0096] The mobile terminal 10 can be equipped with the IC chip 50 in a variety of different ways. For example, a semiconductor IC chip in conjunction with a wireless antenna may be embedded in the mobile terminal 10. Alternatively, a card-shaped IC chip, that is, an IC card, may be used by being inserted into a card slot arranged in the mobile terminal 10. Applications for the IC chip or IC card include functions related to value information, such as prepaid electronic money or an electronic ticket. In the following description, the functions provided by the IC chip or IC card may also be referred to "applications". Yamagata '839 at [0098] The IC chip 50 includes a wireless interface 14 for establishing a wireless link with an external apparatus 100 and a wired interface 15 for establishing a wired connection with the controller 11 of the mobile terminal 10. The wireless interface 14 uses, for example, a contact interface standard defined by ISO 7816

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	or a wireless interface standard defined by ISO 14443. The scheme for establishing a link or connection between the IC chip 50 and the external apparatus 100 will be described later. Yamagata '839 at [0161] FIG. 11 illustrates the internal functional configuration of an IC chip 50 embedded in a mobile terminal 10 according to a second embodiment of the present invention. Yamagata '839 at claim 24 24. A mobile terminal apparatus comprising: Yamagata '839 at claims 29–30 29. A mobile terminal apparatus according to claim 24, wherein the semiconductor integrated circuit device is driven by receiving power using wireless communication with the external apparatus. 30. A mobile terminal apparatus according to claim 29, wherein, in response to being connected to the external apparatus via the wireless interface and thus receiving power, the semiconductor integrated circuit device notifies via the wired interface of the necessity to input the personal identification code for accessing the memory region. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Yamagata '839 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: Yamagata '839 at Fig. 1 

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	Yamagata '839 at Figure 2

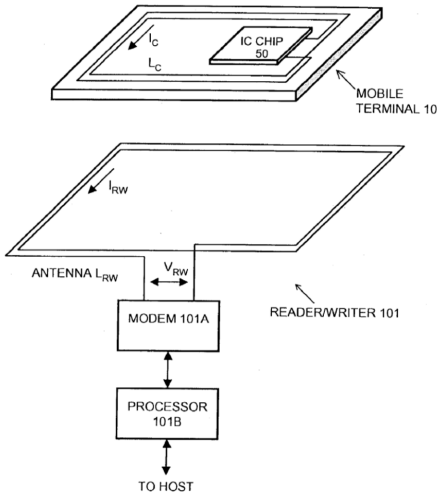


FIG. 2

Yamagata '839 at Figure 3

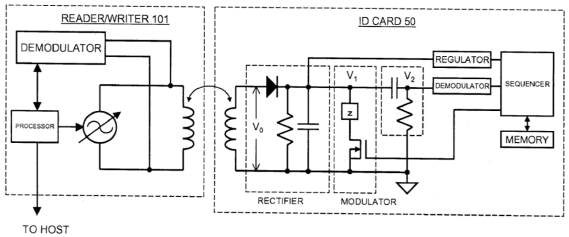
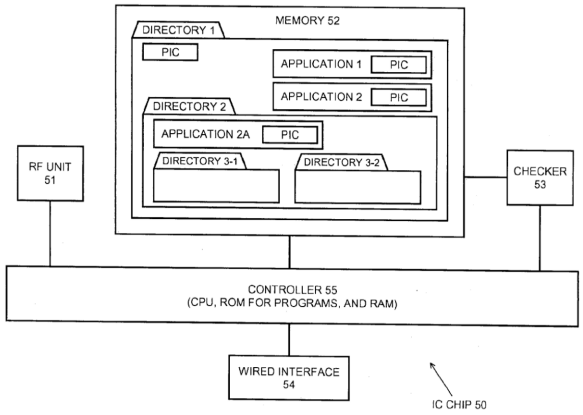
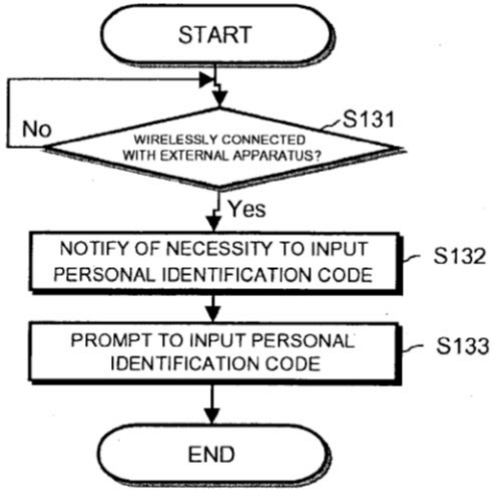


FIG. 3

Yamagata '839 at Figure 4

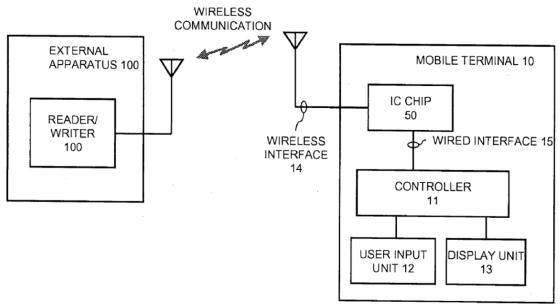
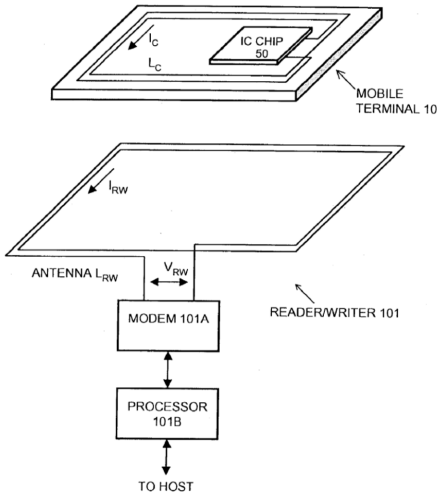
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 4 Yamagata '839 at Figure 15  FIG. 15 Yamagata '839 at [0042]

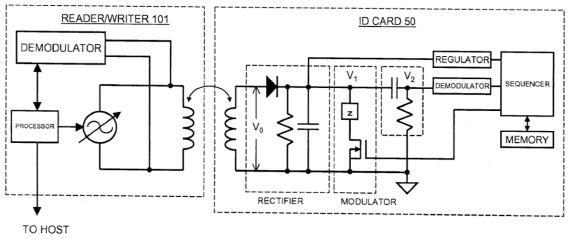
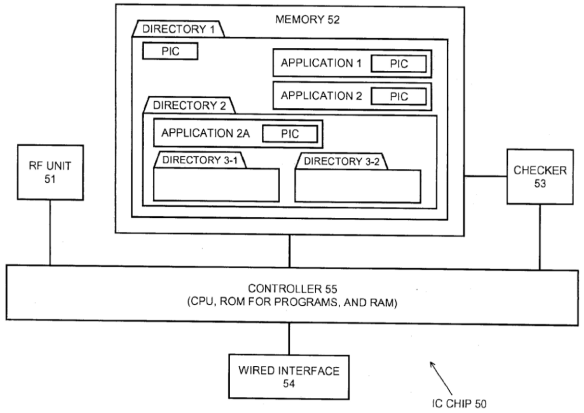
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	a wireless interface for enabling the semiconductor integrated circuit device to perform wireless communication with an external apparatus; Yamagata '839 at [0064] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention is formed of, for example, an IC chip. The IC chip includes a wireless interface for establishing a wireless link with an external apparatus such as a reader/writer and a wired interface for establishing an internal connection with a controller of the mobile terminal apparatus having the IC chip. In response to establishment of a wireless link with the reader/writer, the IC chip is activated by electromagnetic waves sent from the reader/writer. Yamagata '839 at [0107] Wireless communication between the reader/writer 101 and the IC chip 50 is implemented on the basis of, for example, the principle of electromagnetic induction. FIG. 2 conceptually depicts the mechanism of wireless communication between the reader/writer 101 and the IC chip 50 based on electromagnetic induction. The reader/writer 101 includes an antenna L_{RW} formed of a loop coil. Allowing electric current I_{RW} to flow through the antenna L_{RW} generates a magnetic field around the antenna L_{RW}. In contrast, at the IC chip 50 side, a loop coil L_C is provided around the IC chip 50 in an electrical sense. At the ends of the loop coil L_C of the IC chip 50, voltage is induced by the magnetic field generated by the loop antenna L_C of the reader/writer 101, and the induced voltage is input to a terminal of the IC chip 50 connected to the ends of the loop coil L_C. Yamagata '839 at [0108] The degree of coupling between the antenna L_{RW} of the reader/writer 101 and the loop coil L_C of the IC chip 50 changes depending on the positional relationship thereof. It can be regarded that, as a system, a single transformer is provided. This can be depicted in the model diagram shown in FIG. 3. Yamagata '839 at [0109] The reader/writer 101 modulates the current I_{RW} flowing through the antenna L_{RW} to modulate a voltage V_0 induced in the loop coil L_C of the IC chip. Using this phenomenon, the reader/writer 101 sends data to the IC chip 50. The data sent in this case includes a personal identification code, such as a personal identification number or password input from the user at the external apparatus 100 side, for obtaining the right to access each application or directory, and value information e.g., electronic money or an electronic ticket, provided by each application.

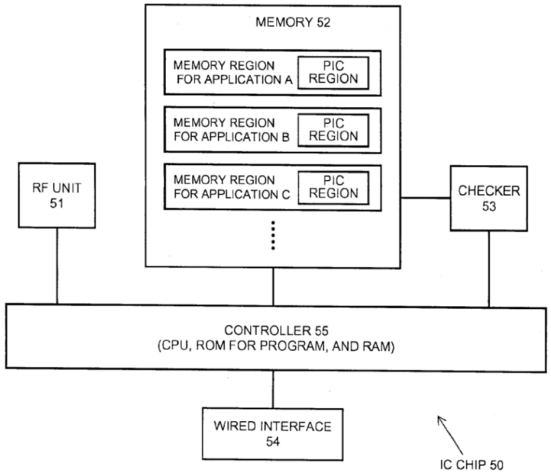
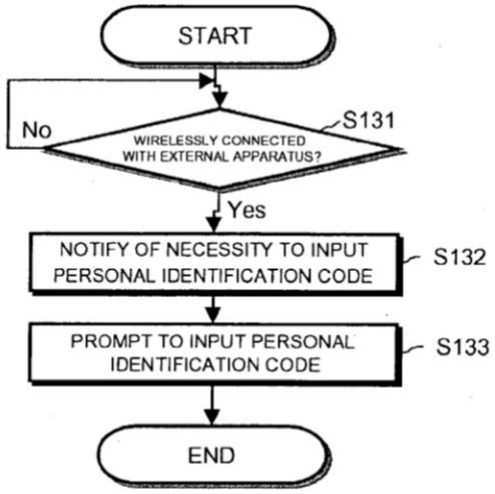
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	Yamagata '839 at [0110] The IC chip 50 has a load switching function for changing a load between terminals of the loop coil L_C in accordance with data to be sent to the reader/writer 101. When the load between the terminals of the loop coil L_C changes, the impedance between the antenna terminals of the reader/writer 101 changes. This results in a fluctuation in passing current I_{RW} or voltage V_{RW} of the antenna L_{RW}. Demodulation of the fluctuation enables the reader/writer 101 to receive the data sent from the IC chip 50. The data received by the external apparatus 100 from the IC chip 50 includes value information, such as electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner Yamagata '839 at [0117] The memory 52 is used to allocate a storage region to one or more applications. The memory 52 can be implemented as any type of readable/writable storage medium, such as a semiconductor memory or a magnetic stripe, and is not limited to a particular device. Yamagata '839 at [0186] FIG. 15 is a flowchart showing a process of prompting the user to input a personal identification code to the mobile terminal in response to establishment of a wireless link between the IC chip 50 and the external apparatus 100 via the RF unit 51 To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a memory to hold transaction data; and	Yamagata '839 discloses or renders obvious "a memory to hold transaction data." For example: Yamagata '839 at [0002]

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	More particularly, the present invention relates to an information storage medium in which one or more applications are allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium, and more particularly relates to an information storage medium for controlling the right to access each application allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0002]–[0003] The present invention also relates to a mobile terminal having an IC chip placed therein, which is driven by receiving power using wireless communication with an external apparatus, and to an IC card for use in conjunction with the mobile terminal, and more particularly relates to a mobile terminal having an IC chip placed therein, which is driven by receiving power using wireless communication with an external apparatus and which has a memory function, a control method therefor, and an IC card with a memory function. Yamagata '839 at [0004] More particularly, the present invention relates to a mobile terminal in which one or more applications are allocated to a memory region on an IC chip, a control method therefor, and an IC card in which one or more applications are allocated to a memory region, and more particularly relates to a mobile terminal for controlling the right to access each application allocated to a memory region on an IC chip in application units, a control method therefor, and an IC card for controlling the right to access each application allocated to a memory region in application units. Yamagata '839 at [0026] By allocating the memory region to each application in a hierarchical manner using directories, the memory allocating means or step manages the memory space in the IC card arranged as a hierarchical structure. Accordingly, correlated applications, such as a plurality of applications used in a series of transactions, are stored in the same directory to enable the user to efficiently classify and organize the applications. Yamagata '839 at [0065] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention has the memory region of relatively high capacity. One or more applications are allocated to the memory region. The right to access each application is controlled by the

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	personal identification code such as a personal identification number or password. The term application here includes value information, such as electronic money or an electronic ticket. Yamagata '839 at [0100] The IC chip 50 according to this embodiment has a memory region. Such a memory region is made possible by miniaturization technology. The memory region is formed of a semiconductor memory, a magnetic stripe, or other readable/writable storage media. One or more applications are allocated to the memory region. One example of application is value information, such as electronic money or an electronic ticket. Yamagata '839 at [0100]–[0101] In this embodiment, a memory space in the IC chip 50 has a hierarchical structure. Each application is allocated a directory. This enables applications to be efficiently managed in directory units. This will be described in detail later Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data;	Yamagata '839 discloses or renders obvious "a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents the transaction data." For example: Yamagata '839 at Fig. 1

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 Yamagata '839 at Figure 2  FIG. 2 Yamagata '839 at Figure 3

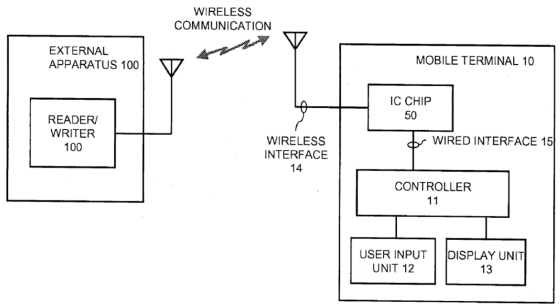
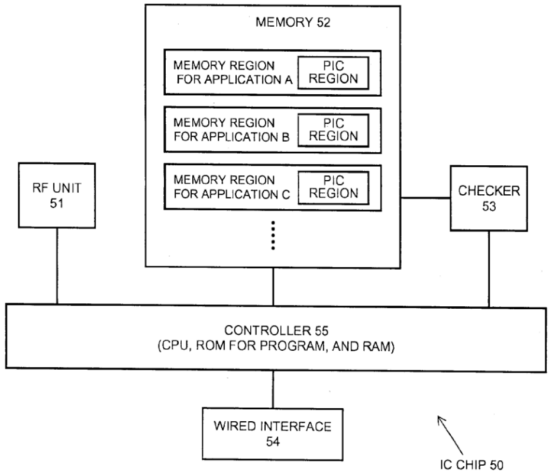
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 3 Yamagata '839 at Figure 4  FIG. 4 Yamagata '839 at Figure 11

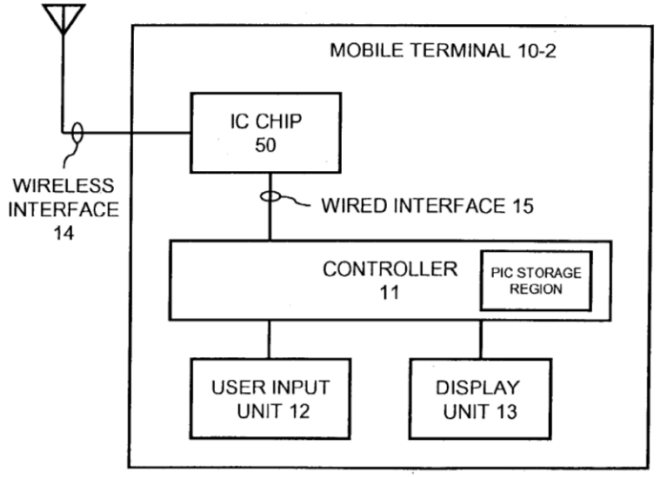
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 11 Yamagata '839 at Figure 15  FIG. 15

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	Yamagata '839 at [0002] More particularly, the present invention relates to an information storage medium in which one or more applications are allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium, and more particularly relates to an information storage medium for controlling the right to access each application allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0042] a wireless interface for enabling the semiconductor integrated circuit device to perform wireless communication with an external apparatus; Yamagata '839 at [0064] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention is formed of, for example, an IC chip. The IC chip includes a wireless interface for establishing a wireless link with an external apparatus such as a reader/writer and a wired interface for establishing an internal connection with a controller of the mobile terminal apparatus having the IC chip. In response to establishment of a wireless link with the reader/writer, the IC chip is activated by electromagnetic waves sent from the reader/writer. Yamagata '839 at [0094] The mobile terminal 10 shown in the diagram includes an IC chip 50 which is driven by receiving power using wireless communication with an external apparatus and which has a memory function, a controller 11 for controlling the overall internal operation of the mobile terminal 10, a user input unit 12 formed of keys/buttons for inputting by the user various character strings and commands, such as a personal identification number or password, and a display unit 13, such as an LCD (liquid Crystal Display), for displaying the processing result. Needless to say, the mobile terminal 10 may include peripheral units and circuit components other than those shown in the diagram in order to implement the primary function of the mobile terminal 10 Yamagata '839 at [0097]

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	The controller 11 is formed by integrating a CPU (Central Processing Unit), a ROM (Read Only Memory), a RAM (Random Access Memory), and the like. The controller 11 executes program code stored on the ROM to control various operations in the mobile terminal 10. Yamagata '839 at [0107] Wireless communication between the reader/writer 101 and the IC chip 50 is implemented on the basis of, for example, the principle of electromagnetic induction. FIG. 2 conceptually depicts the mechanism of wireless communication between the reader/writer 101 and the IC chip 50 based on electromagnetic induction. The reader/writer 101 includes an antenna L_{RW} formed of a loop coil. Allowing electric current I_{RW} to flow through the antenna L_{RW} generates a magnetic field around the antenna L_{RW}. In contrast, at the IC chip 50 side, a loop coil L_C is provided around the IC chip 50 in an electrical sense. At the ends of the loop coil L_C of the IC chip 50, voltage is induced by the magnetic field generated by the loop antenna L_C of the reader/writer 101, and the induced voltage is input to a terminal of the IC chip 50 connected to the ends of the loop coil L_C. Yamagata '839 at [0108] The degree of coupling between the antenna L_{RW} of the reader/writer 101 and the loop coil L_C of the IC chip 50 changes depending on the positional relationship thereof. It can be regarded that, as a system, a single transformer is provided. This can be depicted in the model diagram shown in FIG. 3. Yamagata '839 at [0109] The reader/writer 101 modulates the current I_{RW} flowing through the antenna L_{RW} to modulate a voltage V_0 induced in the loop coil L_C of the IC chip. Using this phenomenon, the reader/writer 101 sends data to the IC chip 50. The data sent in this case includes a personal identification code, such as a personal identification number or password input from the user at the external apparatus 100 side, for obtaining the right to access each application or directory, and value information e.g., electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0110] The IC chip 50 has a load switching function for changing a load between terminals of the loop coil L_C in accordance with data to be sent to the reader/writer 101. When the load between the terminals of the loop coil L_C changes, the impedance between the antenna terminals of the reader/writer 101 changes. This results in a fluctuation in passing current I_{RW} or voltage V_{RW} of the antenna L_{RW}. Demodulation of the fluctuation enables the reader/writer 101 to receive the data sent from the IC chip 50. The data received by

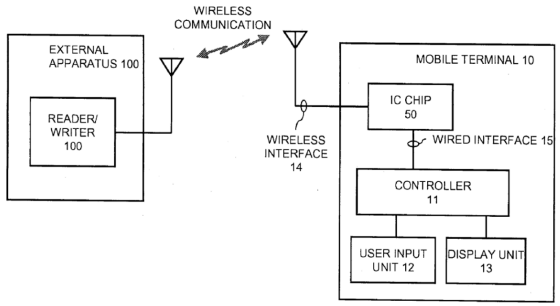
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	the external apparatus 100 from the IC chip 50 includes value information, such as electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner Yamagata '839 at [0117] The memory 52 is used to allocate a storage region to one or more applications. The memory 52 can be implemented as any type of readable/writable storage medium, such as a semiconductor memory or a magnetic stripe, and is not limited to a particular device. Yamagata '839 at [0163] The controller 55 is formed by integrating a CPU (Central Processing Unit), a ROM (Read Only Memory), a RAM (Random Access Memory), and the like. The controller 55 executes program code stored on the ROM to control the internal operation of the IC chip 50. Also, the controller 55 communicates with a controller 11 of the mobile terminal 10 via the wired interface 54. Yamagata '839 at [0186] FIG. 15 is a flowchart showing a process of prompting the user to input a personal identification code to the mobile terminal in response to establishment of a wireless link between the IC chip 50 and the external apparatus 100 via the RF unit 51 To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] wherein the mobile device comprises a mobile phone.	Yamagata '839 discloses or renders obvious "wherein the mobile device comprises a mobile phone." For example: Yamagata '839 at Fig. 1

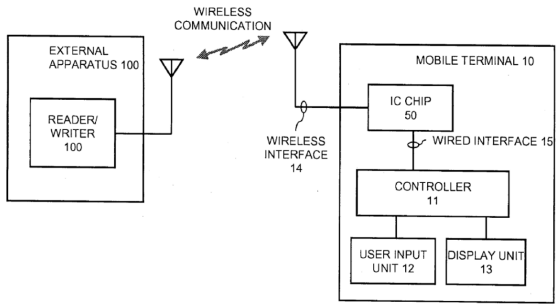
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 Yamagata '839 at Figure 11  FIG. 11 Yamagata '839 at Figure 16

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 16 Yamagata '839 at [0001] The present invention relates to information storage media with memory regions, IC chips with memory regions, information processing apparatuses having the IC chips with the memory regions, and memory management methods for the information storage media, and particularly relates to an information storage medium for use by being placed in an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0002]–[0003] The present invention also relates to a mobile terminal having an IC chip placed therein, which is driven by receiving power using wireless communication with an external apparatus, and to an IC card for use in conjunction with the mobile terminal, and more particularly relates to a mobile terminal having an IC chip placed therein, which is driven by receiving power using wireless communication with an external apparatus and which has a memory function, a control method therefor, and an IC card with a memory function. Yamagata '839 at [0004]

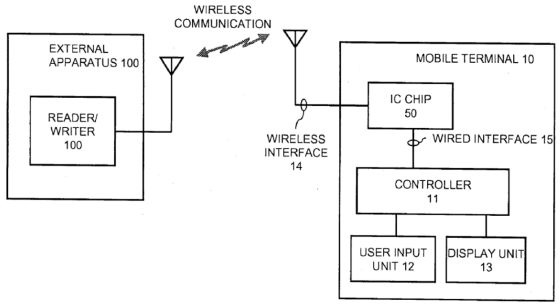
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	More particularly, the present invention relates to a mobile terminal in which one or more applications are allocated to a memory region on an IC chip, a control method therefor, and an IC card in which one or more applications are allocated to a memory region, and more particularly relates to a mobile terminal for controlling the right to access each application allocated to a memory region on an IC chip in application units, a control method therefor, and an IC card for controlling the right to access each application allocated to a memory region in application units. Yamagata '839 at [0017] It is another object of the present invention to provide an improved information storage medium for use by being placed on an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0025] The integrated circuit device according to the first aspect of the present invention is provided in the form of, for example, an IC chip. A cartridge which has the IC chip with an antenna and which is formed in the size of a credit card is generally referred to as an "IC card". The IC chip is used by being embedded in a mobile terminal such as a cellular phone or a PDA or in other information processing apparatuses. The IC card may be used by being inserted into an information processing apparatus. Applications for the IC chip or IC card include functions related to value information, such as prepaid electronic money or an electronic ticket. In the following description, the functions provided by the IC chip or IC card may also be referred to "applications". Yamagata '839 at [0039] According to a second aspect of the present invention, a mobile terminal apparatus is provided including: Yamagata '839 at [0047] The term mobile terminal apparatus here indicates an information processing apparatus, such as a cellular phone or a PDA (Personal Digital Assistant), which is small and light enough to be carried by the user. Also, the term semiconductor integrated circuit device indicates an IC chip with an authentication function for implementing the access operation. Yamagata '839 at [0064] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention is formed of, for example, an IC chip. The IC chip includes a wireless

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	interface for establishing a wireless link with an external apparatus such as a reader/writer and a wired interface for establishing an internal connection with a controller of the mobile terminal apparatus having the IC chip. In response to establishment of a wireless link with the reader/writer, the IC chip is activated by electromagnetic waves sent from the reader/writer. Yamagata '839 at [0093] FIG. 1 schematically shows the hardware configuration of a mobile terminal 10 according to an embodiment of the present invention. The mobile terminal 10 is an information processing terminal, such as a cellular phone or a PDA (Personal Digital Assistant), which is small and light enough to be carried by a user. Yamagata '839 at [0094] The mobile terminal 10 shown in the diagram includes an IC chip 50 which is driven by receiving power using wireless communication with an external apparatus and which has a memory function, a controller 11 for controlling the overall internal operation of the mobile terminal 10, a user input unit 12 formed of keys/buttons for inputting by the user various character strings and commands, such as a personal identification number or password, and a display unit 13, such as an LCD (liquid Crystal Display), for displaying the processing result. Needless to say, the mobile terminal 10 may include peripheral units and circuit components other than those shown in the diagram in order to implement the primary function of the mobile terminal 10 Yamagata '839 at [0096] The mobile terminal 10 can be equipped with the IC chip 50 in a variety of different ways. For example, a semiconductor IC chip in conjunction with a wireless antenna may be embedded in the mobile terminal 10. Alternatively, a card-shaped IC chip, that is, an IC card, may be used by being inserted into a card slot arranged in the mobile terminal 10. Applications for the IC chip or IC card include functions related to value information, such as prepaid electronic money or an electronic ticket. In the following description, the functions provided by the IC chip or IC card may also be referred to "applications". Yamagata '839 at [0161] FIG. 11 illustrates the internal functional configuration of an IC chip 50 embedded in a mobile terminal 10 according to a second embodiment of the present invention. Yamagata '839 at claim 24 24. A mobile terminal apparatus comprising:

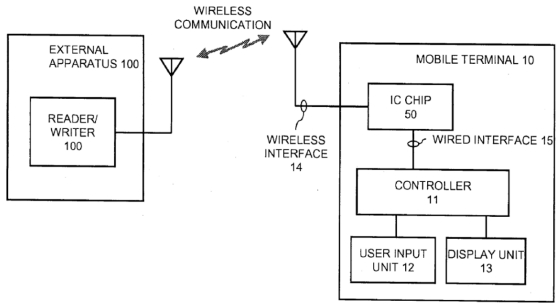
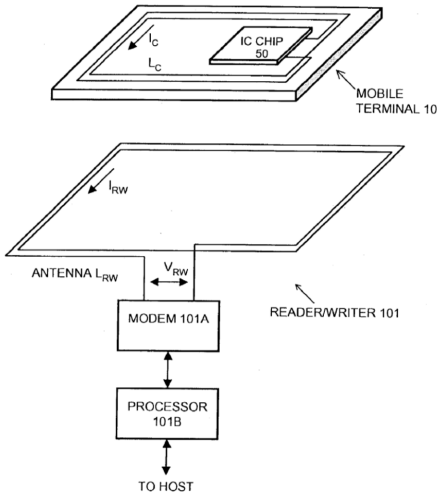
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	Yamagata '839 at claims 29–30 29. A mobile terminal apparatus according to claim 24, wherein the semiconductor integrated circuit device is driven by receiving power using wireless communication with the external apparatus. 30. A mobile terminal apparatus according to claim 29, wherein, in response to being connected to the external apparatus via the wireless interface and thus receiving power, the semiconductor integrated circuit device notifies via the wired interface of the necessity to input the personal identification code for accessing the memory region. *See also* 1[pre] above. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: Yamagata '839 at Fig. 1  Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal

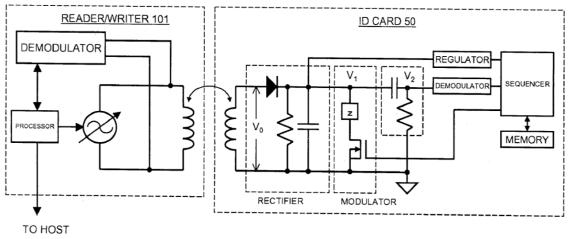
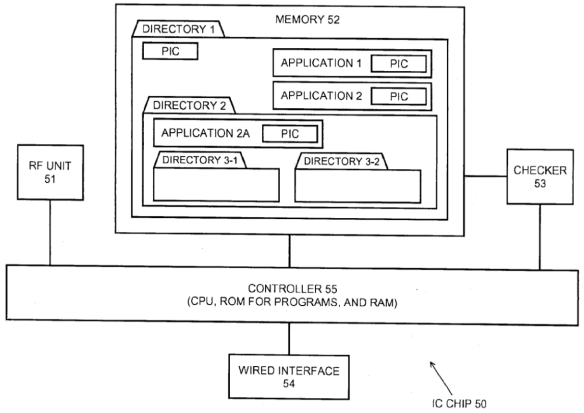
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner Yamagata '839 at [0117] The memory 52 is used to allocate a storage region to one or more applications. The memory 52 can be implemented as any type of readable/writable storage medium, such as a semiconductor memory or a magnetic stripe, and is not limited to a particular device. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
3. The mobile device of claim 1 wherein the transaction data comprises financial data.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 1 wherein the transaction data comprises financial data." For example: Yamagata '839 at Fig. 1  Yamagata '839 at [0065] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention has the memory region of relatively high capacity. One or more applications are allocated to the memory region. The right to access each application is controlled by the personal identification code such as a personal identification number or password. The term application here includes value information, such as electronic money or an electronic ticket. Yamagata '839 at [0100]

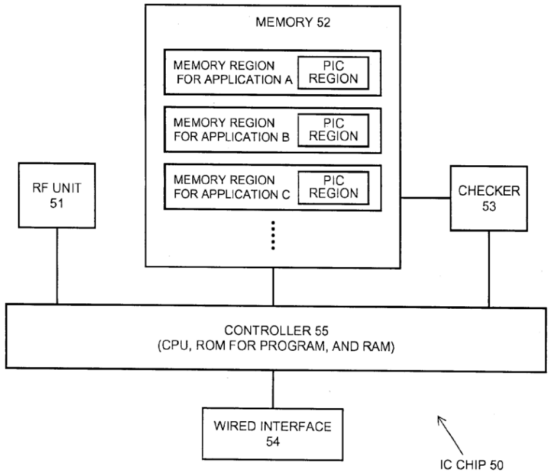
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	The IC chip 50 according to this embodiment has a memory region. Such a memory region is made possible by miniaturization technology. The memory region is formed of a semiconductor memory, a magnetic stripe, or other readable/writable storage media. One or more applications are allocated to the memory region. One example of application is value information, such as electronic money or an electronic ticket. Yamagata '839 at [0109] The reader/writer 101 modulates the current I_{RW} flowing through the antenna L_{RW} to modulate a voltage V_0 induced in the loop coil L_C of the IC chip. Using this phenomenon, the reader/writer 101 sends data to the IC chip 50. The data sent in this case includes a personal identification code, such as a personal identification number or password input from the user at the external apparatus 100 side, for obtaining the right to access each application or directory, and value information e.g., electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0110] The IC chip 50 has a load switching function for changing a load between terminals of the loop coil L_C in accordance with data to be sent to the reader/writer 101. When the load between the terminals of the loop coil L_C changes, the impedance between the antenna terminals of the reader/writer 101 changes. This results in a fluctuation in passing current I_{RW} or voltage V_{RW} of the antenna L_{RW}. Demodulation of the fluctuation enables the reader/writer 101 to receive the data sent from the IC chip 50. The data received by the external apparatus 100 from the IC chip 50 includes value information, such as electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
4. The mobile device of claim 3 wherein the financial data comprises credit card data.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 3 wherein the financial data comprises credit card data." For example: Yamagata '839 at Fig. 1  Yamagata '839 at [0065] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention has the memory region of relatively high capacity. One or more applications are allocated to the memory region. The right to access each application is controlled by the personal identification code such as a personal identification number or password. The term application here includes value information, such as electronic money or an electronic ticket. Yamagata '839 at [0100] The IC chip 50 according to this embodiment has a memory region. Such a memory region is made possible by miniaturization technology. The memory region is formed of a semiconductor memory, a magnetic stripe, or other readable/writable storage media. One or more applications are allocated to the memory region. One example of application is value information, such as electronic money or an electronic ticket. Yamagata '839 at [0109] The reader/writer 101 modulates the current I_{RW} flowing through the antenna L_{RW} to modulate a voltage V_0 induced in the loop coil L_C of the IC chip. Using this phenomenon, the reader/writer 101 sends data to the IC chip 50. The data sent in this case includes a personal identification code, such as a personal identification number or password input from the user at the external apparatus 100 side, for obtaining the

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	right to access each application or directory, and value information e.g., electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0110] The IC chip 50 has a load switching function for changing a load between terminals of the loop coil L_C in accordance with data to be sent to the reader/writer 101. When the load between the terminals of the loop coil L_C changes, the impedance between the antenna terminals of the reader/writer 101 changes. This results in a fluctuation in passing current I_{RW} or voltage V_{RW} of the antenna L_{RW}. Demodulation of the fluctuation enables the reader/writer 101 to receive the data sent from the IC chip 50. The data received by the external apparatus 100 from the IC chip 50 includes value information, such as electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 3 above.
5. The mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 1 further comprising smartcard circuitry coupled to the memory and the processor." For example: Yamagata '839 at Abstract A memory region on an IC card has a hierarchical structure. Each application allocated on the memory region is registered in a directory, and the memory region is managed in directory units. A personal identification code is set for each application and directory, and the access right is controlled in application units or directory units. If a mobile terminal is lost, the right to access each application in the IC card automatically disappears. Therefore, the right to access each application allocated to the memory region on the IC card is efficiently controlled.

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	Yamagata '839 at Fig. 1  Yamagata '839 at Figure 2  FIG. 2 Yamagata '839 at Figure 3

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 3 Yamagata '839 at Figure 4  FIG. 4 Yamagata '839 at Figure 11

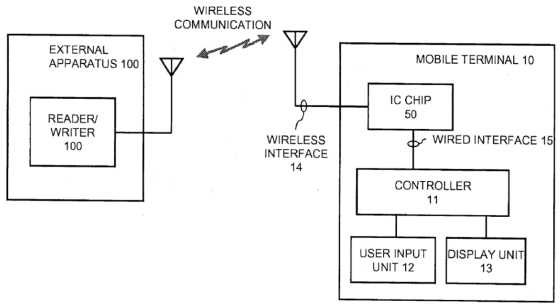
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 11 Yamagata '839 at [0001] The present invention relates to information storage media with memory regions, IC chips with memory regions, information processing apparatuses having the IC chips with the memory regions, and memory management methods for the information storage media, and particularly relates to an information storage medium for use by being placed in an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0002] More particularly, the present invention relates to an information storage medium in which one or more applications are allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium, and more particularly relates to an information storage medium for controlling the right to access each application allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium.

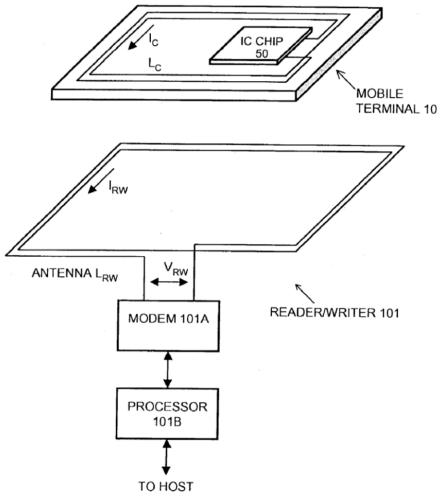
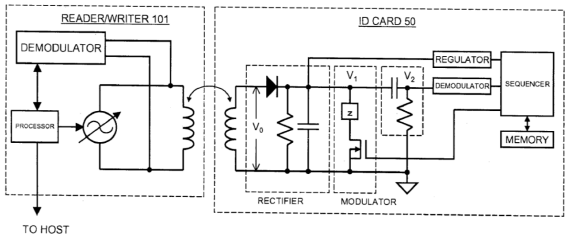
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	Yamagata '839 at [0016] It is an object of the present invention to provide an improved information storage medium with a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0017] It is another object of the present invention to provide an improved information storage medium for use by being placed on an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0025] The integrated circuit device according to the first aspect of the present invention is provided in the form of, for example, an IC chip. A cartridge which has the IC chip with an antenna and which is formed in the size of a credit card is generally referred to as an "IC card". The IC chip is used by being embedded in a mobile terminal such as a cellular phone or a PDA or in other information processing apparatuses. The IC card may be used by being inserted into an information processing apparatus. Applications for the IC chip or IC card include functions related to value information, such as prepaid electronic money or an electronic ticket. In the following description, the functions provided by the IC chip or IC card may also be referred to "applications". Yamagata '839 at [0026] By allocating the memory region to each application in a hierarchical manner using directories, the memory allocating means or step manages the memory space in the IC card arranged as a hierarchical structure. Accordingly, correlated applications, such as a plurality of applications used in a series of transactions, are stored in the same directory to enable the user to efficiently classify and organize the applications. Yamagata '839 at [0027] When an external apparatus has a card reader, the external apparatus can access the IC chip via a wireless interface. The right to access the memory region in the IC chip or the like is controlled by matching of personal identification codes. A personal identification code may be input using an information processing apparatus having embedded therein the IC chip to disengage the lock. Subsequently, a wireless link may be established, and access to the memory region may be permitted. Alternatively, after a wireless

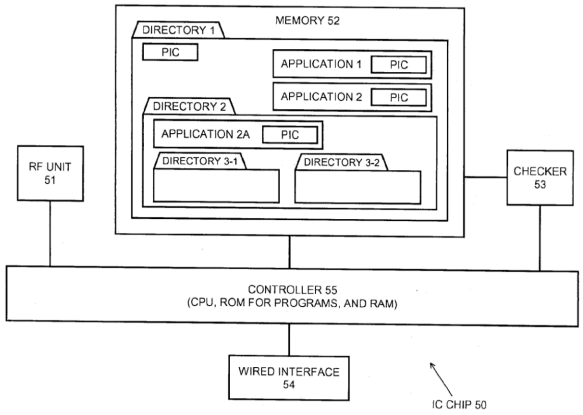
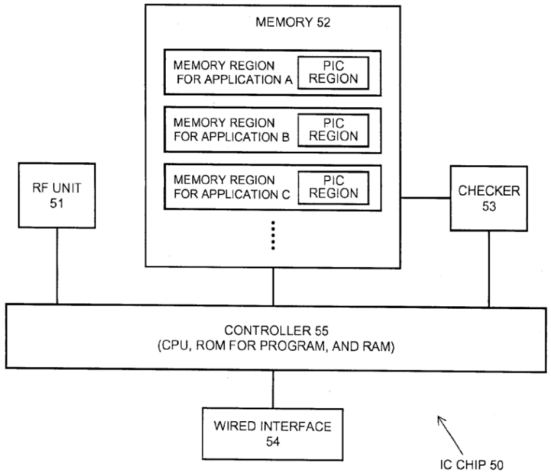
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	link between the IC chip in the information processing apparatus and the external apparatus is established, the access right is controlled on the basis of a personal identification code input using the external apparatus. Yamagata '839 at [0039]–[0040] a semiconductor integrated circuit device having a memory region; Yamagata '839 at [0064] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention is formed of, for example, an IC chip. The IC chip includes a wireless interface for establishing a wireless link with an external apparatus such as a reader/writer and a wired interface for establishing an internal connection with a controller of the mobile terminal apparatus having the IC chip. In response to establishment of a wireless link with the reader/writer, the IC chip is activated by electromagnetic waves sent from the reader/writer. Yamagata '839 at [0097] The controller 11 is formed by integrating a CPU (Central Processing Unit), a ROM (Read Only Memory), a RAM (Random Access Memory), and the like. The controller 11 executes program code stored on the ROM to control various operations in the mobile terminal 10. Yamagata '839 at [0098] The IC chip 50 includes a wireless interface 14 for establishing a wireless link with an external apparatus 100 and a wired interface 15 for establishing a wired connection with the controller 11 of the mobile terminal 10. The wireless interface 14 uses, for example, a contact interface standard defined by ISO 7816 or a wireless interface standard defined by ISO 14443. The scheme for establishing a link or connection between the IC chip 50 and the external apparatus 100 will be described later. Yamagata '839 at [0100] The IC chip 50 according to this embodiment has a memory region. Such a memory region is made possible by miniaturization technology. The memory region is formed of a semiconductor memory, a magnetic stripe, or other readable/writable storage media. One or more applications are allocated to the memory region. One example of application is value information, such as electronic money or an electronic ticket. Yamagata '839 at [0100]–[0101]

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	In this embodiment, a memory space in the IC chip 50 has a hierarchical structure. Each application is allocated a directory. This enables applications to be efficiently managed in directory units. This will be described in detail later Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner Yamagata '839 at [0162] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with a reader/writer 101 of an external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner. Yamagata '839 at [0163] The controller 55 is formed by integrating a CPU (Central Processing Unit), a ROM (Read Only Memory), a RAM (Random Access Memory), and the like. The controller 55 executes program code stored on the ROM to control the internal operation of the IC chip 50. Also, the controller 55 communicates with a controller 11 of the mobile terminal 10 via the wired interface 54. Yamagata '839 at claim 1 1. An integrated circuit device comprising: a memory region; Yamagata '839 at claim 13 An information processing apparatus according to claim 12, wherein the information storage medium is a storage medium in the form of an IC card. Yamagata '839 at claim 24

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	a semiconductor integrated circuit device having a memory region; To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8. The mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Yamagata '839 at [0110] The IC chip 50 has a load switching function for changing a load between terminals of the loop coil L_C in accordance with data to be sent to the reader/writer 101. When the load between the terminals of the loop coil L_C changes, the impedance between the antenna terminals of the reader/writer 101 changes. This results in a fluctuation in passing current I_{RW} or voltage V_{RW} of the antenna L_{RW}. Demodulation of the fluctuation enables the reader/writer 101 to receive the data sent from the IC chip 50. The data received by the external apparatus 100 from the IC chip 50 includes value information, such as electronic money or an electronic ticket, provided by each application. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
9[pre]. A mobile device comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Yamagata '839 discloses or renders obvious "[a] mobile device." For example: *See* above at 1[pre]. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	Yamagata '839 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." For example: *See* above at [1a].

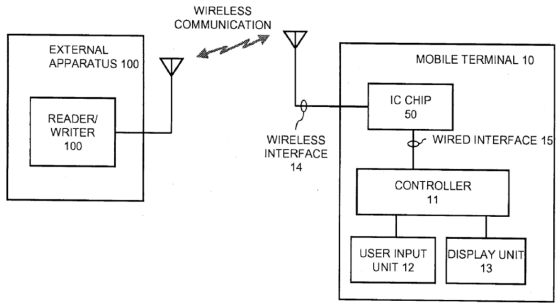
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9b] smartcard circuitry for performing transactions; and	Yamagata '839 discloses or renders obvious "smartcard circuitry for performing transactions." For example: Yamagata '839 at Abstract A memory region on an IC card has a hierarchical structure. Each application allocated on the memory region is registered in a directory, and the memory region is managed in directory units. A personal identification code is set for each application and directory, and the access right is controlled in application units or directory units. If a mobile terminal is lost, the right to access each application in the IC card automatically disappears. Therefore, the right to access each application allocated to the memory region on the IC card is efficiently controlled. Yamagata '839 at Fig. 1  Yamagata '839 at Figure 2

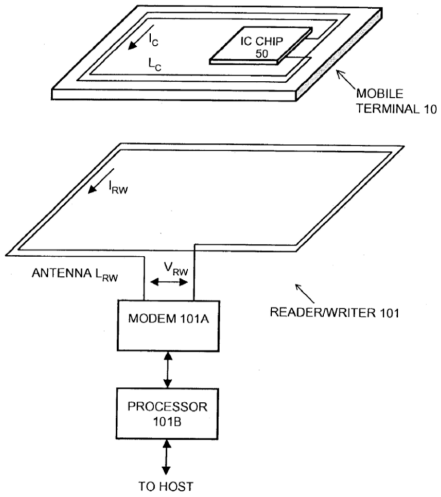
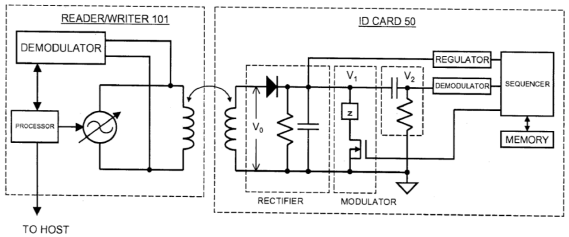
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 2 Yamagata '839 at Figure 3  FIG. 3 Yamagata '839 at Figure 4

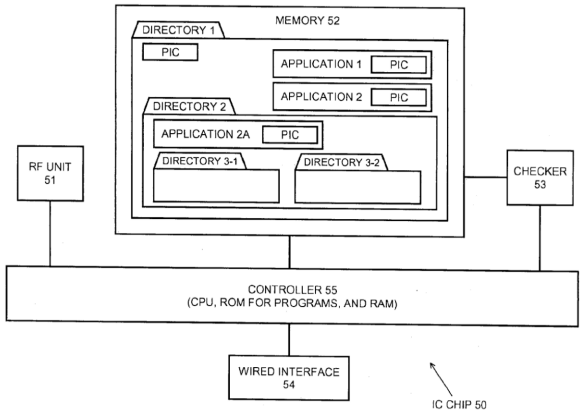
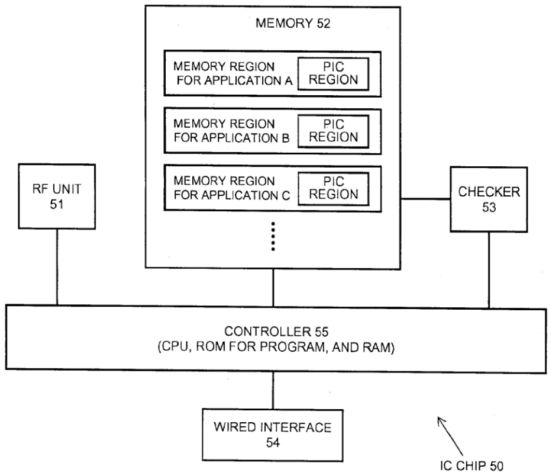
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 4 Yamagata '839 at Figure 11  FIG. 11 Yamagata '839 at [0001]

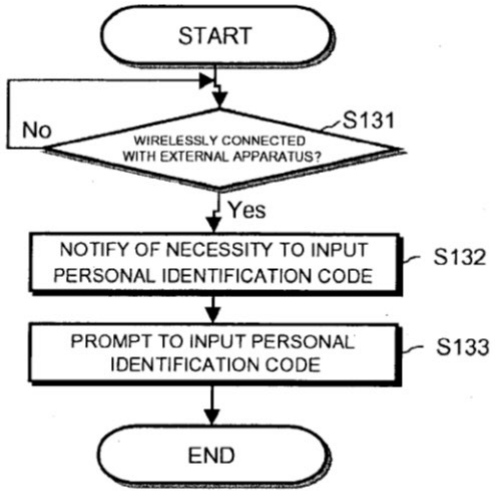
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	The present invention relates to information storage media with memory regions, IC chips with memory regions, information processing apparatuses having the IC chips with the memory regions, and memory management methods for the information storage media, and particularly relates to an information storage medium for use by being placed in an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0016] It is an object of the present invention to provide an improved information storage medium with a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0017] It is another object of the present invention to provide an improved information storage medium for use by being placed on an information processing apparatus such as a cellular phone or a PDA (Personal Digital Assistant), an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0025] The integrated circuit device according to the first aspect of the present invention is provided in the form of, for example, an IC chip. A cartridge which has the IC chip with an antenna and which is formed in the size of a credit card is generally referred to as an "IC card". The IC chip is used by being embedded in a mobile terminal such as a cellular phone or a PDA or in other information processing apparatuses. The IC card may be used by being inserted into an information processing apparatus. Applications for the IC chip or IC card include functions related to value information, such as prepaid electronic money or an electronic ticket. In the following description, the functions provided by the IC chip or IC card may also be referred to "applications". Yamagata '839 at [0027] When an external apparatus has a card reader, the external apparatus can access the IC chip via a wireless interface. The right to access the memory region in the IC chip or the like is controlled by matching of personal identification codes. A personal identification code may be input using an information processing apparatus having embedded therein the IC chip to disengage the lock. Subsequently, a wireless link may be established, and access to the memory region may be permitted. Alternatively, after a wireless

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	link between the IC chip in the information processing apparatus and the external apparatus is established, the access right is controlled on the basis of a personal identification code input using the external apparatus. Yamagata '839 at [0039]–[0040] a semiconductor integrated circuit device having a memory region; Yamagata '839 at [0064] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention is formed of, for example, an IC chip. The IC chip includes a wireless interface for establishing a wireless link with an external apparatus such as a reader/writer and a wired interface for establishing an internal connection with a controller of the mobile terminal apparatus having the IC chip. In response to establishment of a wireless link with the reader/writer, the IC chip is activated by electromagnetic waves sent from the reader/writer. Yamagata '839 at [0098] The IC chip 50 includes a wireless interface 14 for establishing a wireless link with an external apparatus 100 and a wired interface 15 for establishing a wired connection with the controller 11 of the mobile terminal 10. The wireless interface 14 uses, for example, a contact interface standard defined by ISO 7816 or a wireless interface standard defined by ISO 14443. The scheme for establishing a link or connection between the IC chip 50 and the external apparatus 100 will be described later. Yamagata '839 at [0162] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with a reader/writer 101 of an external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner. Yamagata '839 at claim 1 1. An integrated circuit device comprising: a memory region; Yamagata '839 at claim 13

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	An information processing apparatus according to claim 12, wherein the information storage medium is a storage medium in the form of an IC card. Yamagata '839 at claim 24 a semiconductor integrated circuit device having a memory region; *See also* claims 5 and 8 above. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field;	Yamagata '839 discloses or renders obvious "a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field." For example: Yamagata '839 at Fig. 1  Yamagata '839 at Figure 2

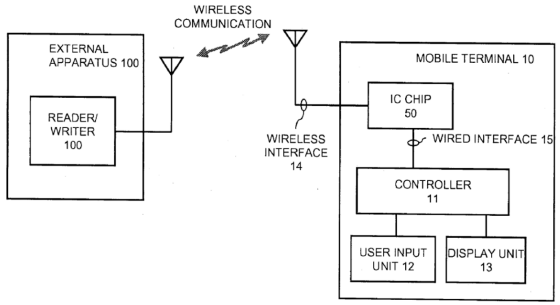
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 2 Yamagata '839 at Figure 3  FIG. 3 Yamagata '839 at Figure 4

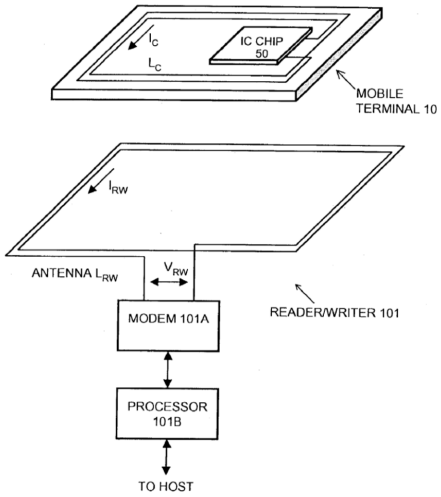
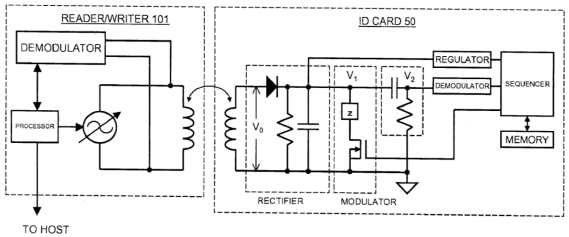
Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 4 Yamagata '839 at Figure 11  FIG. 11 Yamagata '839 at Figure 15

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 15 Yamagata '839 at [0002] More particularly, the present invention relates to an information storage medium in which one or more applications are allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium, and more particularly relates to an information storage medium for controlling the right to access each application allocated to a memory region, an IC chip with a memory region, an information processing apparatus having the IC chip with the memory region, and a memory management method for the information storage medium. Yamagata '839 at [0042] a wireless interface for enabling the semiconductor integrated circuit device to perform wireless communication with an external apparatus; Yamagata '839 at [0064] The semiconductor integrated circuit device placed on the mobile terminal apparatus according to the third aspect of the present invention is formed of, for example, an IC chip. The IC chip includes a wireless interface for establishing a wireless link with an external apparatus such as a reader/writer and a wired interface for establishing an internal connection with a controller of the mobile terminal apparatus having

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	the IC chip. In response to establishment of a wireless link with the reader/writer, the IC chip is activated by electromagnetic waves sent from the reader/writer. Yamagata '839 at [0094] The mobile terminal 10 shown in the diagram includes an IC chip 50 which is driven by receiving power using wireless communication with an external apparatus and which has a memory function, a controller 11 for controlling the overall internal operation of the mobile terminal 10, a user input unit 12 formed of keys/buttons for inputting by the user various character strings and commands, such as a personal identification number or password, and a display unit 13, such as an LCD (liquid Crystal Display), for displaying the processing result. Needless to say, the mobile terminal 10 may include peripheral units and circuit components other than those shown in the diagram in order to implement the primary function of the mobile terminal 10 Yamagata '839 at [0097] The controller 11 is formed by integrating a CPU (Central Processing Unit), a ROM (Read Only Memory), a RAM (Random Access Memory), and the like. The controller 11 executes program code stored on the ROM to control various operations in the mobile terminal 10. Yamagata '839 at [0107] Wireless communication between the reader/writer 101 and the IC chip 50 is implemented on the basis of, for example, the principle of electromagnetic induction. FIG. 2 conceptually depicts the mechanism of wireless communication between the reader/writer 101 and the IC chip 50 based on electromagnetic induction. The reader/writer 101 includes an antenna L_{RW} formed of a loop coil. Allowing electric current I_{RW} to flow through the antenna L_{RW} generates a magnetic field around the antenna L_{RW}. In contrast, at the IC chip 50 side, a loop coil L_C is provided around the IC chip 50 in an electrical sense. At the ends of the loop coil L_C of the IC chip 50, voltage is induced by the magnetic field generated by the loop antenna L_C of the reader/writer 101, and the induced voltage is input to a terminal of the IC chip 50 connected to the ends of the loop coil L_C. Yamagata '839 at [0108] The degree of coupling between the antenna L_{RW} of the reader/writer 101 and the loop coil L_C of the IC chip 50 changes depending on the positional relationship thereof. It can be regarded that, as a system, a single transformer is provided. This can be depicted in the model diagram shown in FIG. 3. Yamagata '839 at [0109]

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	The reader/writer 101 modulates the current I_{RW} flowing through the antenna L_{RW} to modulate a voltage V_0 induced in the loop coil L_C of the IC chip. Using this phenomenon, the reader/writer 101 sends data to the IC chip 50. The data sent in this case includes a personal identification code, such as a personal identification number or password input from the user at the external apparatus 100 side, for obtaining the right to access each application or directory, and value information e.g., electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0110] The IC chip 50 has a load switching function for changing a load between terminals of the loop coil L_C in accordance with data to be sent to the reader/writer 101. When the load between the terminals of the loop coil L_C changes, the impedance between the antenna terminals of the reader/writer 101 changes. This results in a fluctuation in passing current I_{RW} or voltage V_{RW} of the antenna L_{RW}. Demodulation of the fluctuation enables the reader/writer 101 to receive the data sent from the IC chip 50. The data received by the external apparatus 100 from the IC chip 50 includes value information, such as electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0115] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with the reader/writer 101 of the external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner Yamagata '839 at [0117] The memory 52 is used to allocate a storage region to one or more applications. The memory 52 can be implemented as any type of readable/writable storage medium, such as a semiconductor memory or a magnetic stripe, and is not limited to a particular device. Yamagata '839 at [0163] The controller 55 is formed by integrating a CPU (Central Processing Unit), a ROM (Read Only Memory), a RAM (Random Access Memory), and the like. The controller 55 executes program code stored on the ROM to control the internal operation of the IC chip 50. Also, the controller 55 communicates with a controller 11 of the mobile terminal 10 via the wired interface 54.

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	Yamagata '839 at [0186] FIG. 15 is a flowchart showing a process of prompting the user to input a personal identification code to the mobile terminal in response to establishment of a wireless link between the IC chip 50 and the external apparatus 100 via the RF unit 51 *See also* 1[c] and claim 5 above. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[9d] wherein the mobile device comprises a mobile phone.	*See* [1pre]. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Yamagata '839 at Fig. 1  Yamagata '839 at Figure 2

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	 FIG. 2 Yamagata '839 at Figure 3  FIG. 3 Yamagata '839 at Figure 11

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")

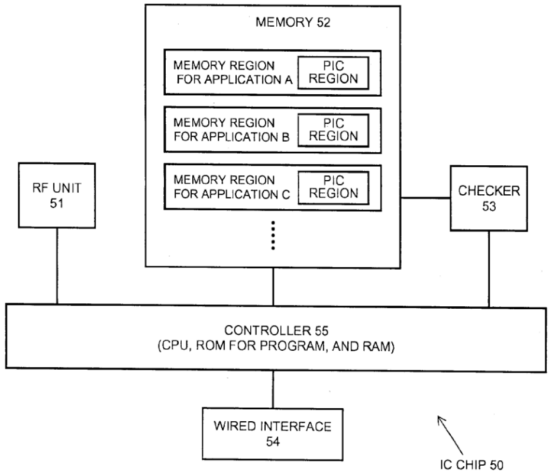


FIG. 11

Yamagata '839 at [0025]

> The integrated circuit device according to the first aspect of the present invention is provided in the form of, for example, an IC chip. A cartridge which has the IC chip with an antenna and which is formed in the size of a credit card is generally referred to as an "IC card". The IC chip is used by being embedded in a mobile terminal such as a cellular phone or a PDA or in other information processing apparatuses. The IC card may be used by being inserted into an information processing apparatus. Applications for the IC chip or IC card include functions related to value information, such as prepaid electronic money or an electronic ticket. In the following description, the functions provided by the IC chip or IC card may also be referred to "applications".

Yamagata '839 at [0027]

> When an external apparatus has a card reader, the external apparatus can access the IC chip via a wireless interface. The right to access the memory region in the IC chip or the like is controlled by matching of personal identification codes. A personal identification code may be input using an information processing apparatus having embedded therein the IC chip to disengage the lock. Subsequently, a wireless link may be established, and access to the memory region may be permitted. Alternatively, after a wireless link between the IC chip in the information processing apparatus and the external apparatus is established,

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	the access right is controlled on the basis of a personal identification code input using the external apparatus. Yamagata '839 at [0098] The IC chip 50 includes a wireless interface 14 for establishing a wireless link with an external apparatus 100 and a wired interface 15 for establishing a wired connection with the controller 11 of the mobile terminal 10. The wireless interface 14 uses, for example, a contact interface standard defined by ISO 7816 or a wireless interface standard defined by ISO 14443. The scheme for establishing a link or connection between the IC chip 50 and the external apparatus 100 will be described later. Yamagata '839 at [0107] Wireless communication between the reader/writer 101 and the IC chip 50 is implemented on the basis of, for example, the principle of electromagnetic induction. FIG. 2 conceptually depicts the mechanism of wireless communication between the reader/writer 101 and the IC chip 50 based on electromagnetic induction. The reader/writer 101 includes an antenna L_{RW} formed of a loop coil. Allowing electric current I_{RW} to flow through the antenna L_{RW} generates a magnetic field around the antenna L_{RW}. In contrast, at the IC chip 50 side, a loop coil L_C is provided around the IC chip 50 in an electrical sense. At the ends of the loop coil L_C of the IC chip 50, voltage is induced by the magnetic field generated by the loop antenna L_C of the reader/writer 101, and the induced voltage is input to a terminal of the IC chip 50 connected to the ends of the loop coil L_C. Yamagata '839 at [0109] The reader/writer 101 modulates the current I_{RW} flowing through the antenna L_{RW} to modulate a voltage V_0 induced in the loop coil L_C of the IC chip. Using this phenomenon, the reader/writer 101 sends data to the IC chip 50. The data sent in this case includes a personal identification code, such as a personal identification number or password input from the user at the external apparatus 100 side, for obtaining the right to access each application or directory, and value information e.g., electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0110] The IC chip 50 has a load switching function for changing a load between terminals of the loop coil L_C in accordance with data to be sent to the reader/writer 101. When the load between the terminals of the loop coil L_C changes, the impedance between the antenna terminals of the reader/writer 101 changes. This results in a fluctuation in passing current I_{RW} or voltage V_{RW} of the antenna L_{RW}. Demodulation of the fluctuation enables the reader/writer 101 to receive the data sent from the IC chip 50. The data received by

Claim Element	Exemplary Citations to US20030174839A1 ("Yamagata '839")
	the external apparatus 100 from the IC chip 50 includes value information, such as electronic money or an electronic ticket, provided by each application. Yamagata '839 at [0162] As shown in the diagram, the IC chip 50 includes an RF unit 51 having connected thereto an antenna for establishing a wireless link with a reader/writer 101 of an external apparatus 100, a memory 52 having a storage region individually allocated to each application, such as purchased-ticket information or depositor information (electronic money) at a bank, a checker 53 for comparing and checking a personal identification code, a wired interface 54, and a controller 55 for controlling the components in a general manner. *See also* claim 8 above. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
11. The mobile device of claim 9 wherein the transactions are financial transactions.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 9 wherein the transactions are financial transactions." For example: *See* above at claim 3. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.
12. The mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Yamagata '839 discloses or renders obvious "[t]he mobile device of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: *See* above at claim 2. To the extent this limitation is not disclosed by Yamagata '839, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Yamagata '839, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 9 above.

Patent Owner's Ex. 2020
Page 527