DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,208,423

EXHIBIT F

US7917444B1 ("Bursch '444"), WO2003015043A1 ("Codron '043"), US20040066273A1 ("Cortina '273"), US20060165060A1 ("Dua '060"), US6636833B1 ("Flitcroft '833"), US5943624A ("Fox"), JP2004295365A("Hanada '365"), US20010013542A1 ("Horowitz '542"), KR20000036744A ("Jo '744"), US5418837A ("Johansson '837"), US20050137986A1 ("Kean '986"), US20080194200A1 ("Keen '200"), US20070057073A1 ("Mamba '073"), JP2000115373A ("Oishi '373"), Contactless Payments ("SCAR PT-04002"), US20050187882A1 ("Sovio '882"), US20050015275A1 ("Takekawa '275"), US20030174839A1 ("Yamagata '839"), i-mode FeliCa ("Yoshinaga 2004"), and US20050097038A1 ("Yu '038")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,208,423 ("the '423 patent") are invalid (a) under 35 U.S.C. § 103 as obvious over each of Bursch '444, Codron '043, Cortina '273, Dua '060, Flitcroft '833, Fox '624, Hanada '365, Horowitz '542, Jo '744, Johansson '837, Kean '986, Keen '200, Mamba '073, Oishi '373, SCAR PT-04002, Sovio '882, Takekawa '275, Yamagata '839, Yoshinaga 2004, and Yu '038 and (b) under 35 U.S.C. § 103(a) as obvious over Bursch '444, Codron '043, Cortina '273, Dua '060, Flitcroft '833, Fox '624, Hanada '365, Horowitz '542, Jo '744, Johansson '837, Kean '986, Keen '200, Mamba '073, Oishi '373, SCAR PT-04002, Sovio '882, Takekawa '275, Yamagata '839, 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 F and Exhibits F1–F5, 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 '423 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 '423 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 phone 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. Cortina '273 at Fig. 4, Figure 12, [0006], [0026], [0096], [0097], [0130], [0131], [0132], [0133], [0137], [0139], [0202], claim 3, claim 4, claim 9, claim 10, claim 15, claim 16, and claim 19.

Patent Owner's Ex. 2021
Samsung v. iCashe (IPR2025-00644)
Page 001

Claim Element	Exemplary Citations
	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. Fox ’624 at Abstract, Fig. 1, Fig. 2, Fig. 4, Fig. 5, 1:5–8, 1:60–61, 1:62–64, 2:1–2, 2:3–7, 2:10–29, 2:30–37, 2:39–42, 2:43–52, 2:64–3:2, 3:3–9, 3:10–22, 3:23–26, 3:27–34, 3:35–48, 4:43–56, 5:13–25, 5:27–34, 5:35–46, 5:48–60, 6:2–3, 6:6–10, 6:20–22, 6:31–35, 6:41–44, 6:45–48, 6:49–51, 6:52–57, 6:58–67, 7:1–6, 7:7–14, 7:34, 7:36–41, 8:1–9, 8:16–19, 8:20–27, 8:34–37, and 8:38–41. 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. 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. Yamagata ’839 at Fig. 1, Figure 11, Figure 16, [0001], [0002]–[0003], [0004], [0017], [0025], [0039], [0047], [0064], [0093], [0094], [0096], [0161], claim 24, and claims 29–30. Yoshinaga 2004 at 24, Figure 1, and 26.

Claim Element	Exemplary Citations
	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.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card; and	Cortina ’273 at Abstract, Fig. 1, Figure 16, [0003], [0012], [0015], [0020], [0022], [0096], [0137], [0140], [0143], [0144], [0165], [0166], [0178], [0199], [0202], claim 1, claim 3, claim 4, claim 9, claim 10, claim 15, claim 16, claim 20, claim 21, and claim 42. 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. Fox ’624 at Fig. 2, 2:10–29, 2:53–59, 4:9–13, 5:1–12, 5:13–25, 5:48–60, 6:11–13, 6:41–44, and 6:58–67. Jo ’744 at 1, 2, 3, 6, and 14. Kean ’986 at Abstract, [0006], [0007], [0011], [0012], [0026], [0030], [0034], claim 2, claim 23, and claim 24. 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]. Yamagata ’839 at Fig. 1, Figure 2, Figure 3, Figure 4, Figure 15, [0042], [0064], [0107], [0108], [0109], [0110], [0115], [0117], and [0186]. 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.

Patent Owner's Ex. 2021
Page 003

Claim Element	Exemplary Citations
[1b] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents a single transaction account number.	Bursch '444 at 2:22–32 and 7:30–49. Cortina '273 at Figure 16, [0137], [0140], [0143], [0144], [0165], [0166], and [0178]. Dua '060 at [0009], [0016], [0041], [0315], [0317], [0353], [0354], [0405], and [0433]. Flitcroft '833 at Fig. 2, 7:55–8:10, 8:11–29, and 10:26–56. Fox '624 at Fig. 2, Fig. 5, 2:10–29, 2:53–59, 3:23–26, 3:35–48, 4:9–13, 4:43–56, 5:1–12, 5:13–25, 5:48–60, 6:4–5, 6:6–10, 6:11–13, 6:41–44, 6:45–48, 6:58–67, and 8:1–9. Hanada '365 at [0019]. Horowitz '542 at [0012]. Jo '744 at 1, 3, 6, and 14. Kean '986 at Abstract, [0006], [0011], [0012], [0026], [0027], [0030], [0034], and claim 24. 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, PayPass Figure (p. 8), 8, ExpressPay Figure (p. 9), 10, Table 1, 22, 23, 24, 37, 38, 39, and 40. Sovio '882 at Abstract, Fig. 1, Fig. 2, [0010], [0017], [0020], [0043], [0045], [0048], [0049], [0073], [0080], and [0084]. Yamagata '839 at Fig. 1, Figure 2, Figure 3, Figure 4, Figure 11, [0002], [0094], [0097], [0107], [0108], [0109], [0110], [0115], [0117], and [0163]. Yoshinaga 2004 at 26–27. Yu '038 at Fig. 2, Fig. 3, Fig. 4, Figure 18, Fig. 19, [0034], [0036], [0046], [0093], [0096], and [0097].
2. The mobile phone 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.

Claim Element	Exemplary Citations
	Horowitz ’542 at Figure 2, Figure 3A, and [0021]. Kean ’986 at Abstract, [0006], [0007], [0011], [0012], [0030], [0034], claim 23, and claim 24. SCAR PT-04002 at 7–8, 8, ExpressPay Figure (p. 9), 9, 10, Table 1, 22, 23, and 24. Yamagata ’839 at Fig. 1, [0115], and [0117]. Yu ’038 at [0036] and [0046].
3. The mobile phone of claim 1 wherein the single transaction account number represents financial data.	Bursch ’444 at Abstract, Fig. 1, Fig. 2, Fig.3A–B, Fig.4A–B, 2:22–32, 2:33–44, 2:65–3:9, 3:17–27, 4:1–34, 4:35–49, 5:66–6:10, 7:30–49, and 7:55–8:3. Dua ’060 at Abstract, [0002], [0022], [0048], [0055], [0059], [0060], [0302], and [0402]. Flitcroft ’833 at Abstract, Fig. 2, Fig. 3, Fig. 5, Fig. 8, 4:59–5:4, 5:20–25, 6:53–64, 7:37–54, 7:55–8:10, 8:11–29, 8:35–39, 9:64–10:19, 10:26–56, 10:67–11:14, and 11:66–12:23. Hanada ’365 at [0011], [0026], [0029], [0044], [0058], and Fig. 9. Horowitz ’542 at Abstract, Figure 1, Figure 2, Figure 3A, [0012], [0013], [0015], [0016], [0024], [0027], claim 1, claim 2, claim 17, and claim 21. Sovio ’882 at [0010] and [0084]. Yu ’038 at claim 2.
4. The mobile phone of claim 3 wherein the financial data comprises credit card data.	Bursch ’444 at 7:55–8:3. Cortina ’273 at [0141], [0143], and [0144]. Dua ’060 at claim 89. Flitcroft ’833 at 4:59–5:4 and 5:20–25. Horowitz ’542 at Figure 2, Figure 3A, [0012], [0021], [0024], and [0025]. Kean ’986 at [0012] and [0030]. Yu ’038 at Fig. 12.

Claim Element	Exemplary Citations
5. The mobile phone of claim 1 further comprising smartcard circuitry coupled to the processor.	Codron ’043 at 4:19–27. Cortina ’273 at [0140]. Flitcroft ’833 at Fig. 1 and 10:26–56. Fox ’624 at Fig. 3, 3:35–48, 4:43–56, 6:4–5, and 6:45–48. Hanada ’365 at [0019]. Horowitz ’542 at [0012]. Johansson ’837 at Fig. 1B, 3:47–62, 5:4–14, 5:15–30, 5:31–42, 6:29–42, and 9:28–32. Kean ’986 at [0011], [0012], [0027], and claim 24. Keen ’200 at Fig. 5, [0046]–[0047], [0055], [0084], [0098], and claim 1. Mamba ’073 at Abstract, Fig. 2, [0011]–[0012], [0026], [0029], [0034], [0041], and [0046]. Sovio ’882 at Fig. 2, Fig. 3, [0021], [0023], [0043], and [0045]. Takekawa ’275 at Fig. 10, Fig. 11, Fig. 12, [0056], [0057], [0058], [0111], [0112], and [0113]. Yamagata ’839 at Fig. 1, Figure 2, Figure 3, Figure 4, Figure 11, [0001], [0002], [0016], [0017], [0064], [0097], [0098], [0162], and [0163].
8, The mobile phone of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	Cortina ’273 at [0143]. 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. Fox ’624 at 5:1–12, 5:13–25, 6:41–44, and 6:58–67. Jo ’744 at 2. Kean ’986 at Figure 1, [0012], and [0030]. SCAR PT-04002 at 4, 8, 10, Table 1, 22, 23, and 24. Sovio ’882 at [0010]. Yamagata ’839 at [0110].

Claim Element	Exemplary Citations
	Yoshinaga 2004 at 25 and 26–27. Yu ’038 at Fig. 3, Fig. 4, [0034], and [0046].
9[pre]. A mobile phone comprising:	*See* above at 1[pre].
[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 using single transaction account numbers; and	Bursch ’444 at Abstract, Fig. 1, Fig. 2, Fig.3A–B, Fig.4A–B, 1:6–9, 2:22–32, 2:33–44, 2:65–3:9, 3:17–27, 4:1–34, 4:35–49, 5:9–27, 5:28–52, 5:53–60, 5:66–6:10, 6:26–52, 7:30–49, and 7:55–8:3. Cortina ’273 at Fig. 4, [0096], [0097], [0141], and [0178]. Dua ’060 at Abstract, [0002], [0007], [0009], [0022], [0048], [0055], [0059], [0180], [0297], [0302], [0402], and [0405]. Flitcroft ’833 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 5, Fig. 8, 4:59–5:4, 5:20–25, 6:53–64, 7:37–54, 7:55–8:10, 8:11–29, 10:26–56, 10:67–11:14, 11:66–12:23, 13:17–32, and 14:12–29. Fox ’624 at Fig. 3, 1:9–30, 1:62–64, 5:13–25, 6:41–44, 6:58–67, and 8:20–27. Hanada ’365 at [0011], [0012], [0014], [0026], [0029], [0044], [0058], Fig. 2, Fig. 5, and Fig. 9. Horowitz ’542 at Abstract, Figure 1, Figure 2, Figure 3A, [0003], [0011], [0012], [0013], [0016], [0025], [0027], claim 1, claim 2, claim 5, claim 6, claim 14, claim 15, claim 17, and claim 21. Kean ’986 at [0026] and [0027]. Keen ’200 at Fig. 5. SCAR PT-04002 at 4, Fig. 1., 7, 7–8, 8, 9, 10, 11, Table 1, and 24. Sovio ’882 at Fig. 1, Fig. 2, [0010], [0020], [0045], [0048], [0049], [0080], and [0084]. Yamagata ’839 at Fig. 1, Figure 2, Figure 3, Figure 11, [0025], [0027], and [0162]. Yoshinaga 2004 at 24–25, 25, Figure 1, and 26. Yu ’038 at Fig. 4, [0001], [0036], [0039], and [0046].

Claim Element	Exemplary Citations
[9c] a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field.	Codron ’043 at 4:19–27. Cortina ’273 at Abstract, Fig. 1, Figure 16, [0003], [0012], [0015], [0020], [0022], [0096], [0137], [0140], [0143], [0144], [0165], [0166], [0178], [0199], [0202], claim 1, claim 3, claim 4, claim 9, claim 10, claim 15, claim 16, claim 20, claim 21, and claim 42. 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 Fig. 1 and 10:26–56. Fox ’624 at Fig. 2, Fig. 3, Fig. 5, 2:10–29, 2:53–59, 3:23–26, 3:35–48, 4:9–13, 4:43–56, 5:1–12, 5:13–25, 5:48–60, 6:4–5, 6:6–10, 6:11–13, 6:41–44, 6:45–48, 6:58–67, and 8:1–9. Hanada ’365 at [0019]. Horowitz ’542 at [0012]. Jo ’744 at 1, 2, 3, 6, and 14. Johansson ’837 at Fig. 1B, 3:47–62, 5:4–14, 5:15–30, 5:31–42, 6:29–42, and 9:28–32. Kean ’986 at Abstract, [0006], [0007], [0011], [0012], [0026], [0027], [0030], [0034], claim 2, and claim 24. 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], [0046]–[0047], [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], [0041], and [0046]. 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, Fig. 3, [0010], [0017], [0020], [0021], [0023], [0041], [0043], [0045], [0049], [0073], and [0080]. Takekawa ’275 at Fig. 10, Fig. 11, Fig. 12, [0056], [0057], [0058], [0111], [0112], and [0113]. Yamagata ’839 at Fig. 1, Figure 2, Figure 3, Figure 4, Figure 11, Figure 15, [0001], [0002], [0016], [0017], [0042], [0064], [0094], [0097], [0098], [0107], [0108], [0109], [0110], [0115], [0117], [0162], [0163], and [0186]. Yoshinaga 2004 at 26–27.

Claim Element	Exemplary Citations
	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.
10. The mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Cortina ’273 at Fig. 4, [0096], [0097], [0137], [0141], [0143], and [0178]. Dua ’060 at [0007], [0009], and [0433]. Flitcroft ’833 at Fig. 1 and 10:26–56. Fox ’624 at Fig. 3, 1:9–30, 1:62–64, 5:1–12, 5:13–25, 6:41–44, 6:58–67, and 8:20–27. 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. Kean ’986 at Figure 1, [0012], [0023], [0030], and claim 23. 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]. Yamagata ’839 at Fig. 1, Figure 2, Figure 3, Figure 11, [0025], [0027], [0098], [0107], [0109], [0110], and [0162]. 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 phone of claim 9 wherein the transactions are financial transactions.	Cortina ’273 at [0141], [0143], and [0144]. Dua ’060 at [0293], [0422], claim 75, claim 88, and claim 89. Flitcroft ’833 at 8:35–39. Fox ’624 at 5:13–25 and 8:20–27. Horowitz ’542 at Abstract, Figure 2, Figure 3A, [0011], [0012], [0015], [0021], [0024], [0025], claim 1, claim 2, and claim 17.

Patent Owner's Ex. 2021
Page 009

Claim Element	Exemplary Citations
	Kean ’986 at [0025], [0030], and [0034]. SCAR PT-04002 at 4 and 8. Yamagata ’839 at Fig. 1, [0065], [0100], [0109], [0110], and [0115]. Yu ’038 at Fig. 12.
12. The mobile phone of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	*See* above at claim 2.
13. The mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence.	Bursch ’444 at Fig. 1, 2:22–32, 2:33–44, 3:17–27, 3:38–51, 3:52–67, 4:1–34, 4:35–49, 5:9–27, 5:28–52, 5:53–60, 6:26–52, and 7:30–49. Flitcroft ’833 at Fig. 2, Fig. 3, Fig. 5, Fig. 8, 4:59–5:4, 5:20–25, 10:26–56, 10:67–11:14, 11:66–12:23, 13:6–16, 13:17–32, 13:59–66, and 14:12–29. Hanada ’365 at [0029], [0044], [0046], [0049], [0058], Fig. 2, Fig. 5, Fig. 9, and Fig. 11. Horowitz ’542 at Abstract, Figure 1, [0013], [0015], [0024], [0027], and [0035]. Sovio ’882 at [0010] and [0084].
14. The mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	Bursch ’444 at Abstract, Fig. 1, Fig. 2, Fig.3A–B, 1:6–9, 2:22–32, 2:33–44, 2:65–3:9, 3:17–27, 3:52–67, 4:1–34, 4:35–49, 5:9–27, 5:28–52, 5:53–60, 5:60–65, 6:26–52, and 7:30–49. Dua ’060 at [0055] and [0180]. Flitcroft ’833 at Abstract, Fig. 2, Fig. 3, Fig. 5, Fig. 8, 4:59–5:4, 5:5–19, 5:20–25, 6:53–64, 7:23–30, 7:37–54, 7:55–8:10, 8:11–29, 8:35–39, 9:64–10:19, 10:26–56, 10:67–11:14, 11:20–36, 11:66–12:23, 13:6–16, 13:17–32, 13:40–58, 13:59–66, and 14:12–29. Hanada ’365 at Abstract, [0012], [0026], [0029], [0034], [0044], [0046], [0049], [0058], Fig. 2, Fig. 5, Fig. 9, and Fig. 11. Horowitz ’542 at Abstract, Figure 1, [0013], [0015], and [0024]. Sovio ’882 at [0010] and [0084].

Claim Element	Exemplary Citations
15[pre]. A mobile phone comprising:	*See* above at 1[pre].
[15a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	*See* above at [1a].
[15b] circuitry to enable use of single transaction account numbers; and	Bursch '444 at Abstract, Fig. 1, Fig. 2, Fig.3A–B, Fig.4A–B, 1:6–9, 2:22–32, 2:33–44, 2:65–3:9, 3:17–27, 4:1–34, 4:35–49, 5:9–27, 5:28–52, 5:53–60, 5:66–6:10, 6:26–52, 7:30–49, and 7:55–8:3. Dua '060 at Abstract, [0002], [0022], [0048], [0055], [0059], [0180], [0297], [0302], [0402], and [0405]. Flitcroft '833 at Abstract, Fig. 2, Fig. 3, Fig. 5, Fig. 8, 4:59–5:4, 5:20–25, 6:53–64, 7:37–54, 7:55–8:10, 8:11–29, 10:26–56, 10:67–11:14, 11:66–12:23, 13:17–32, and 14:12–29. Hanada '365 at [0011], [0012], [0014], [0026], [0029], [0044], [0058], Fig. 2, Fig. 5, and Fig. 9. Horowitz '542 at Abstract, Figure 1, Figure 2, Figure 3A, [0012], [0013], [0016], [0027], claim 1, claim 2, claim 17, and claim 21. Kean '986 at [0026] and [0027]. SCAR PT-04002 at 7, 10, and 24. Sovio '882 at [0010], [0048], [0049], [0080], and [0084].
[15c] a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number.	Bursch '444 at Fig.3A–B, 2:22–32, 5:66–6:10, 6:26–52, and 7:30–49. Cortina '273 at Abstract, Fig. 1, Figure 16, [0003], [0012], [0015], [0020], [0022], [0096], [0137], [0140], [0143], [0144], [0165], [0166], [0178], [0199], [0202], claim 1, claim 3, claim 4, claim 9, claim 10, claim 15, claim 16, claim 20, claim 21, and claim 42. 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 Fig. 2, 7:55–8:10, 8:11–29, and 10:26–56. Fox '624 at Fig. 2, Fig. 5, 2:10–29, 2:53–59, 3:23–26, 3:35–48, 4:9–13, 4:43–56, 5:1–12, 5:13–25, 5:48–60, 6:4–5, 6:6–10, 6:11–13, 6:41–44, 6:45–48, 6:58–67, and 8:1–9.

Claim Element	Exemplary Citations
	Hanada ’365 at [0019]. Horowitz ’542 at Abstract, Figure 1, [0012], [0013], [0027], and claim 1. Jo ’744 at 1, 2, 3, 6, and 14. Kean ’986 at Abstract, [0006], [0007], [0011], [0012], [0026], [0027], [0030], [0034], claim 2, and claim 24. 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], [0080], and [0084]. Yamagata ’839 at Fig. 1, Figure 2, Figure 3, Figure 4, Figure 11, Figure 15, [0002], [0042], [0064], [0094], [0097], [0107], [0108], [0109], [0110], [0115], [0117], [0163], and [0186]. 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.
16. The mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry.	Bursch ’444 at Fig.3A–B, 2:22–32, 5:66–6:10, and 6:26–52. Flitcroft ’833 at Fig. 1, 7:55–8:10, and 10:26–56. Fox ’624 at Fig. 2, Fig. 3, Fig. 5, 1:9–30, 1:60–61, 2:3–7, 2:30–37, 3:35–48, 3:49–59, 4:43–56, 5:13–25, 5:48–60, 6:2–3, 6:6–10, 6:45–48, 6:58–67, 7:7–14, and 8:1–9. Horowitz ’542 at Abstract, Figure 1, Figure 2, [0003], [0012], [0013], [0027], claim 1, claim 5, claim 6, claim 14, claim 15, and claim 21. Keen ’200 at [0046]–[0047] and [0086]. Mamba ’073 at Fig. 2, [0007], [0008], [0009], [0022], [0034], [0041], and [0046].

Claim Element	Exemplary Citations
	SCAR PT-04002 at 9 and Table 1. Sovio '882 at [0010], [0048], [0049], and [0084]. Yu '038 at Fig. 4.
17. The mobile phone of claim 15 wherein the single transaction account numbers have a pre-defined sequence.	*See* above at claim 13.
18. The mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	*See* above at claim 14.

Patent Owner's Ex. 2021
Page 013

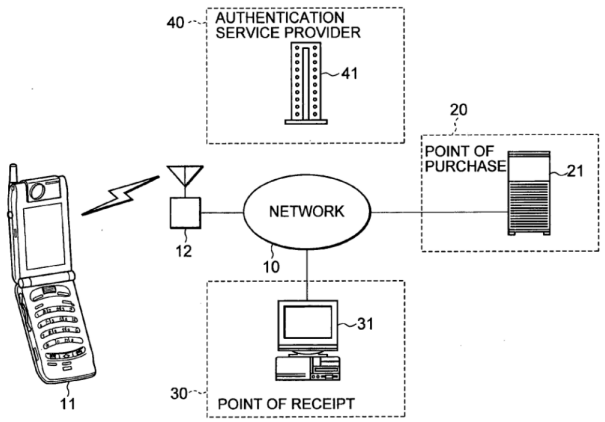
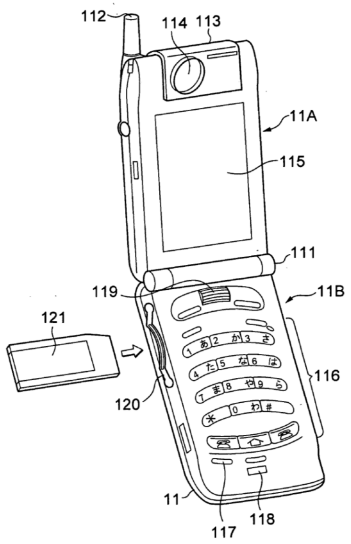
DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,208,423

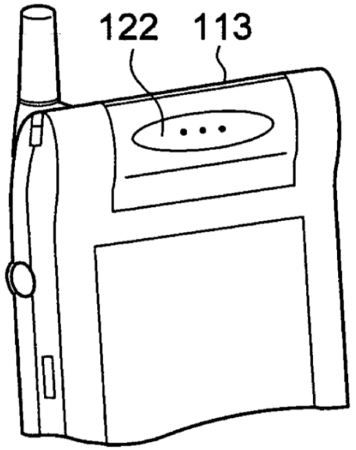
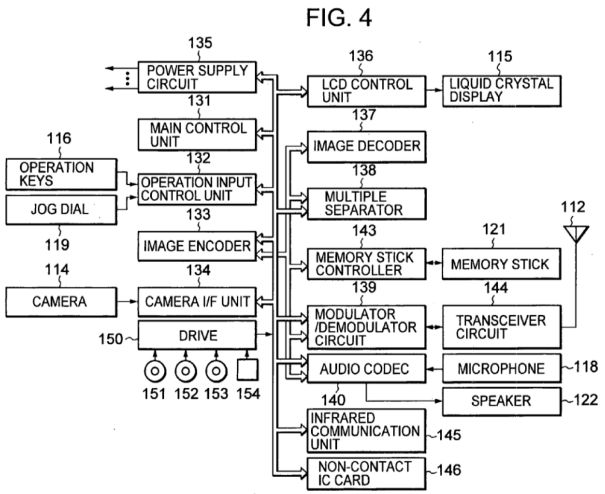
EXHIBIT F1: US20050086171A1 ("Abe '171")

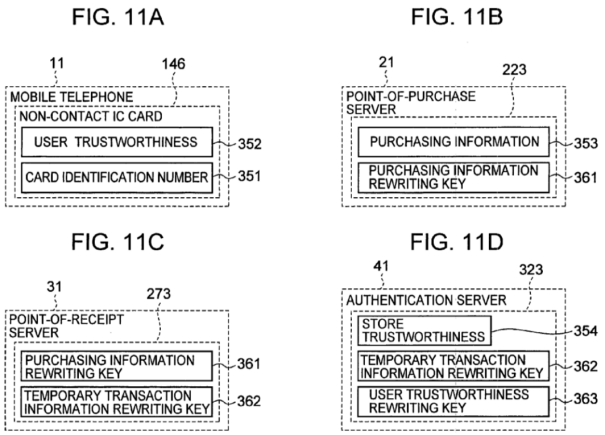
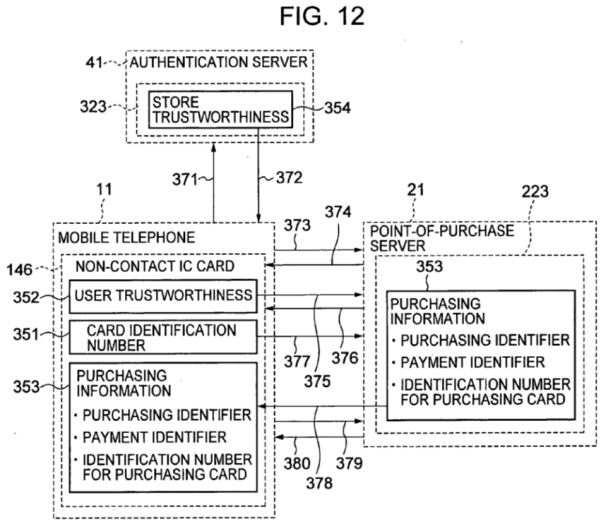
As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,208,423 ("the '423 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Abe '171 and (b) under 35 U.S.C. § 103(a) as obvious over Abe '171 standing alone and as set forth herein, and/or combined 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 F and Exhibits F1–F5, 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 '423 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.

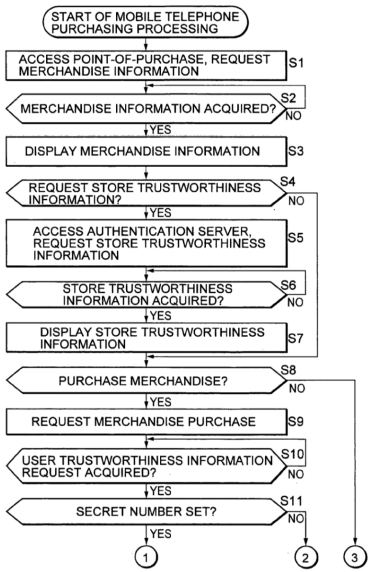
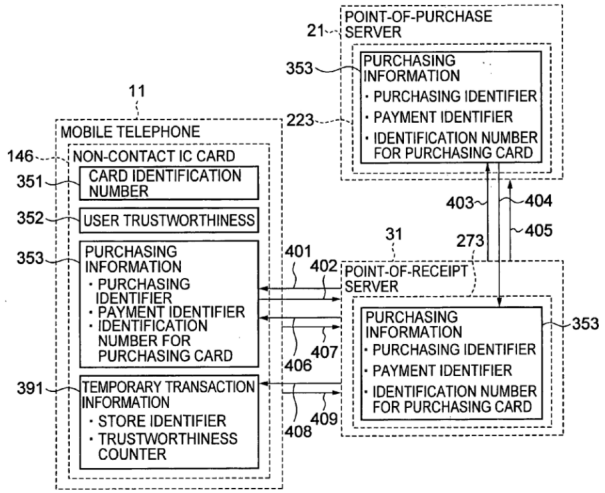
Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '423 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's 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.

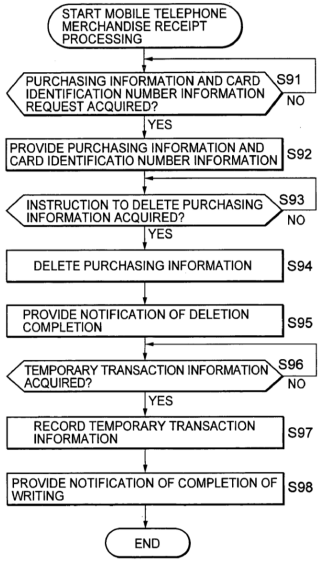
Claim Element	**Exemplary Citations to US20050086171A1 ("Abe '171")**
1[pre]. A mobile phone comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Abe '171 discloses or renders obvious "[a] mobile phone." For example: Abe '171 at Abstract 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 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 

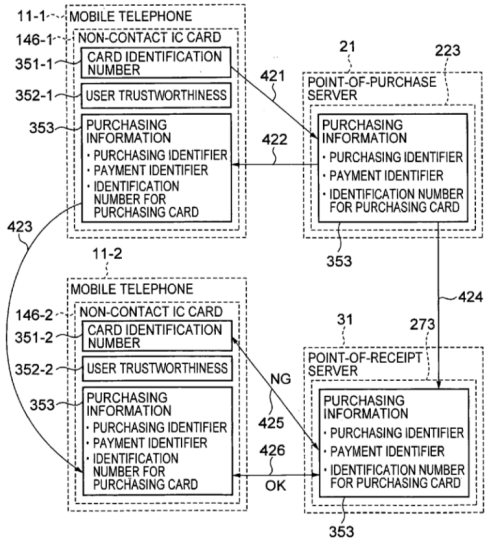
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at Fig.11A–D  Abe ’171 at Fig. 12  Abe ’171 at Fig. 13

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

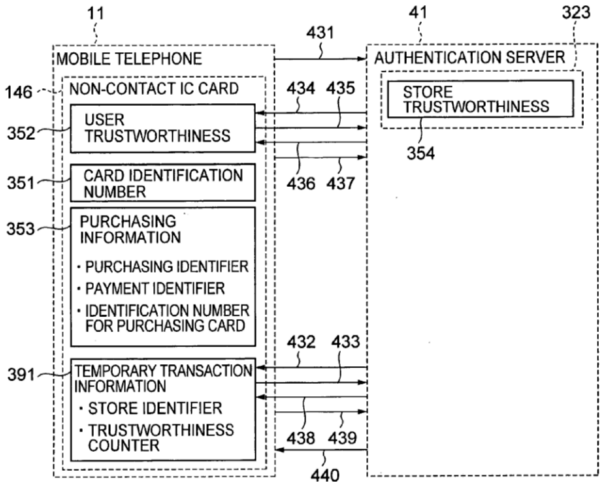
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")

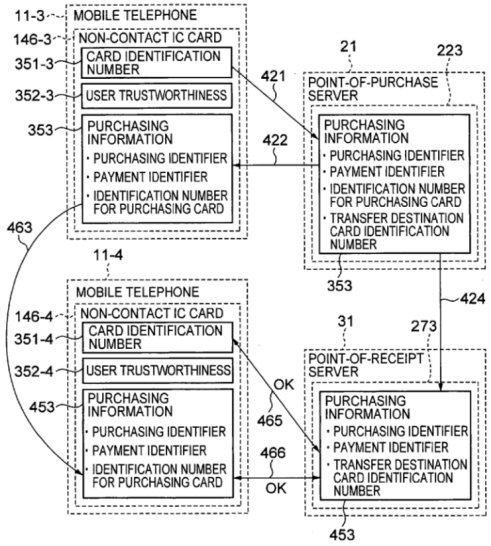
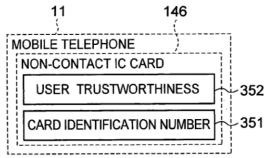
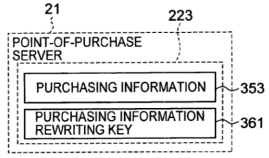
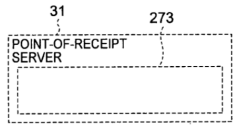
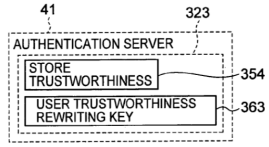
FIG. 23

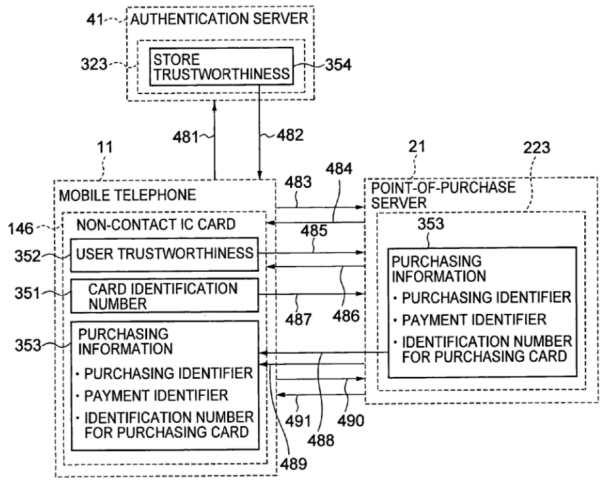
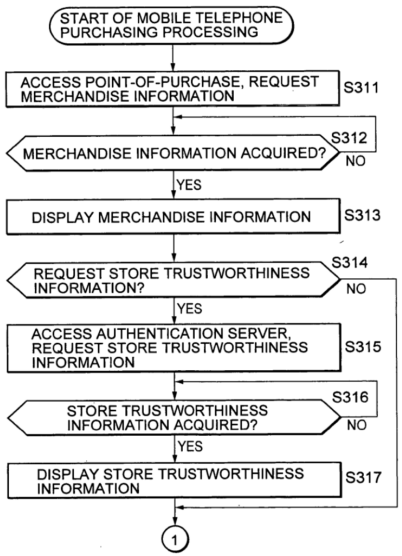


Abe '171 at Fig. 24

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]

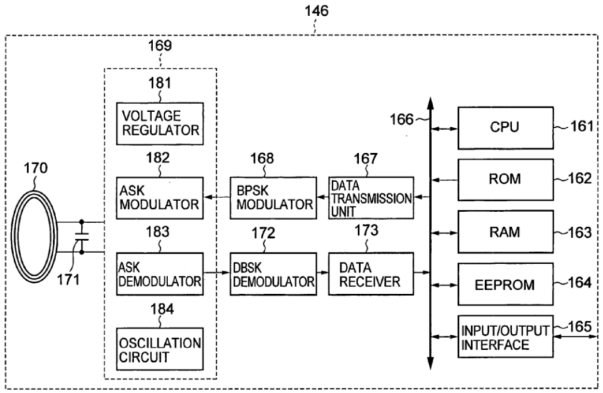
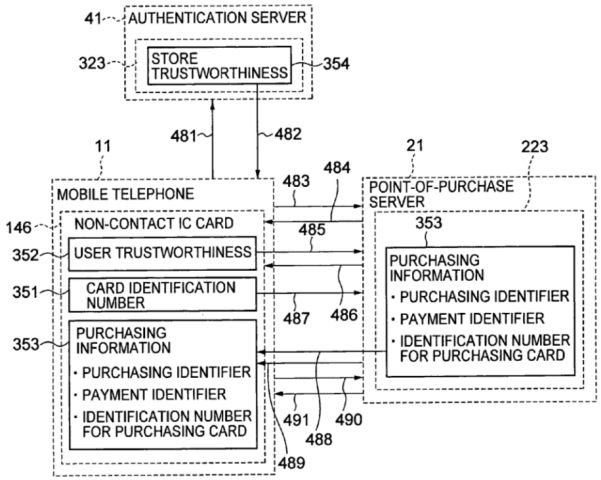
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance 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]

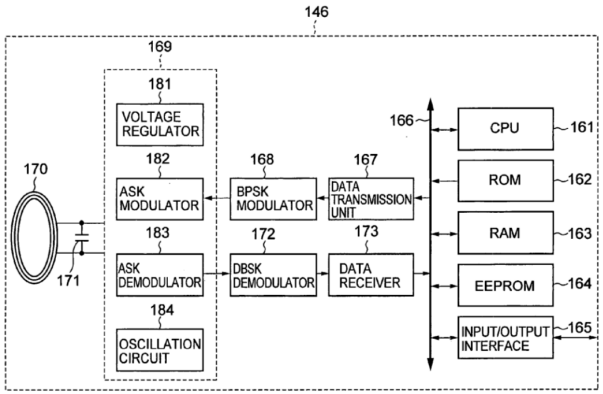
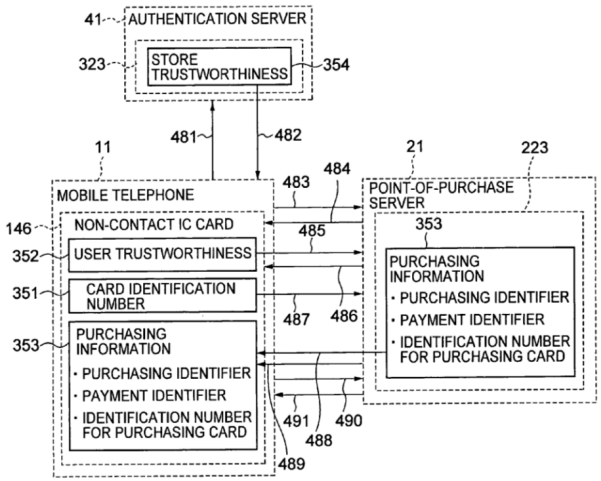
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	In FIG. 47, as with the case in FIG. 24, the mobile telephone 11 accesses the authentication server 41 (arrow 511), but in a point of difference with the case of FIG. 24, the authentication server 41 does not request temporary commercial 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. 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.
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card; and	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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 5  Abe '171 at Fig. 36 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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 demodulator 294 demodulates a modulated wave (ASK modulated wave) acquired via the antenna 295 and outputs the demodulated data to the SPU 296.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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.
[1b] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic	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 a single transaction account number." For example:

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
field that represents a single transaction account number.	Abe '171 at Figure 5 FIG. 5  Abe '171 at Fig. 36 FIG. 36  Abe '171 at [0011] Information relating to the commercial transaction is made to contain a first identifier for identifying the commercial transaction, a second identifier for identifying whether or not payment of fees is complete for

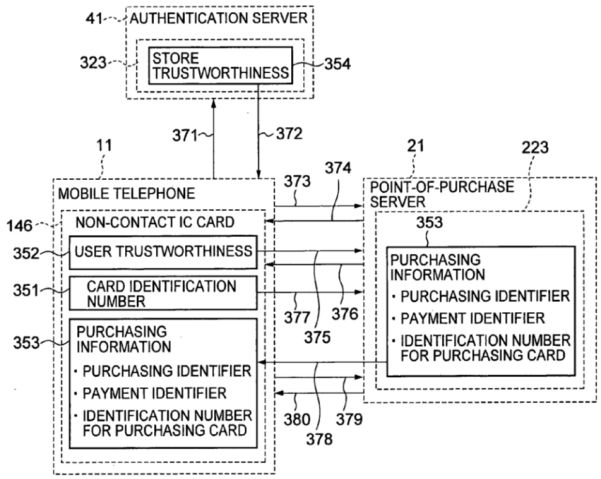
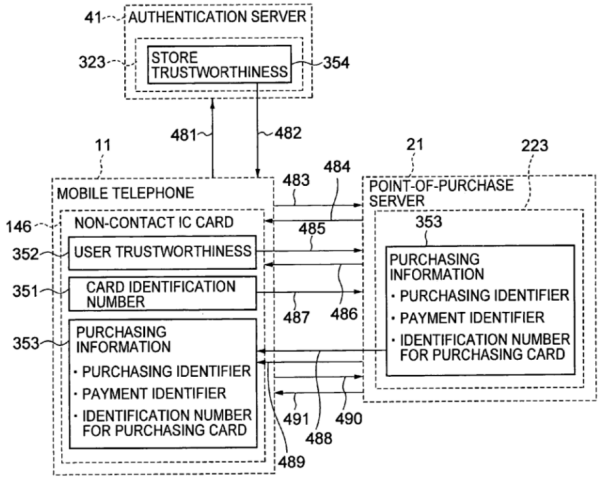
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	the commercial transaction, and the identification number of the information communication terminal used in the commercial transaction. Abe ’171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is 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 [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 [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.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [0179] The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method. Abe '171 at [0199] As shown in FIG. 12, the purchasing information 353 is comprised of a purchasing identifier for identifying the corresponding commercial transaction, a payment identifier for identifying whether or not payment for the sale of the merchandise has been made, and a purchasing card identification number constituted by the card identification number 351 allotted to the non-contact IC card 146 in the possession of the user purchasing the merchandise. Abe '171 at [0259] The point-of-receipt server 31 that has acquired the purchasing information 353 and the card identification number information (card identification number 351) acquires purchasing information 353 (i.e. purchasing information for which the contained purchasing identifier is the same) corresponding to the acquired purchasing information 353 from the point-of-purchase server 21 (arrow 403 and arrow 404). Abe '171 at [0284] When it is determined that the purchasing information 353 and the card identification number information have been acquired, the CPU 251 advances processing to step S114, controls the communication unit 274, and makes a request to the point-of-purchase server 21 for purchasing information 353 (for which the purchasing identifier is the same) corresponding to the purchasing information 353 acquired from the non-contact IC card 146. This processing corresponds to the processing of arrow 403 of FIG. 18.

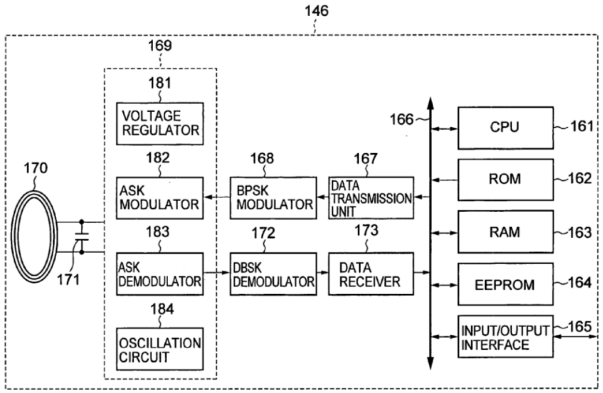
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Abe '171 at [0371] When the purchaser mobile telephone 11-3 and the transfer destination mobile telephone 11-4 are close to each other so that the non-contact IC card 146-4 is positioned within the communication range of the non-contact 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 [0392] When it is determined that the purchasing information 353 and the card identification number information, the CPU 201 advances processing to step S264, purchasing information 353 corresponding to (having the same purchasing identifier as) the acquired purchasing information is retrieved from the storage unit 223, and the purchasing information 353 provided by the purchaser mobile telephone 11-3 and card identification number 351-3 contained in the card identification number information are authenticated using the retrieved purchasing information 353. Abe '171 at [0465] Namely, in step S401 to step S403 of FIG. 44, the CPU 251 makes a request to and acquires from the mobile telephone 11 the purchasing information 353 and the card identification number information. In the processing of step S404 and step S405, purchasing information corresponding to (having the same purchasing identifier as) the purchasing information 353 acquired from the mobile telephone 11 is requested from the point-of-purchase server 21 and is acquired. 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")
2. The mobile phone 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 phone of claim 1 wherein the single transaction account number represents financial data.	Abe '171 discloses or renders obvious "[t]he mobile phone of claim 1 wherein the single transaction account number represents financial data." 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 Fig. 12

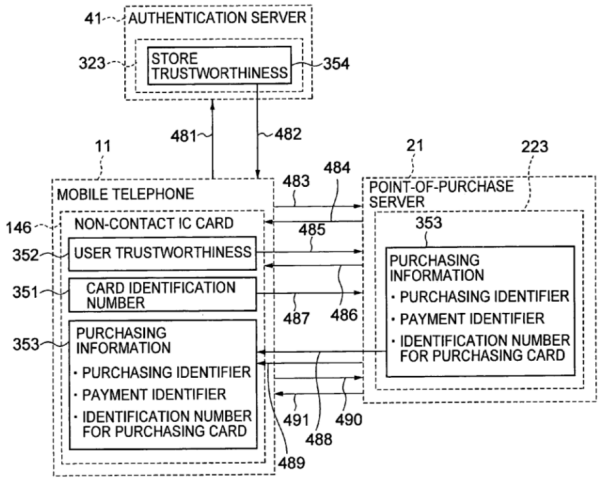
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 12  Abe '171 at Fig. 36 FIG. 36  Abe '171 at [0011]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	Information relating to the commercial transaction is made to contain a first identifier for identifying the commercial transaction, a second identifier for identifying whether or not payment of fees is complete for the commercial transaction, and the identification number of the information communication terminal used in the commercial transaction. 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 [0179] The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method. 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 [0198] The point-of-purchase server 21 that has acquired the card identification number 351 then carries out processing relating to purchasing and charging, and sells the merchandise. The point-of-purchase server 21 then generates purchasing information 353 constituting information relating to the current commercial transaction and provides this to the mobile telephone 11 together with the purchasing information rewriting key 361 (arrow 378). Abe '171 at [0199]

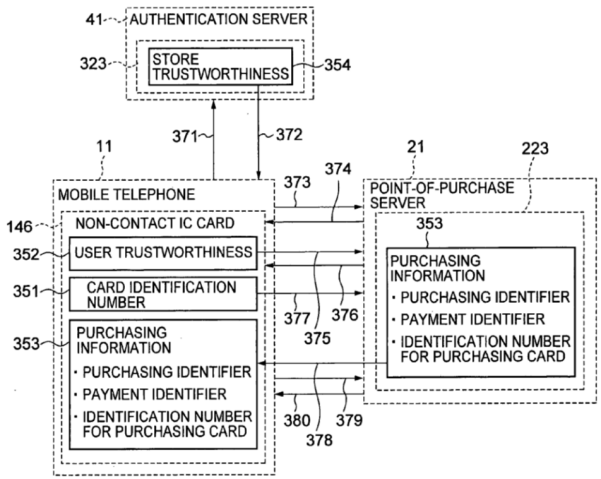
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	As shown in FIG. 12, the purchasing information 353 is comprised of a purchasing identifier for identifying the corresponding commercial transaction, a payment identifier for identifying whether or not payment for the sale of the merchandise has been made, and a purchasing card identification number constituted by the card identification number 351 allotted to the non-contact IC card 146 in the possession of the user purchasing the merchandise. Abe '171 at [0245] To conform with this request, in step S26 of FIG. 14, the main control unit 131 of the mobile telephone 11 supplies card identification number information to the point-of-purchase server 21. 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 claim 35 a generating step for generating information relating to said commercial transaction during product sales; 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.
4. The mobile phone of claim 3 wherein the financial data comprises credit card data.	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 phone of claim 1 further comprising smartcard circuitry coupled to the processor.	Abe '171 discloses or renders obvious "[t]he mobile phone of claim 1 further comprising smartcard circuitry coupled to the processor." For example: Abe '171 at Figure 5

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 5  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 [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,

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [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 [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")
	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 phone 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 phone of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Abe '171 at Fig. 36 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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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). *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. *See also* claim 1 above.
9[pre]. A mobile phone 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 phone." 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.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
[9b] smartcard circuitry for performing transactions using single transaction account numbers; and	Abe '171 discloses or renders obvious "smartcard circuitry for performing transactions using single transaction account numbers." 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 Fig. 12 FIG. 12  Abe '171 at Fig. 35A–D

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

FIG. 35A

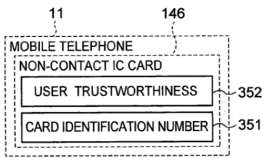


FIG. 35B

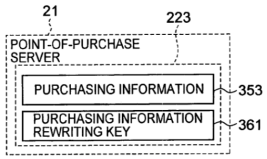


FIG. 35C

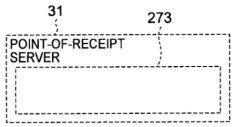
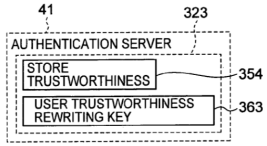
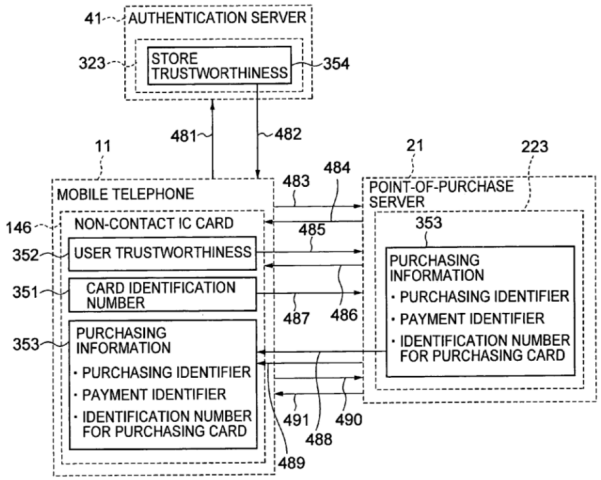


FIG. 35D



Abe '171 at Fig. 36

FIG. 36



Abe '171 at [0011]

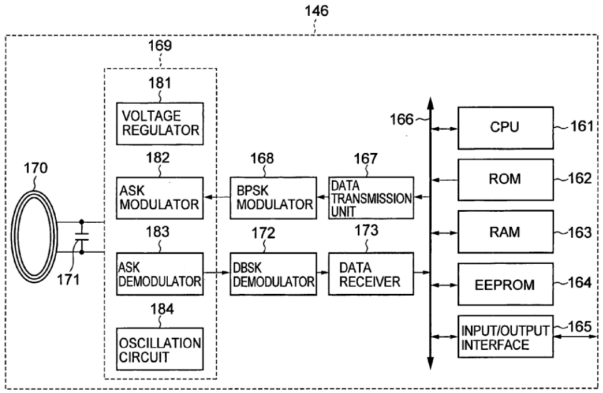
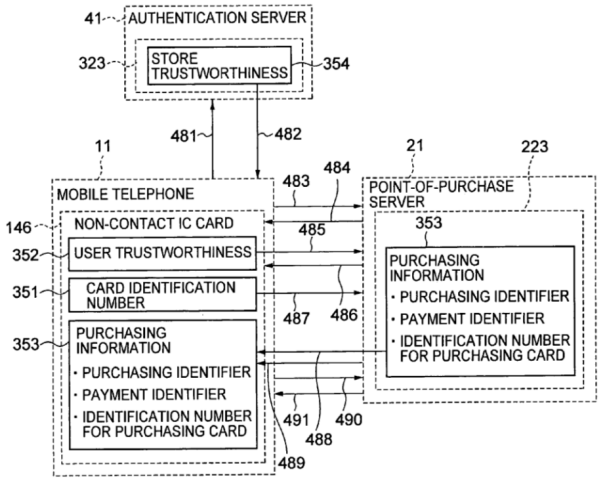
> Information relating to the commercial transaction is made to contain a first identifier for identifying the commercial transaction, a second identifier for identifying whether or not payment of fees is complete for the commercial transaction, and the identification number of the information communication terminal used in the commercial transaction.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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). 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 [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 [0179] The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method. 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 [0198] The point-of-purchase server 21 that has acquired the card identification number 351 then carries out processing relating to purchasing and charging, and sells the merchandise. The point-of-purchase server 21 then generates purchasing information 353 constituting information relating to the current commercial transaction and provides this to the mobile telephone 11 together with the purchasing information rewriting key 361 (arrow 378). Abe '171 at [0199] As shown in FIG. 12, the purchasing information 353 is comprised of a purchasing identifier for identifying the corresponding commercial transaction, a payment identifier for identifying whether or not payment for the sale of the merchandise has been made, and a purchasing card identification number constituted by the card identification number 351 allotted to the non-contact IC card 146 in the possession of the user purchasing the merchandise. Abe '171 at [0245] To conform with this request, in step S26 of FIG. 14, the main control unit 131 of the mobile telephone 11 supplies card identification number information to the point-of-purchase server 21. 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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [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 [0259] The point-of-receipt server 31 that has acquired the purchasing information 353 and the card identification number information (card identification number 351) acquires purchasing information 353 (i.e. purchasing information for which the contained purchasing identifier is the same) corresponding to the acquired purchasing information 353 from the point-of-purchase server 21 (arrow 403 and arrow 404). 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 [0284] When it is determined that the purchasing information 353 and the card identification number information have been acquired, the CPU 251 advances processing to step S114, controls the communication unit 274, and makes a request to the point-of-purchase server 21 for purchasing information 353 (for which the purchasing identifier is the same) corresponding to the purchasing information 353 acquired from the non-contact IC card 146. This processing corresponds to the processing of arrow 403 of FIG. 18. 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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [0392] When it is determined that the purchasing information 353 and the card identification number information, the CPU 201 advances processing to step S264, purchasing information 353 corresponding to (having the same purchasing identifier as) the acquired purchasing information is retrieved from the storage unit 223, and the purchasing information 353 provided by the purchaser mobile telephone 11-3 and card identification number 351-3 contained in the card identification number information are authenticated using the retrieved purchasing information 353. Abe '171 at [0465] Namely, in step S401 to step S403 of FIG. 44, the CPU 251 makes a request to and acquires from the mobile telephone 11 the purchasing information 353 and the card identification number information. In the processing of step S404 and step S405, purchasing information corresponding to (having the same purchasing identifier as) the purchasing information 353 acquired from the mobile telephone 11 is requested from the point-of-purchase server 21 and is acquired. Abe '171 at claim 35 a generating step for generating information relating to said commercial transaction during product sales; *See also* [1b] and 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.
[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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 5  Abe '171 at Fig. 36 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

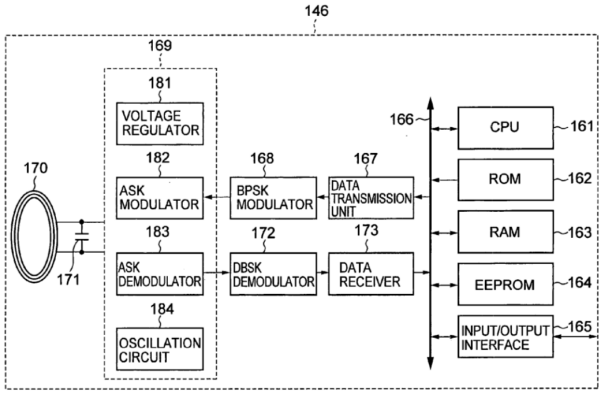
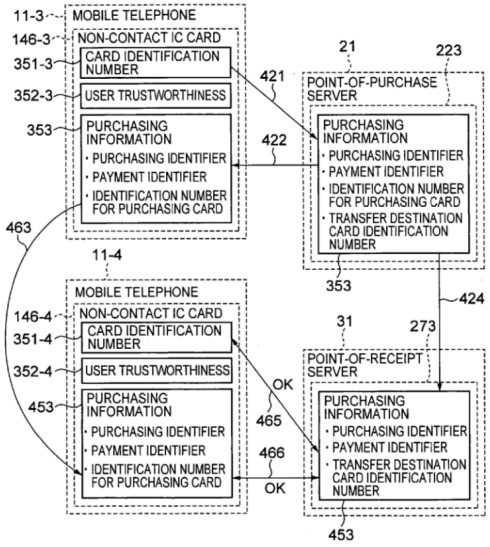
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	information relating to the commercial transaction to the first information processing apparatus using short-range wireless communication by the wireless communication means. Abe '171 at [0030] The first information processing system 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 receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112.

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

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	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 [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]

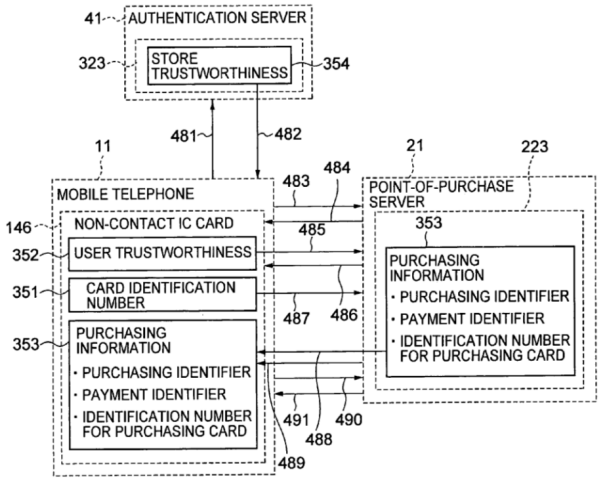
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	In step S93, the main control unit 131 controls the CPU 161 of the non-contact IC card 146 so as to determine whether or not an instruction to delete the purchasing information rewriting key 361 from the point-of-receipt server 31 and 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 [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 [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. *See also* [1b] 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.
10. The mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Abe '171 discloses or renders obvious "[t]he mobile phone 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 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

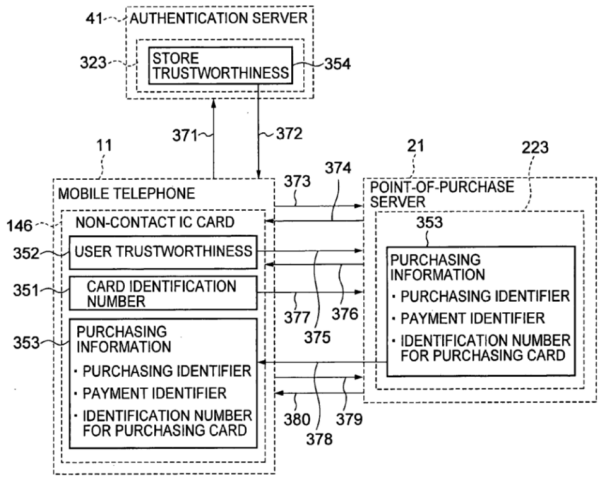
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 5  Abe '171 at Fig. 29 FIG. 29  Abe '171 at [0092]

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 [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.

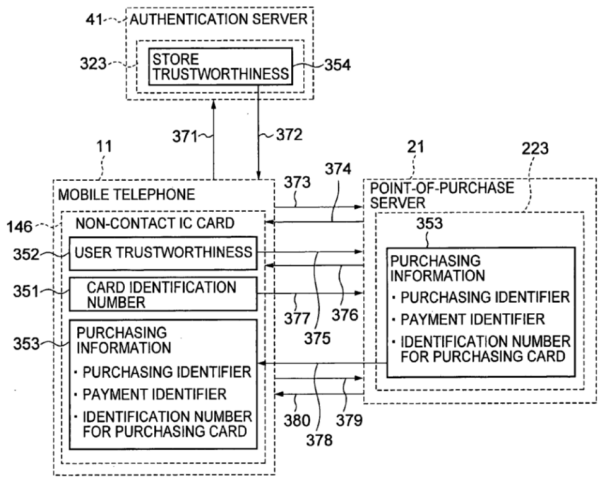
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at [0197] The point-of-purchase server 21 that has acquired the user trustworthiness 352 and confirmed that the user of the mobile telephone 11 is trustworthy then makes a request to the mobile telephone 11 for the card identification 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. 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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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.
11. The mobile phone of claim 9 wherein the transactions are financial transactions.	Abe '171 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the transactions are financial transactions." For example: Abe '171 at Fig. 36 FIG. 36  Abe '171 at [0147]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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; *See also* claim 3 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.
12. The mobile phone 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.
13. The mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence.	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.
14. The mobile phone of claim 9 wherein the single transaction account numbers comprise pre-	Abe '171 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: Abe '171 at Fig. 12

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
assigned single-use transaction numbers.	FIG. 12  Abe '171 at [0179] The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method. 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 [0199] As shown in FIG. 12, the purchasing information 353 is comprised of a purchasing identifier for identifying the corresponding commercial transaction, a payment identifier for identifying whether or not payment for the sale of the merchandise has been made, and a purchasing card identification number

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	constituted by the card identification number 351 allotted to the non-contact IC card 146 in the possession of the user purchasing the merchandise. Abe '171 at [0200] The mobile telephone 11 provided with the purchasing information 353 and the purchasing information rewriting key 361 then records the purchasing information 353 in the non-contact IC card 146 using the purchasing information rewriting key 361. When this writing is complete, the mobile telephone 11 deletes the purchasing information rewriting key 361 and provides notification of completion of writing to the point-of-purchase server 21 (arrow 379). Abe '171 at claim 35 a generating step for generating information relating to said commercial transaction during product sales; 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.
15[pre]. A mobile phone 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 phone." 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.
[15a] 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.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
[15b] circuitry to enable use of single transaction account numbers; and	Abe '171 discloses or renders obvious "circuitry to enable use of single transaction account numbers." 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 Fig. 12 FIG. 12  Abe '171 at Fig. 35A–D

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

FIG. 35A

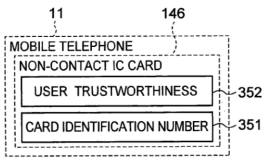


FIG. 35B

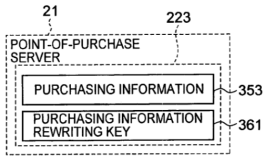


FIG. 35C

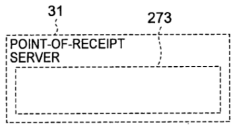
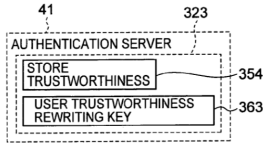
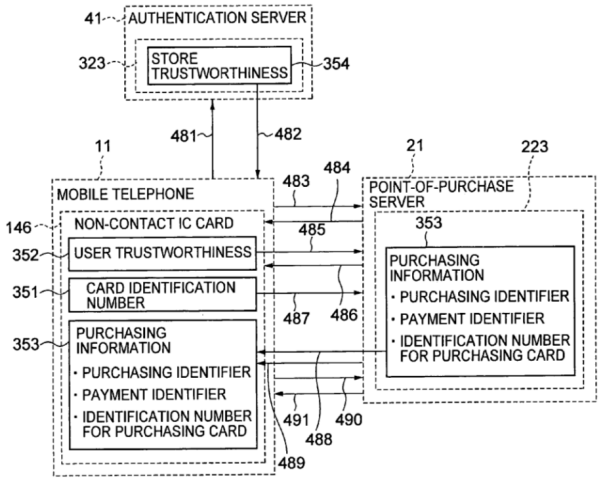


FIG. 35D



Abe '171 at Fig. 36

FIG. 36



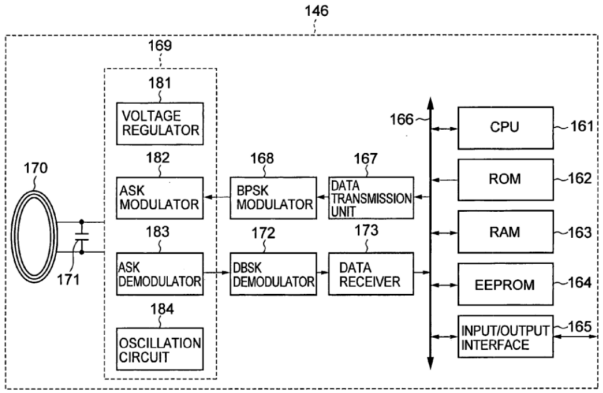
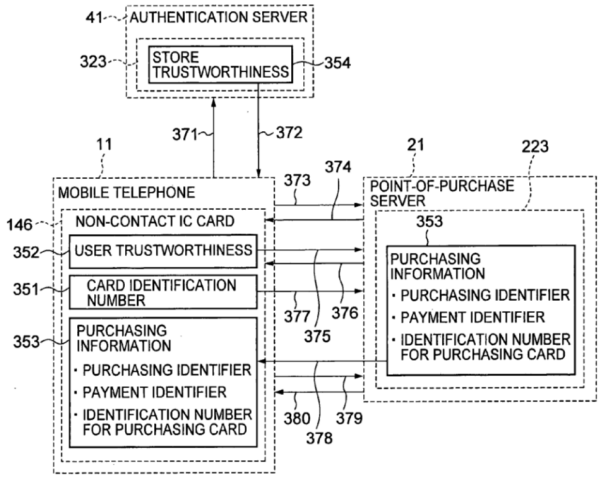
Abe '171 at [0011]

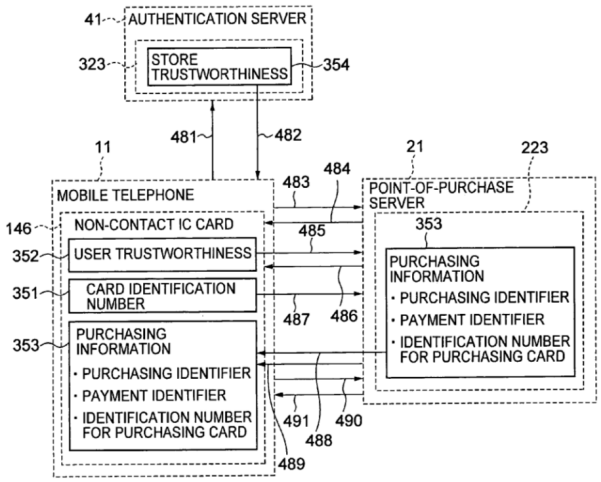
> Information relating to the commercial transaction is made to contain a first identifier for identifying the commercial transaction, a second identifier for identifying whether or not payment of fees is complete for the commercial transaction, and the identification number of the information communication terminal used in the commercial transaction.

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [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 [0179] The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method. 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 [0198] The point-of-purchase server 21 that has acquired the card identification number 351 then carries out processing relating to purchasing and charging, and sells the merchandise. The point-of-purchase server 21 then generates purchasing information 353 constituting information relating to the current commercial transaction and provides this to the mobile telephone 11 together with the purchasing information rewriting key 361 (arrow 378). Abe '171 at [0199]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	As shown in FIG. 12, the purchasing information 353 is comprised of a purchasing identifier for identifying the corresponding commercial transaction, a payment identifier for identifying whether or not payment for the sale of the merchandise has been made, and a purchasing card identification number constituted by the card identification number 351 allotted to the non-contact IC card 146 in the possession of the user purchasing the merchandise. Abe '171 at [0245] To conform with this request, in step S26 of FIG. 14, the main control unit 131 of the mobile telephone 11 supplies card identification number information to the point-of-purchase server 21. 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 [0259] The point-of-receipt server 31 that has acquired the purchasing information 353 and the card identification number information (card identification number 351) acquires purchasing information 353 (i.e. purchasing information for which the contained purchasing identifier is the same) corresponding to the acquired purchasing information 353 from the point-of-purchase server 21 (arrow 403 and arrow 404). Abe '171 at [0284] When it is determined that the purchasing information 353 and the card identification number information have been acquired, the CPU 251 advances processing to step S114, controls the communication unit 274, and makes a request to the point-of-purchase server 21 for purchasing information 353 (for which the purchasing identifier is the same) corresponding to the purchasing information 353 acquired from the non-contact IC card 146. This processing corresponds to the processing of arrow 403 of FIG. 18. 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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [0392] When it is determined that the purchasing information 353 and the card identification number information, the CPU 201 advances processing to step S264, purchasing information 353 corresponding to (having the same purchasing identifier as) the acquired purchasing information is retrieved from the storage unit 223, and the purchasing information 353 provided by the purchaser mobile telephone 11-3 and card identification number 351-3 contained in the card identification number information are authenticated using the retrieved purchasing information 353. Abe '171 at [0465] Namely, in step S401 to step S403 of FIG. 44, the CPU 251 makes a request to and acquires from the mobile telephone 11 the purchasing information 353 and the card identification number information. In the processing of step S404 and step S405, purchasing information corresponding to (having the same purchasing identifier as) the purchasing information 353 acquired from the mobile telephone 11 is requested from the point-of-purchase server 21 and is acquired. Abe '171 at claim 35 a generating step for generating information relating to said commercial transaction during product sales; *See also* [1b] and [9b] and 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.
[15c] a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that	Abe '171 discloses or renders obvious "a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number." For example: Abe '171 at Figure 5

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
represents a single transaction account number.	FIG. 5  Abe '171 at Fig. 12 FIG. 12  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 [0011] Information relating to the commercial transaction is made to contain a first identifier for identifying the commercial transaction, a second identifier for identifying whether or not payment of fees is complete for the commercial transaction, and the identification number of the information communication terminal used in the commercial transaction. 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

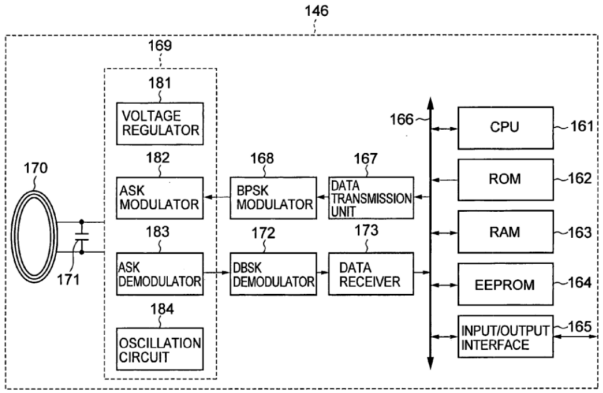
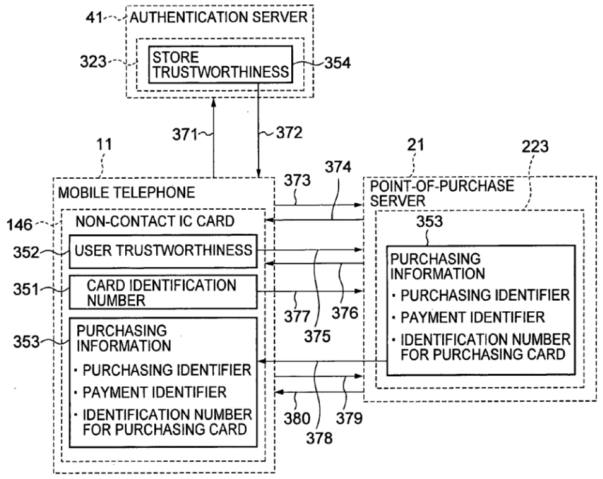
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	purchasing. Acquired information relating to the commercial transaction is then stored. Information relating to the stored commercial transaction is then provided to the information processing apparatus during receipt of the merchandise. 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 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]

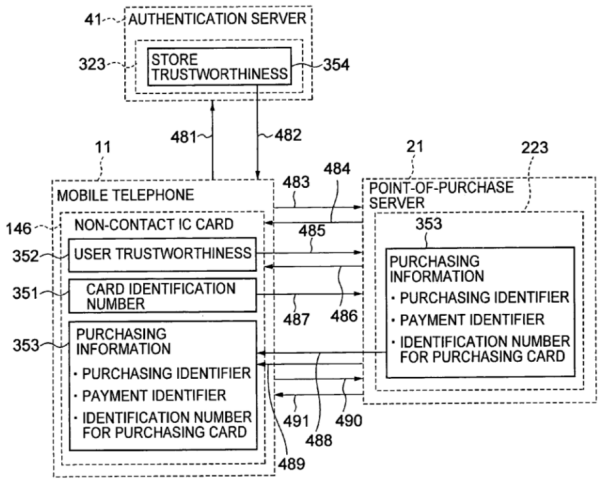
Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	The non-contact IC card 146 may then be brought close to another information processing apparatus having an IC card reader/writer so that when electromagnetic waves radiated from the IC card reader/writer are received, various information 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 [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 [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]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	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 [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 [0179] The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method. Abe ’171 at [0199] As shown in FIG. 12, the purchasing information 353 is comprised of a purchasing identifier for identifying the corresponding commercial transaction, a payment identifier for identifying whether or not payment for the sale of the merchandise has been made, and a purchasing card identification number constituted by the card identification number 351 allotted to the non-contact IC card 146 in the possession of the user purchasing the merchandise. Abe ’171 at [0259] The point-of-receipt server 31 that has acquired the purchasing information 353 and the card identification number information (card identification number 351) acquires purchasing information 353

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	(i.e. purchasing information for which the contained purchasing identifier is the same) corresponding to the acquired purchasing information 353 from the point-of-purchase server 21 (arrow 403 and arrow 404). 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 [0284] When it is determined that the purchasing information 353 and the card identification number information have been acquired, the CPU 251 advances processing to step S114, controls the communication unit 274, and makes a request to the point-of-purchase server 21 for purchasing information 353 (for which the purchasing identifier is the same) corresponding to the purchasing information 353 acquired from the non-contact IC card 146. This processing corresponds to the processing of arrow 403 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

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [0392] When it is determined that the purchasing information 353 and the card identification number information, the CPU 201 advances processing to step S264, purchasing information 353 corresponding to (having the same purchasing identifier as) the acquired purchasing information is retrieved from the storage unit 223, and the purchasing information 353 provided by the purchaser mobile telephone 11-3 and card identification number 351-3 contained in the card identification number information are authenticated using the retrieved purchasing information 353. Abe '171 at [0465] Namely, in step S401 to step S403 of FIG. 44, the CPU 251 makes a request to and acquires from the mobile telephone 11 the purchasing information 353 and the card identification number information. In the processing of step S404 and step S405, purchasing information corresponding to (having the same purchasing identifier as) the purchasing information 353 acquired from the mobile telephone 11 is requested from the point-of-purchase server 21 and is acquired. *See also* 1[b] and 9[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.
16. The mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry.	Abe '171 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry." For example: Abe '171 at Figure 5

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 5  Abe '171 at Fig. 12 FIG. 12  Abe '171 at Fig. 36

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	FIG. 36  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 [0178]

Claim Element	Exemplary Citations to US20050086171A1 ("Abe '171")
	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 [0179] The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method. Abe '171 at [0199] As shown in FIG. 12, the purchasing information 353 is comprised of a purchasing identifier for identifying the corresponding commercial transaction, a payment identifier for identifying whether or not payment for the sale of the merchandise has been made, and a purchasing card identification number constituted by the card identification number 351 allotted to the non-contact IC card 146 in the possession of the user purchasing the merchandise. *See also* claims 5 and 8 and 9[b] 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 15 above.
17. The mobile phone of claim 15 wherein the single transaction account numbers have a pre-defined sequence.	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 15 above.
18. The mobile phone of claim 15 wherein the single transaction account numbers comprise pre-	Abe '171 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: *See* above at claim 14.

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
assigned single-use transaction numbers.	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 15 above.

Patent Owner's Ex. 2021
Page 083

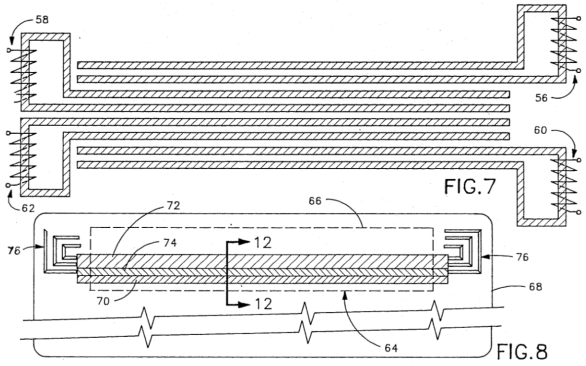
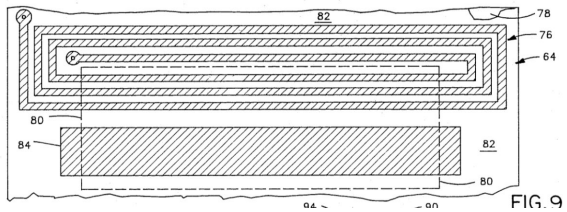
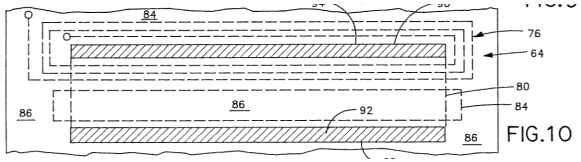
DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 9,208,423

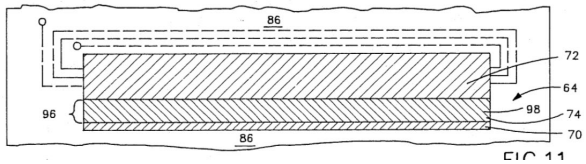
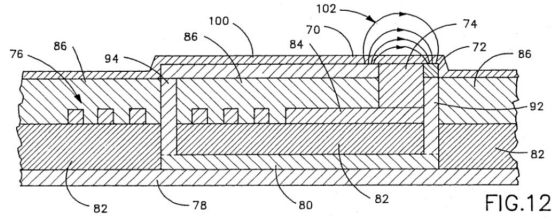
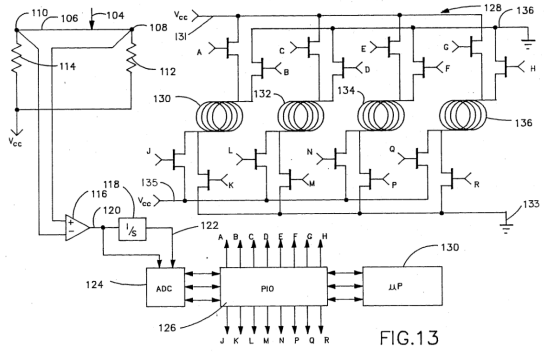
EXHIBIT F2: US4791283A ("Burkhardt '283")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,208,423 ("the '423 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 F and Exhibits F1–F5, 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 '423 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 '423 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 phone 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 phone." For example: 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; and	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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 1:8–10 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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

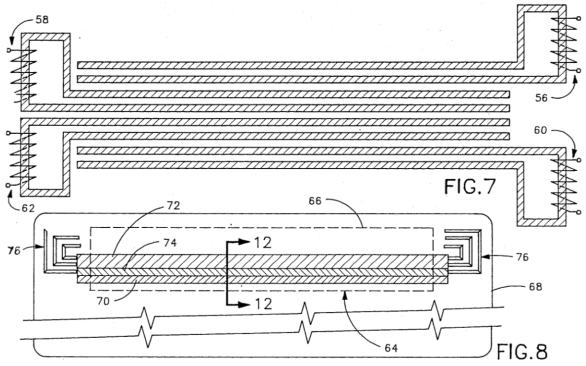
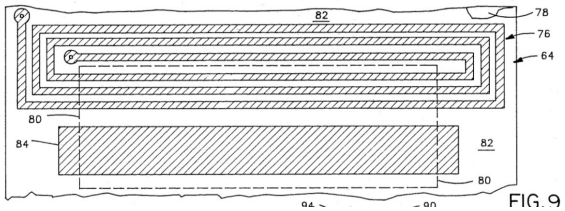
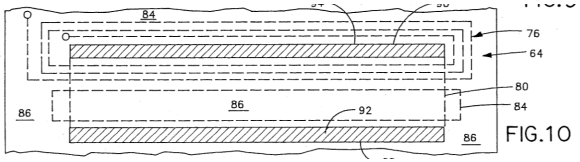
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	magnetic field generator for sequentially generating magnetic fields across substantially the entire portion of the predetermined area in response to the data, the magnetic fields having a field strength substantially equivalent to prerecorded 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 4:9–13 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

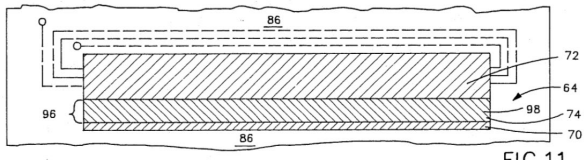
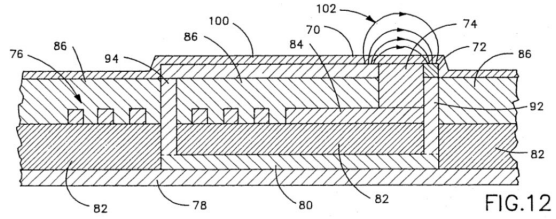
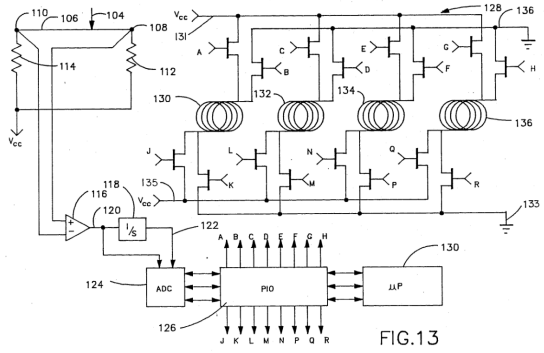
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	provide power contacts for providing supplemental power which can be applied to the internal power supply of the card 10 and/or quadrature driving circuits. Burkhardt '283 at 6:15–22 FIG. 7 is a schematic plan view illustrating the manner 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 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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 processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents a single transaction account number.	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 a single transaction account number." 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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.

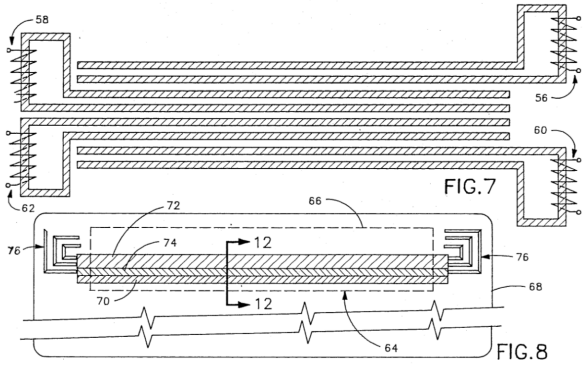
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 3:30–49 The advantages of the present invention are that specially designed card readers are not required to interact with the magnetic field generator of the present invention. The present invention emulates a prerecorded 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

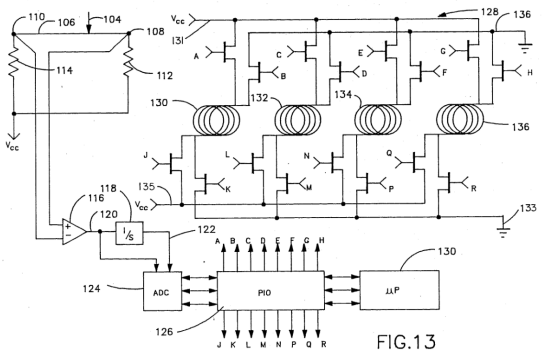
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	6. A method of transferring data from a transaction card to a card reader as said card is moved through said card reader by emulating a magnetic stripe disposed on a predetermined area on said card comprising the steps of: Burkhardt '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 10:63–68 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.
2. The mobile phone 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 phone 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

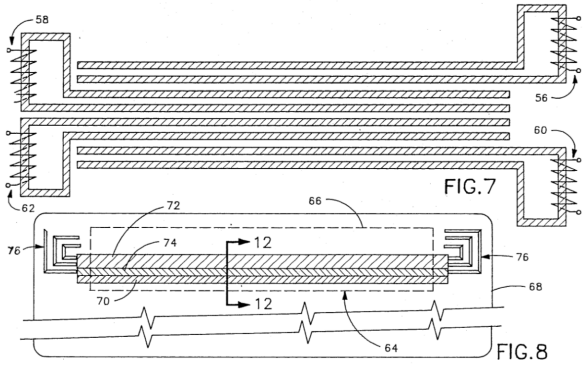
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	magnetic stripe of a transaction card. This allows transfer of data from a microprocessor to standard card readers without the necessity of substantially modifying the card reader device. Circuitry is also provided for detecting the 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 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 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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: 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 phone of claim 1 wherein the single transaction account number represents 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.

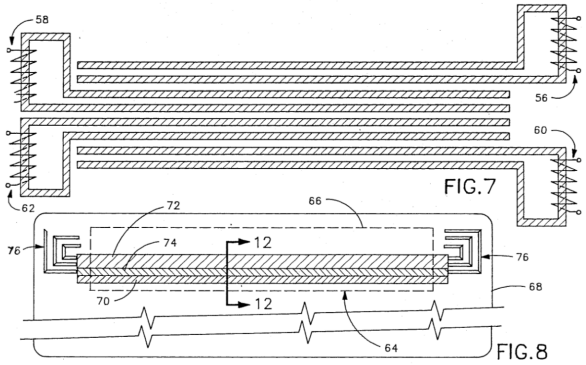
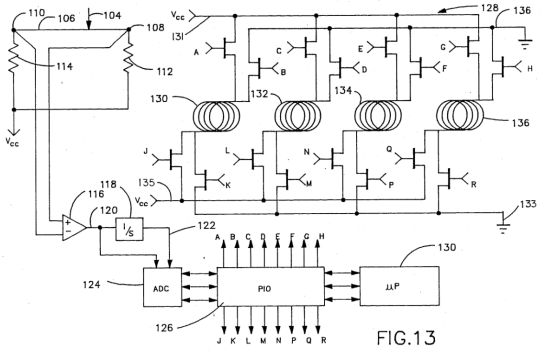
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
4. The mobile phone of claim 3 wherein the financial data comprises credit card data.	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the 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 phone of claim 1 further comprising smartcard circuitry coupled to the processor.	Burkhardt '283 discloses or renders obvious "[t]he mobile phone of claim 1 further comprising smartcard circuitry coupled to the processor." For example: Burkhardt '283 at Fig. 13  FIG.13 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 phone 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 phone 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

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 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.

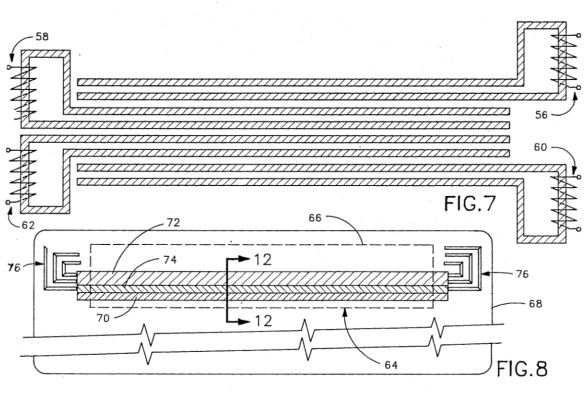
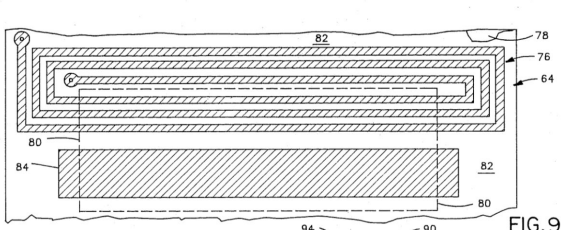
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 6:15–22 FIG. 7 is a schematic plan view illustrating the manner in which four magnetic field generators 56, 58, 60, 62 may be disposed on the card to form four separate magnetic stripes which emulate four prerecorded 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 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 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;

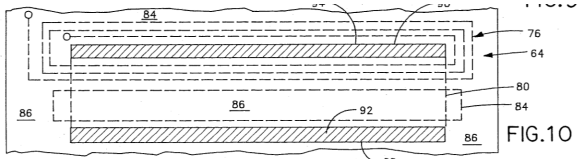
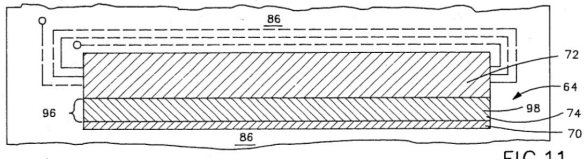
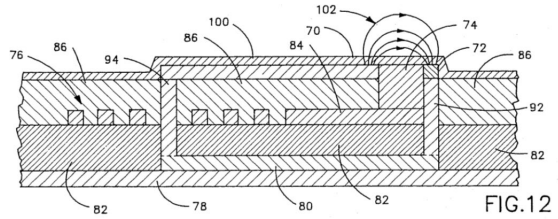
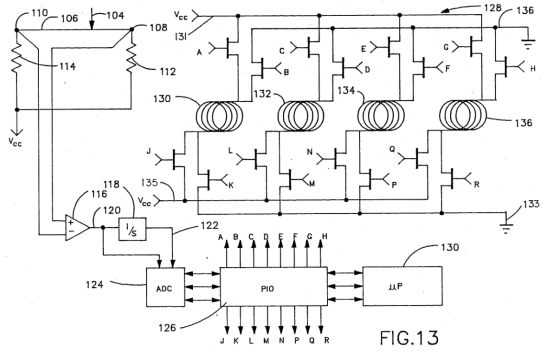
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	Burkhardt '283 at 10:25–28 A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader comprising: Burkhardt '283 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: *See also* 1[a] 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 1 above.
9[pre]. A mobile phone 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 phone." For example: 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 using single transaction account numbers; and	Burkhardt '283 discloses or renders obvious "smartcard circuitry for performing transactions using single transaction account numbers." 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 Fig. 13  FIG.13

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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* [1b] and 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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  Burkhardt '283 at Figure 9  Burkhardt '283 at Figure 10

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 FIG.10 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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

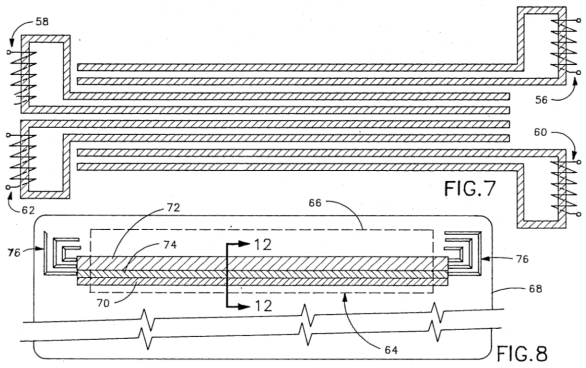
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	The present invention is therefore comprised of a device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from the transaction card to a card reader comprising 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 4:9–13 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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. 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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. 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

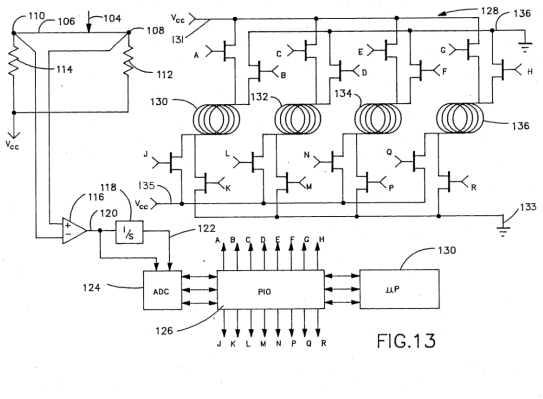
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	1. A device for emulating a magnetic stripe having prerecorded data disposed in a predetermined area on a transaction card to transfer data from said transaction card to a card reader as said card is moved through said card reader, comprising: 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 10:31–36 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[b] and claim 5 above.

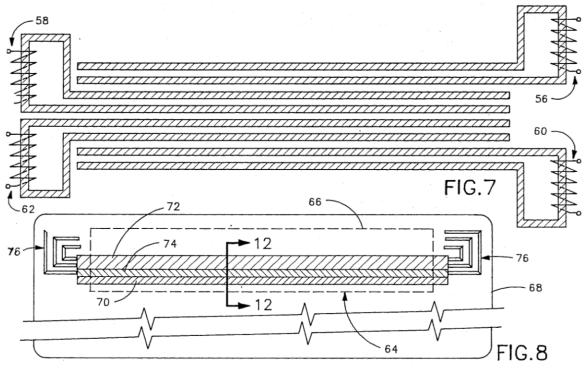
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	To the extent this limitation is not disclosed by Burkhardt '283, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Burkhardt '283, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
10. The mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Burkhardt '283 discloses or renders obvious "[t]he mobile phone 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

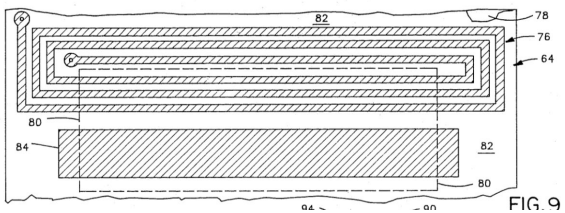
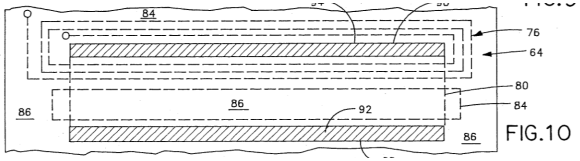
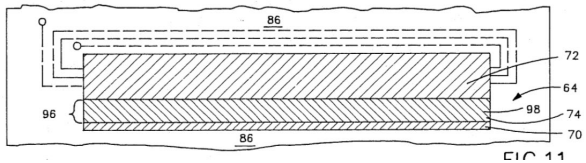
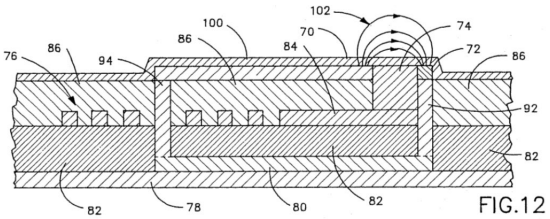
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	sequentially applies the data to the magnetic field generator so that the magnetic field for each data bit is sequentially produced along the entire length of the magnetic recording stripe. The present invention also includes a device 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

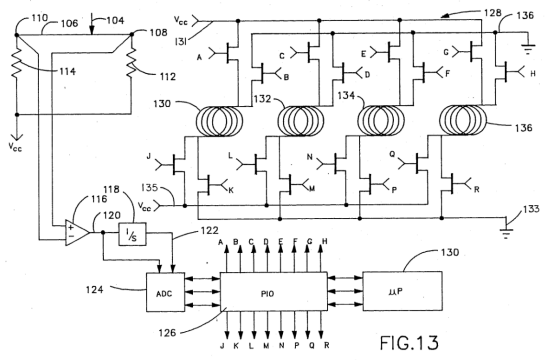
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	that each data bit is sequentially generated along the entire length of the magnetic stripe 12. As also illustrated in FIG. 1, transaction card 10 includes a signature line 14, an embossed account number 16 and an embossed expiration 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 phone 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 phone 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 phone 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.
13. The mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence.	Burkhardt '283 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence." For example: 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.
14. The mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	Burkhardt '283 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: 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.
15[pre]. A mobile phone 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 phone." For example: 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.
[15a] 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.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
[15b] circuitry to enable use of single transaction account numbers; and	Burkhardt '283 discloses or renders obvious "circuitry to enable use of single transaction account numbers." For example: Burkhardt '283 at Fig. 13  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* [1b] and [9b] and 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.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
[15c] a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number.	Burkhardt '283 discloses or renders obvious "a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number." 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 Figure 9

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 Burkhardt '283 at Figure 10  Burkhardt '283 at Figure 11  Burkhardt '283 at Figure 12  Burkhardt '283 at Fig. 13

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	 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 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

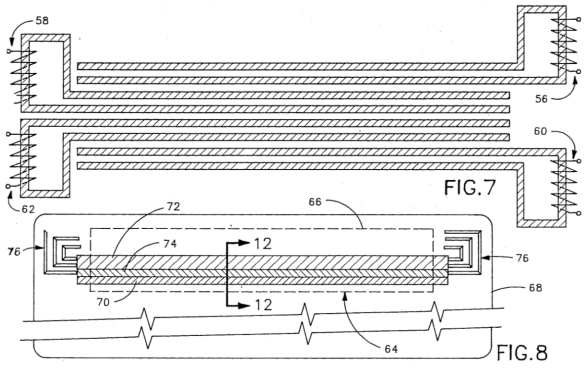
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	storage with high resolution. The Springer patents disclose various plating techniques for forming the concentric magnetic structures. Burkhardt '283 at 3:5–17 The present invention overcomes the disadvantages and limitations of the 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. 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

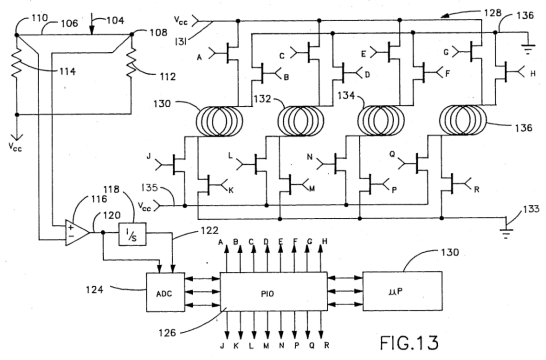
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	FIG. 7 is a schematic view illustrating the manner in which multiple magnetic field generators can be used to emulate multiple prerecorded magnetic stripes. Burkhardt '283 at 4:9–13 FIG. 13 is a schematic diagram of the device of the 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 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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. 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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. 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.

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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[b] and 9[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.
16. The mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry.	Burkhardt '283 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry." For example: Burkhardt '283 at Figs. 7+8  FIG.7 FIG.8 Burkhardt '283 at Fig. 13

Claim Element	Exemplary Citations to US4791283A (“Burkhardt ’283”)
	 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. 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

Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
	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 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. *See also* claims 5 and 8 and 9[b] 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 15 above.
17. The mobile phone of claim 15 wherein the single transaction account numbers have a pre-defined sequence.	Burkhardt '283 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the single transaction account numbers have a pre-defined sequence." For example: *See also* claim 13 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 15 above.

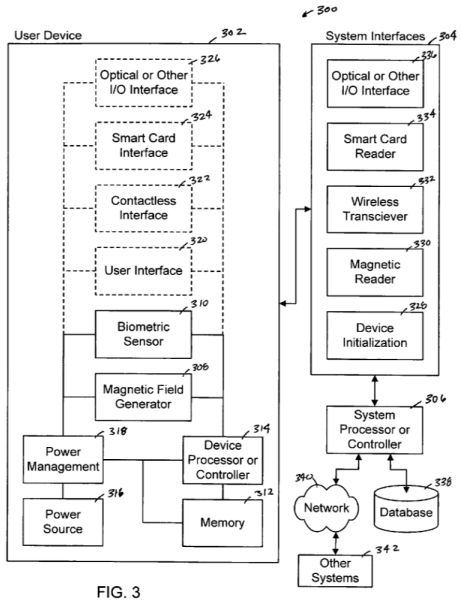
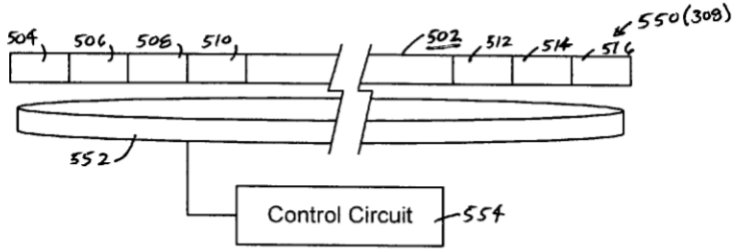
Claim Element	Exemplary Citations to US4791283A ("Burkhardt '283")
18. The mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	Burkhardt '283 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: 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 15 above.

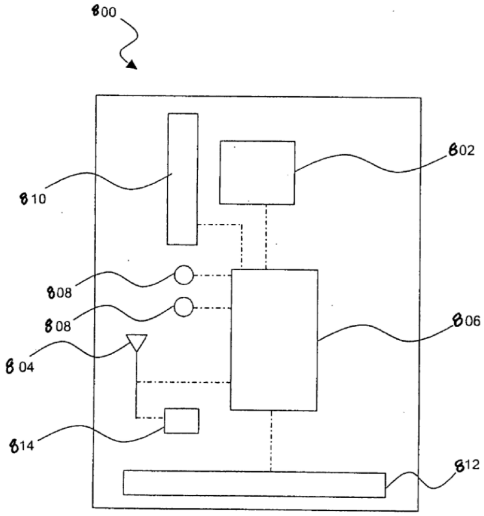
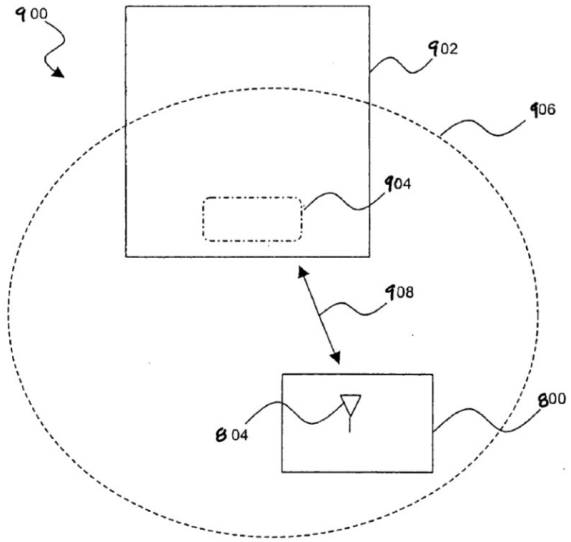
As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,208,423 ("the '423 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Doughty '787 and (b) under 35 U.S.C. § 103(a) as obvious over Doughty '787 standing alone and as set forth herein, and/or 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 F and Exhibits F1–F5, 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 '423 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.

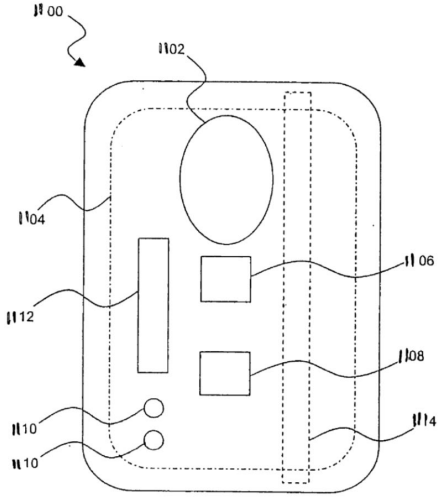
Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '423 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's 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 phone 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 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

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; and	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

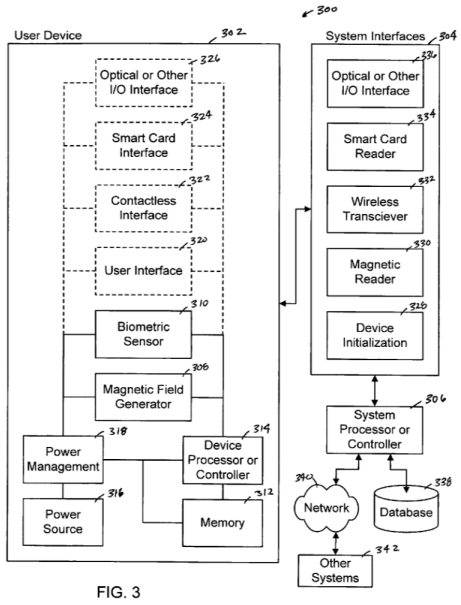
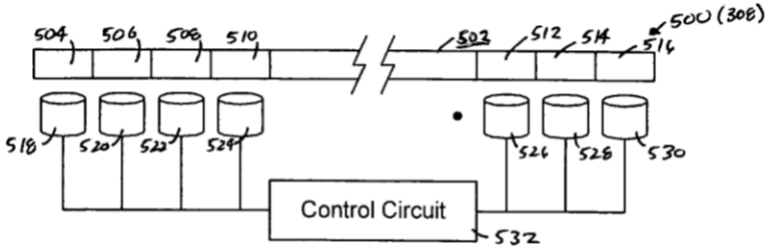
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to 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

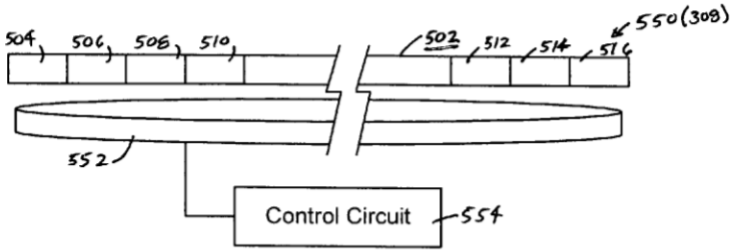
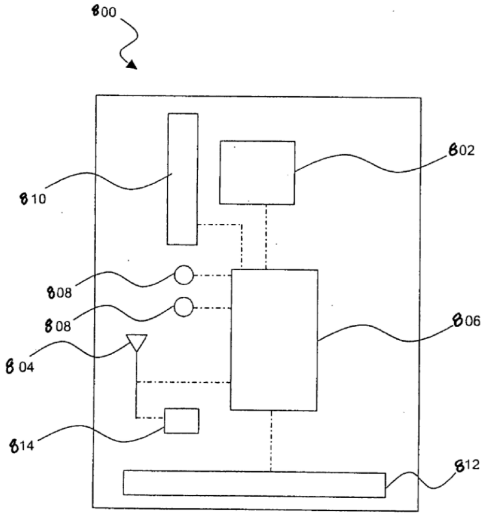
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	magnetic field generator has been active for a specified period of time) or the biometric sensor no longer detects the authorized user. Note that this method can be performed by a computer program, such as middleware, embodied in 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.

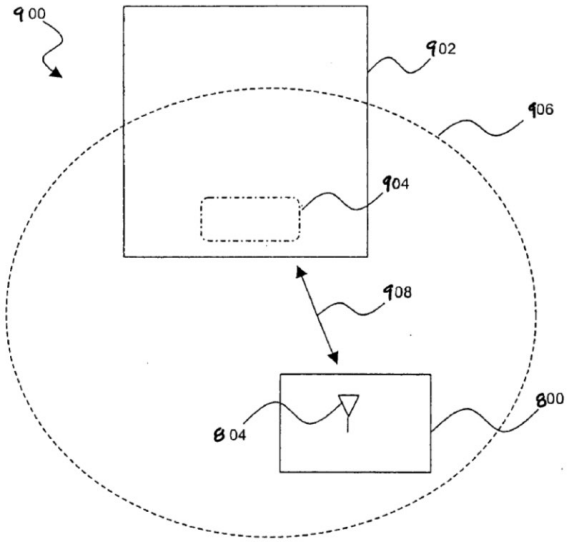
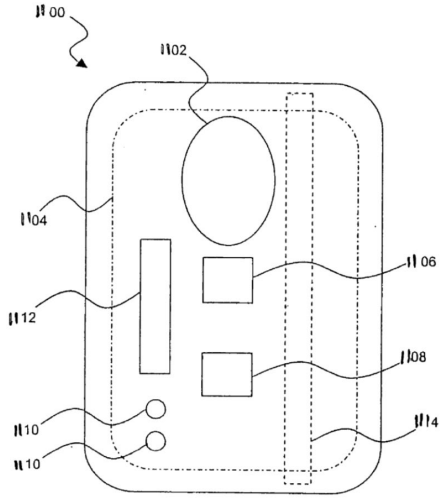
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at [0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the 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 processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents a single transaction account number.	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 a single transaction account number." 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

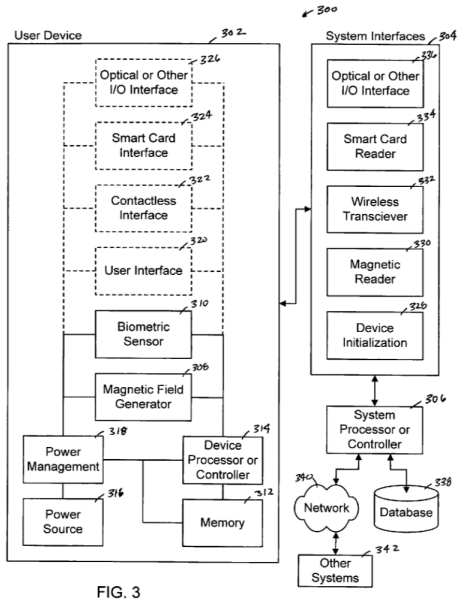
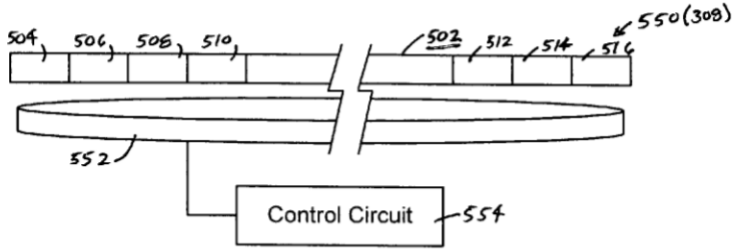
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media 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

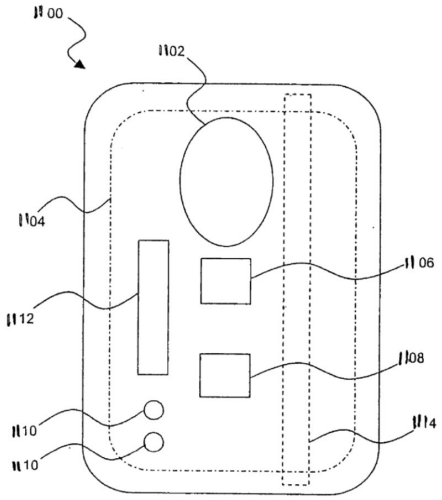
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	antennae 903 to communicate with device 800, as well as emanate a RF field 906 with the purpose of supplying power to compatible devices, such as device 800. In operation, a two-way communication link 908 may be established between 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.

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.
2. The mobile phone 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 phone 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.

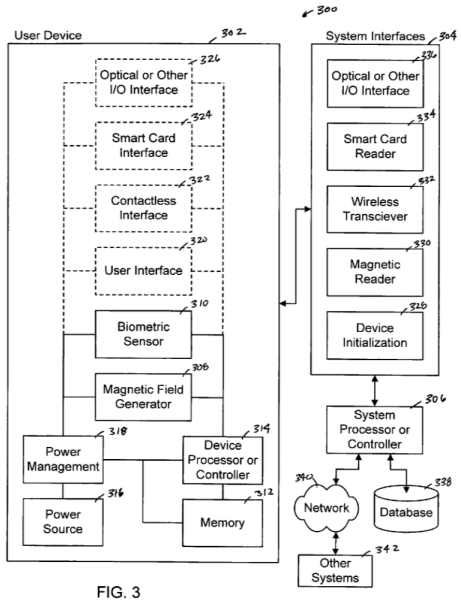
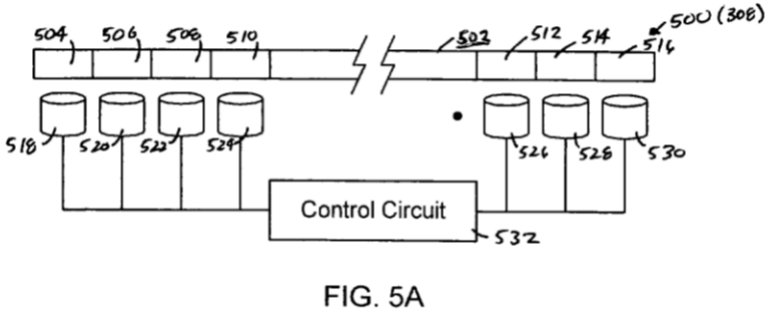
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
3. The mobile phone of claim 1 wherein the single transaction account number represents financial data.	To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art 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 phone of claim 3 wherein the financial data comprises credit card data.	Doughty '787 discloses or renders obvious "[t]he mobile phone of claim 3 wherein the financial data comprises credit card data." 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 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

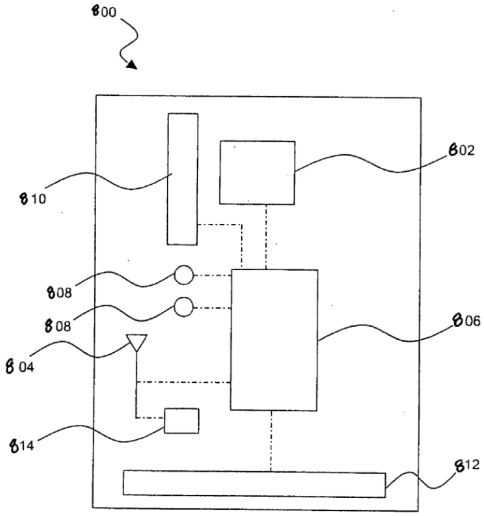
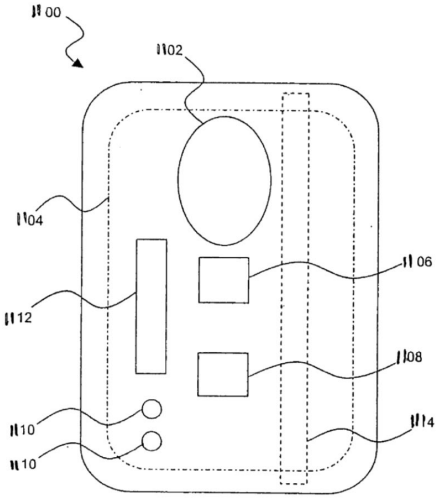
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into 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 [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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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] 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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	(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] 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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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. 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 phone of claim 1 further comprising smartcard circuitry coupled to the processor.	Doughty '787 discloses or renders obvious "[t]he mobile phone of claim 1 further comprising smartcard circuitry coupled to the processor." 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 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]–[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 [0012]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 [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 [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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 [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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 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

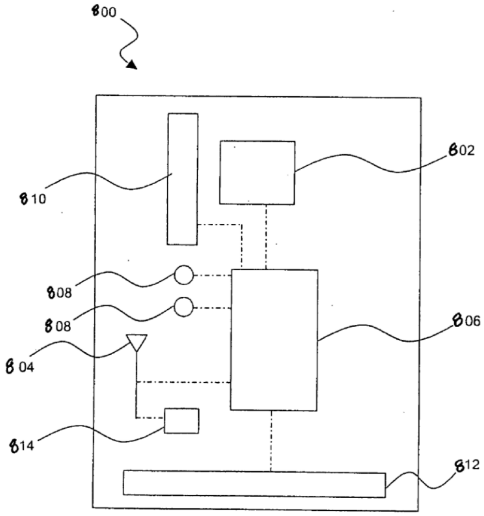
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	814. A number of inter-component communications paths 816 provide connections between various components of the device 800. Doughty '787 at [0059] The controller 806 interacts with the biometric sensor 802 and other components of 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 [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.

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 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 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 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.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
8, The mobile phone 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 phone 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 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

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 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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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. *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. *See also* claim 1 above.
9[pre]. A mobile phone 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 phone." 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]. 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 using single transaction account numbers; and	Doughty '787 discloses or renders obvious "smartcard circuitry for performing transactions using single transaction account numbers." For example: Doughty '787 at Figure 8

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

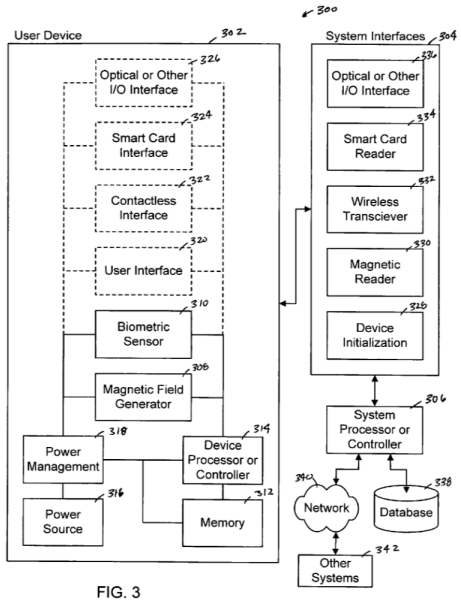
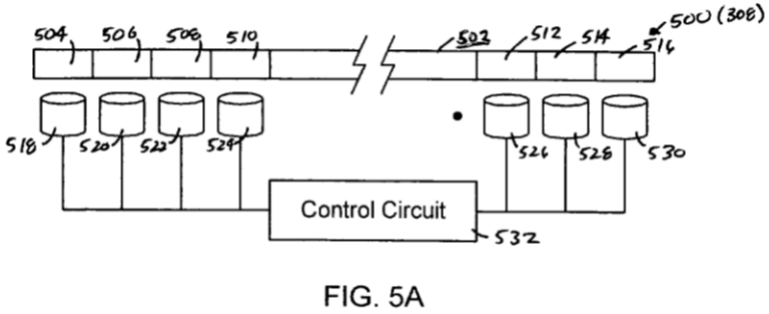
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely 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

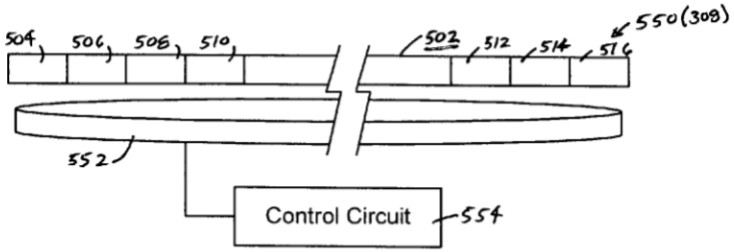
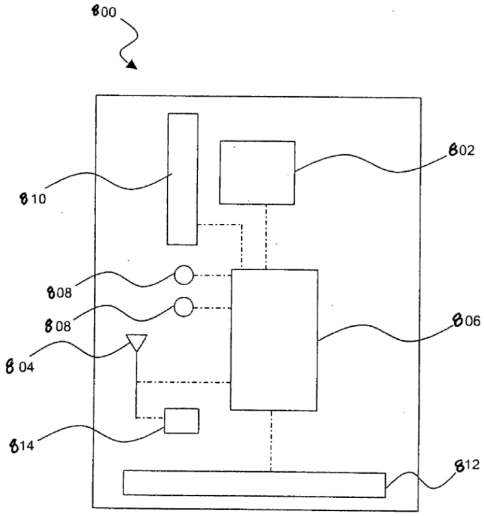
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more 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,

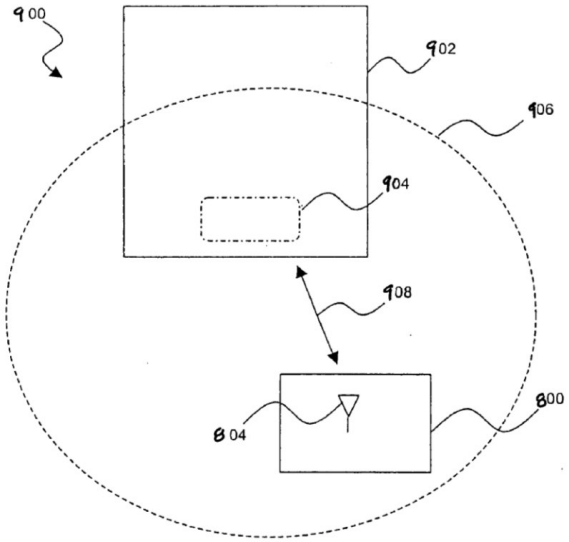
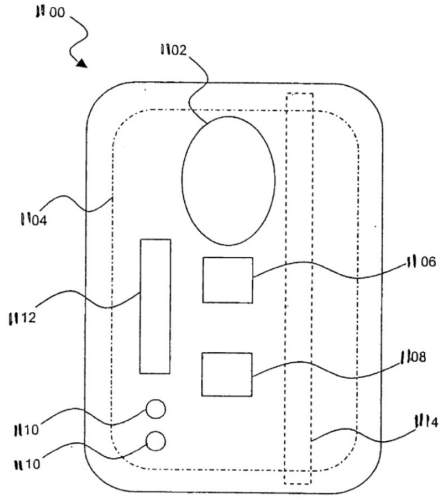
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received 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 [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, 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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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. 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.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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* [1b] and 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 [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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 [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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 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]

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 [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

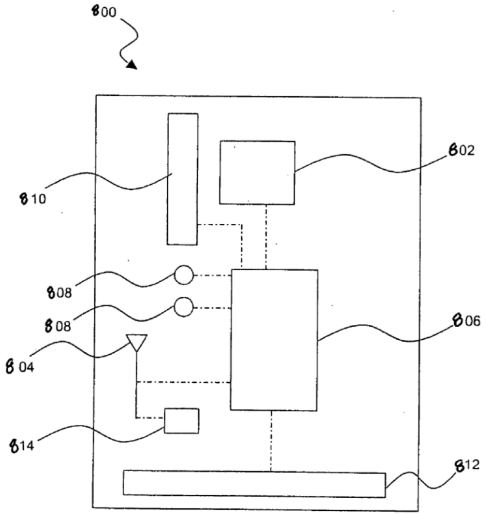
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	information output step (block 722) may also display information to the user, allow the user to select the information to enable the transaction or allow the user to select the device output or interface to be used. Once the transaction 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 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

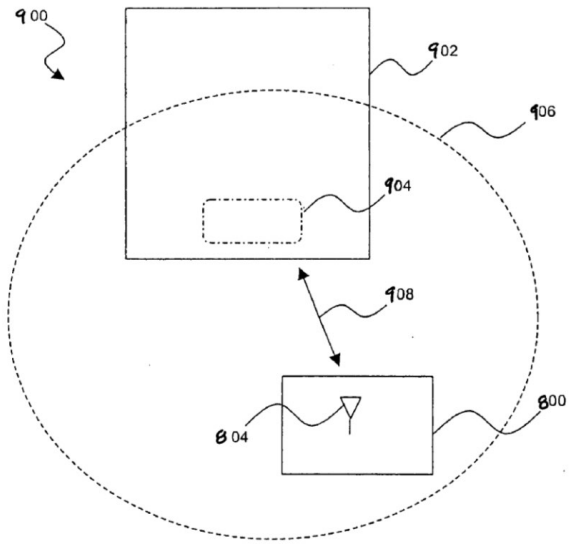
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	components, such as audio or optical components, may replace or supplement the antenna 804. In addition, the antenna 804 may be operable to function with wavelengths other than RF. Doughty '787 at [0059] The controller 806 interacts 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 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 [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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 [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 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.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	88. The system as recited in claim 60, wherein the device processor and the memory are integrated into a single integrated circuit. *See also* [1b] and claim 5 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.
10. The mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Doughty '787 discloses or renders obvious "[t]he mobile phone 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 phone of claim 9 wherein the transactions are financial transactions.	Doughty '787 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the transactions are financial transactions." 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

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 [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. 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

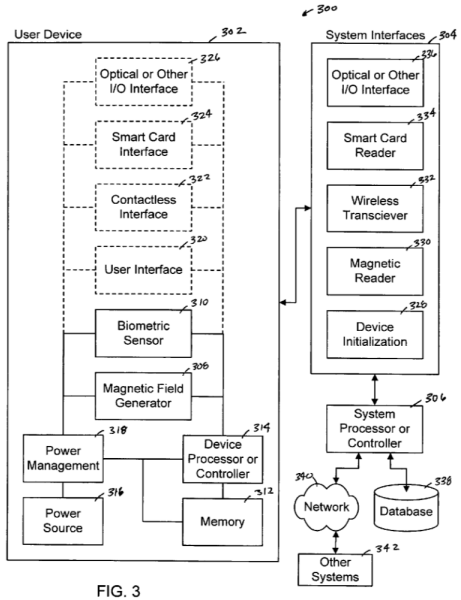
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased 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 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.

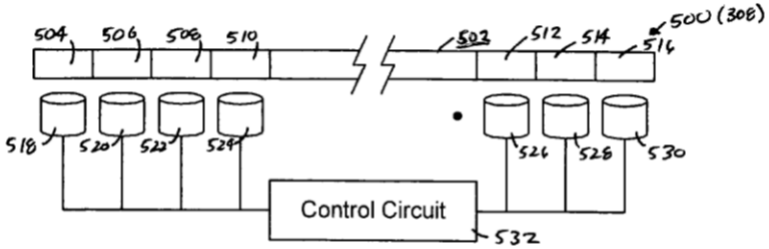
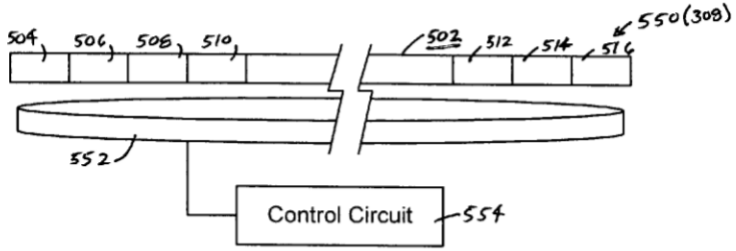
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 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] 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

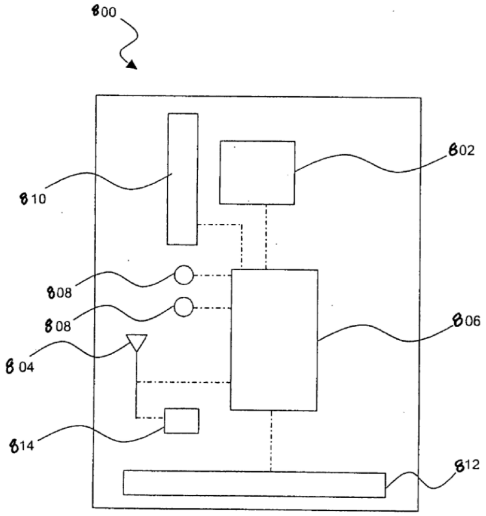
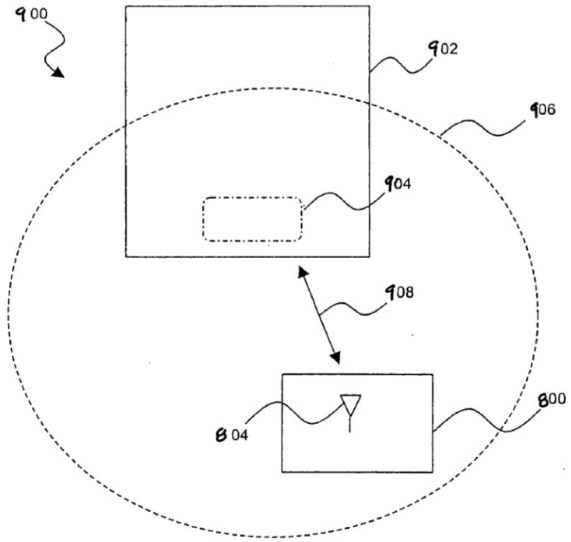
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	function control buttons 1110. For example, the buttons 1110 may be used to select a credit card number (if the device 1100 stores multiple numbers) viewed via the display 1112 or to enter a personal identification number. The pliability 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] 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

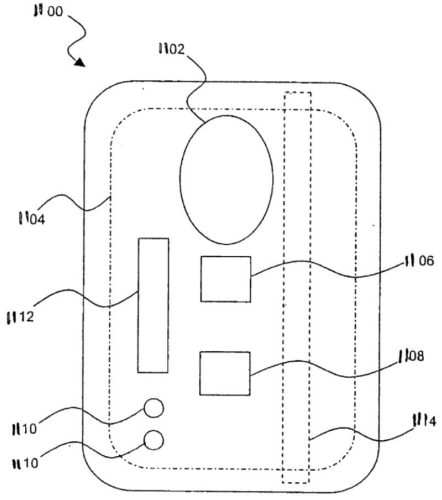
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	compare the buyer's signature on the back of the card presented for payment versus the requested signature on the purchase receipt provided for the goods or services purchased. In some cases, cards have a photograph of the card owner 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. *See also* claim 3 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.
12. The mobile phone 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 phone 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.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
13. The mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence.	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.
14. The mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	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.
15[pre]. A mobile phone 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 phone." 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.
[15a] 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]. 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.
[15b] circuitry to enable use of single transaction account numbers; and	*See also* [1b] and [9b] and 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.
[15c] a processor coupled to the circuitry to produce a time-varying	Doughty '787 discloses or renders obvious "a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number.	configured to cause a time-varying magnetic field to be produced that represents a single transaction account number." 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 Doughty '787 at Fig. 5A

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 5A 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 [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 [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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 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.

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 [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

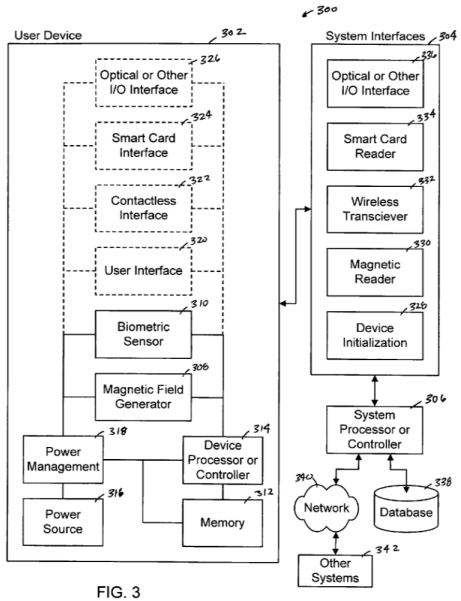
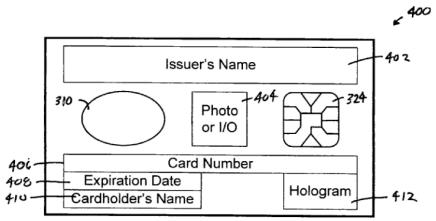
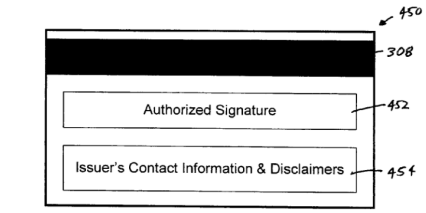
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	308 and generating a magnetic signal corresponding to the information associated with the authenticated user. In addition, the authentication step (block 716), the information access step (block 720) or the information output step (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 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

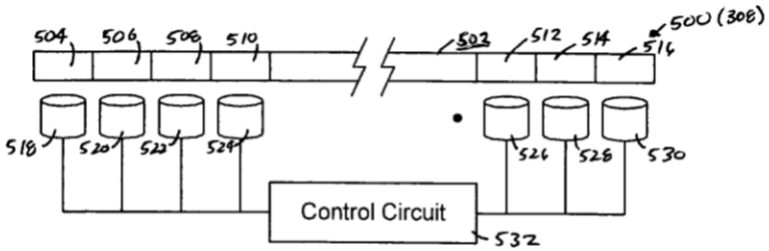
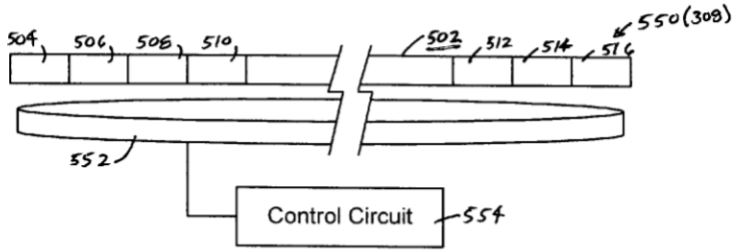
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	secured using mechanisms such as data encryption. It is understood that other communications components, such as audio or optical components, may replace or supplement the antenna 804. In addition, the antenna 804 may be operable 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 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]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 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

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 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 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[b] and 9[c] and claim 5 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.
16. The mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry.	Doughty '787 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry." For example: Doughty '787 at Fig. 3

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	 FIG. 3 Doughty '787 at Fig. 4A–B  FIG. 4A  FIG. 4B

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	Doughty '787 at Fig. 5A  FIG. 5A Doughty '787 at Fig. 5B  FIG. 5B 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 [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 [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 [0048]

Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	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 [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 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 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 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 and 9[b] above.

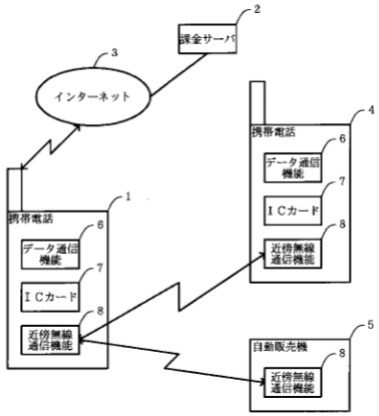
Claim Element	Exemplary Citations to US20040133787A1 ("Doughty '787")
	To the extent this limitation is not disclosed by Doughty '787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty '787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 15 above.
17. The mobile phone of claim 15 wherein the single transaction account numbers have a pre-defined sequence.	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 15 above.
18. The mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	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 15 above.

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,208,423 ("the '423 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 F and Exhibits F1–F5, 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 '423 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.

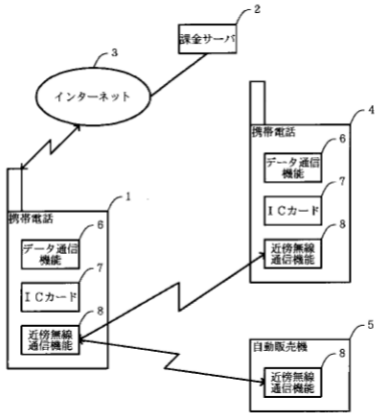
Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '423 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's 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 phone 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 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

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 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]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 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.

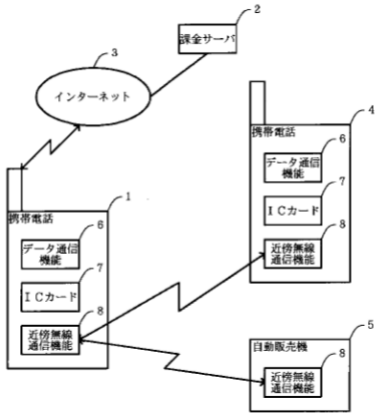
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
[1a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card; and	Haginiwa '847 discloses or renders obvious "circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card." 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.

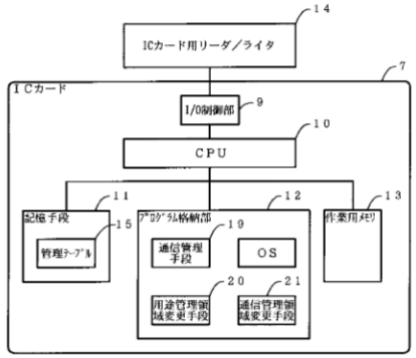
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at [0040] The near field communication function 8 is for performing wireless communication at a short distance such as Bluetooth (registered trademark). For example, the mobile phone 1 is provided with the near field 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 processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents a single transaction account number.	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 a single transaction account number." 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]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 [0017] According to a sixth aspect of the present invention, in the IC card according to the first to fifth aspects described above, the communication management means is configured to use the communication identification means based on a use identification number received from a near-field communication wireless function of a peripheral device. The communication management area is searched to determine whether or not to perform communication using the near field communication wireless function indicated by the use identification number. Haginiwa '847 at [0018] According to a seventh aspect of the present invention, in the IC card according to any one of the first to sixth aspects described above, the communication management means includes: With the use identification number and the electronic certificate received from the wireless function for near field communication of the devices present in the vicinity, configured to confirm the presence or absence of unauthorized use in addition to the propriety of communication by the wireless function for near field communication. It is. 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 [0026]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 [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] 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 [0052] The near field communication function 8 of the mobile phone 1 receives the use identification number "9999" from the vending machine 5, activates the communication management means 19, and determines whether to permit the reception of the use identification number "9999". Request a judgment.

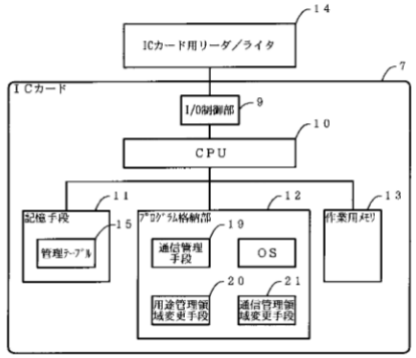
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Haginiwa '847 at [0053] The communication management unit 19 searches the communication management area 18 using the use identification number "9999". Since "0" indicating permission to receive the application identification number "9999" is set in the communication management area 18, the near-field wireless communication with the vending machine 5 is continued. Haginiwa '847 at [0073] 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 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.
2. The mobile phone of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." For example: 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.

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. 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 phone of claim 1 wherein the single transaction account number represents financial data.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 1 wherein the single transaction account number represents financial data." For example: Haginiwa '847 at [0016] According to a fifth aspect of the present invention, there is provided the IC card according to the first to fourth aspects, wherein communication enable / disable information for each application identification number stored in the communication management area in response to a user input of the portable information terminal is input. A communication management area changing means capable of adding, changing, and deleting is provided. Haginiwa '847 at [0017] According to a sixth aspect of the present invention, in the IC card according to the first to fifth aspects described above, the communication management means is configured to use the communication identification means based on a use identification number received from a near-field communication

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	wireless function of a peripheral device. The communication management area is searched to determine whether or not to perform communication using the near field communication wireless function indicated by the use identification number. Haginiwa '847 at [0018] According to a seventh aspect of the present invention, in the IC card according to any one of the first to sixth aspects described above, the communication management means includes: With the use identification number and the electronic certificate received from the wireless function for near field communication of the devices present in the vicinity, configured to confirm the presence or absence of unauthorized use in addition to the propriety of communication by the wireless function for near field communication. It is. 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 [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 [0052] The near field communication function 8 of the mobile phone 1 receives the use identification number "9999" from the vending machine 5, activates the communication management means 19, and determines whether to permit the reception of the use identification number "9999". Request a judgment. Haginiwa '847 at [0073] 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

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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. 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.
4. The mobile phone of claim 3 wherein the financial data comprises credit card data.	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 phone of claim 1 further comprising smartcard circuitry coupled to the processor.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 1 further comprising smartcard circuitry coupled to the processor." For example: 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 [citation unavailable] FIG. 2 is a schematic configuration diagram of the inside of an IC card (UIM) of the present invention. Haginiwa '847 at Figure 2

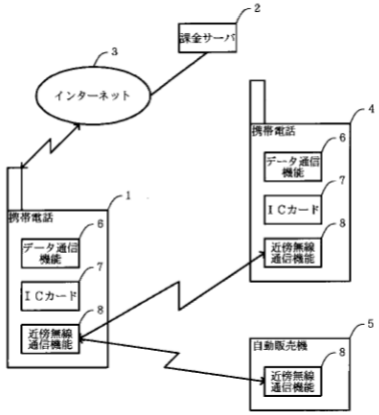
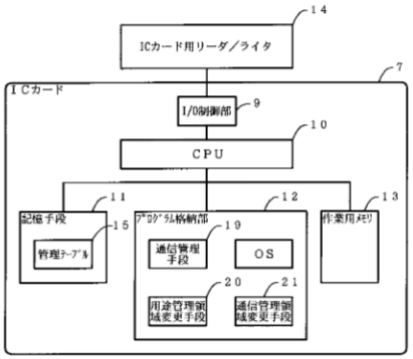
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図２】  To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 1 above.
8, The mobile phone 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 phone 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. *See also* 1[a] 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 1 above.
9[pre]. A mobile phone 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 phone." 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 using single transaction account numbers; and	Haginiwa '847 discloses or renders obvious "smartcard circuitry for performing transactions using single transaction account numbers." 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 [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 [0016] According to a fifth aspect of the present invention, there is provided the IC card according to the first to fourth aspects, wherein communication enable / disable information for each application identification number stored in the communication management area in response to a user input of the portable information terminal is input. A communication management area changing means capable of adding, changing, and deleting is provided. Haginiwa '847 at [0017] According to a sixth aspect of the present invention, in the IC card according to the first to fifth aspects described above, the communication management means is configured to use the communication identification means based on a use identification number received from a near-field communication wireless function of a peripheral device. The communication management area is searched to determine whether or not to perform communication using the near field communication wireless function indicated by the use identification number. Haginiwa '847 at [0018] According to a seventh aspect of the present invention, in the IC card according to any one of the first to sixth aspects described above, the communication management means includes: With the use identification number and the electronic certificate received from the wireless function for near field communication of the devices present in the vicinity, configured to confirm the presence or absence of unauthorized use in addition to the propriety of communication by the wireless function for near field communication. It is. Haginiwa '847 at [0020]

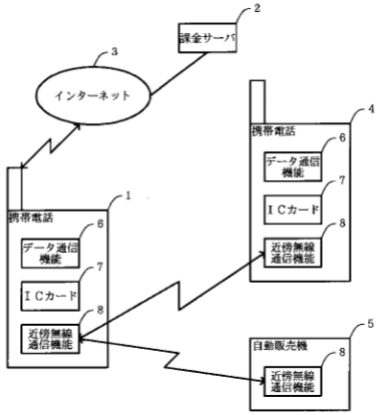
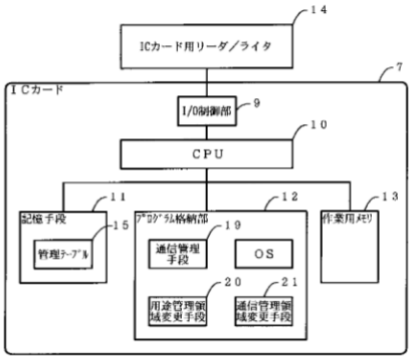
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	A ninth aspect of the present invention is a charging method using an IC card that is detachable from a portable information terminal that has a data communication function and can be connected to a wireless network. Receiving a use 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 [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] 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.

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 [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 [0052] The near field communication function 8 of the mobile phone 1 receives the use identification number "9999" from the vending machine 5, activates the communication management means 19, and determines whether to permit the reception of the use identification number "9999". Request a judgment. Haginiwa '847 at [0053] The communication management unit 19 searches the communication management area 18 using the use identification number "9999". Since "0" indicating permission to receive the application identification number "9999" is set in the communication management area 18, the near-field wireless communication with the vending machine 5 is continued. Haginiwa '847 at [0073] 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. 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

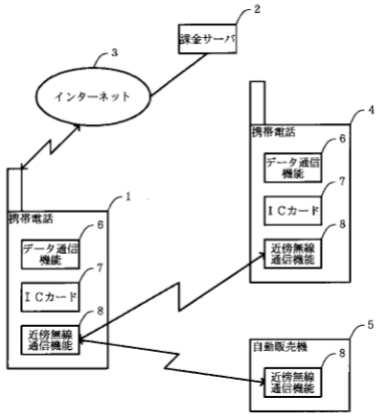
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図１】  Haginiwa '847 at Figure 2 【図２】  *See also* [1b] and claims 5 and 8 above. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings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

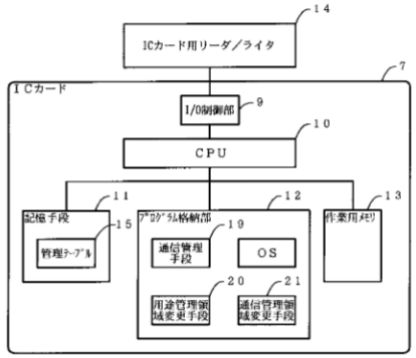
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	PROBLEM TO BE SOLVED: To provide an IC card and a charging method using an IC card in which, for near radiocommunication, whether or not receiving is possible and charging are controlled by exchanging use identification numbers for 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. 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.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 [citation unavailable] FIG. 2 is a schematic configuration diagram of the inside of an IC card (UIM) of the present invention. Haginiwa '847 at Figure 1

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図１】  Haginiwa '847 at Figure 2 【図２】  *See also* [1b] 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.
10. The mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions." For example: Haginiwa '847 at [0001]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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] 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.

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 [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 【図１】  Haginiwa '847 at Figure 2

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【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 phone of claim 9 wherein the transactions are financial transactions.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the transactions are financial 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.

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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* claim 3 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.
12. The mobile phone 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 phone 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.
13. The mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence.	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.
14. The mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: Haginiwa '847 at [0033] The use management area 17 is an area for storing, for example, the name of the use of the near field communication and the use identification number assigned to the communication use, as shown in FIG. The use management area 17 is provided in the memory of the mobile phone. Also, since the name of the

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	communication use and the use identification number are set in advance by agreement between devices performing near field communication, the storage unit 11 performs the use management. A configuration without the region 17 is also possible. 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 9 above.
15[pre]. A mobile phone 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 phone." 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.
[15a] 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.
[15b] circuitry to enable use of single transaction account numbers; and	Haginiwa '847 discloses or renders obvious "circuitry to enable use of single transaction account numbers." For example: Haginiwa '847 at Abstract

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 [0016] According to a fifth aspect of the present invention, there is provided the IC card according to the first to fourth aspects, wherein communication enable / disable information for each application identification number stored in the communication management area in response to a user input of the portable information terminal is input. A communication management area changing means capable of adding, changing, and deleting is provided. Haginiwa '847 at [0017] According to a sixth aspect of the present invention, in the IC card according to the first to fifth aspects described above, the communication management means is configured to use the communication identification means based on a use identification number received from a near-field communication wireless function of a peripheral device. The communication management area is searched to determine whether or not to perform communication using the near field communication wireless function indicated by the use identification number. Haginiwa '847 at [0018] According to a seventh aspect of the present invention, in the IC card according to any one of the first to sixth aspects described above, the communication management means includes: With the use identification number and the electronic certificate received from the wireless function for near field communication of the devices present in the vicinity, configured to confirm the presence or absence of unauthorized use in addition to the propriety of communication by the wireless function for near field communication. It is. 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

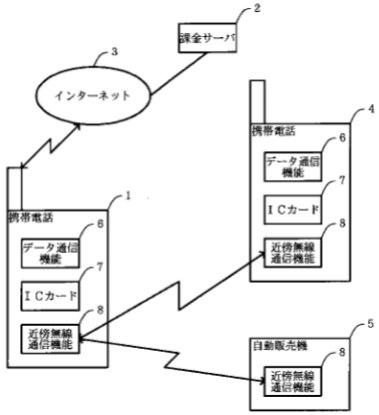
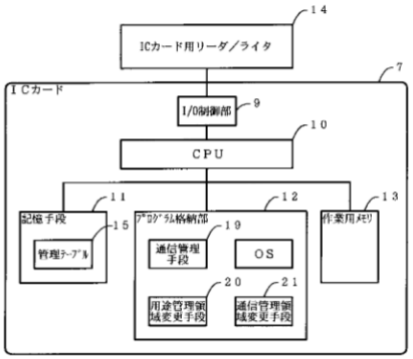
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	indicated by the application identification number. Adding the communication traffic of the communication to the communication traffic management area provided in the IC card, requesting the server to charge the communication traffic, and charging the communication traffic by the server. It is obtained to perform and performing. Haginiwa '847 at [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 [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 [0052] The near field communication function 8 of the mobile phone 1 receives the use identification number "9999" from the vending machine 5, activates the communication management means 19, and determines whether to permit the reception of the use identification number "9999". Request a judgment. Haginiwa '847 at [0053] The communication management unit 19 searches the communication management area 18 using the use identification number "9999". Since "0" indicating permission to receive the application identification number "9999" is set in the communication management area 18, the near-field wireless communication with the vending machine 5 is continued. Haginiwa '847 at [0073] 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

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	the billing server. It is possible to judge whether or not to perform communication according to, and to accumulate the communication amount. *See also* [1b] and [9b] and 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.
[15c] a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number.	Haginiwa '847 discloses or renders obvious "a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number." 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

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 [0016] According to a fifth aspect of the present invention, there is provided the IC card according to the first to fourth aspects, wherein communication enable / disable information for each application identification number stored in the communication management area in response to a user input of the portable information terminal is input. A communication management area changing means capable of adding, changing, and deleting is provided. Haginiwa '847 at [0017] According to a sixth aspect of the present invention, in the IC card according to the first to fifth aspects described above, the communication management means is configured to use the communication identification means based on a use identification number received from a near-field communication wireless function of a peripheral device. The communication management area is searched to determine whether or not to perform communication using the near field communication wireless function indicated by the use identification number. Haginiwa '847 at [0018] According to a seventh aspect of the present invention, in the IC card according to any one of the first to sixth aspects described above, the communication management means includes: With the use identification number and the electronic certificate received from the wireless function for near field communication of the devices present in the vicinity, configured to confirm the presence or absence of unauthorized use in addition to the propriety of communication by the wireless function for near field communication. It is. Haginiwa '847 at [0020]

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 [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 [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] 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]

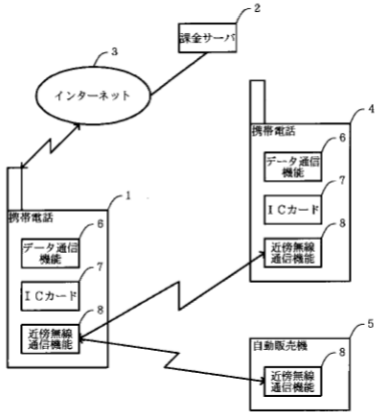
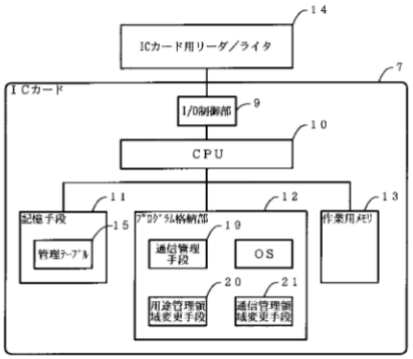
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	Hereinafter, 1) purchase a product from the vending machine 5; 2) the vending machine 5 transmits an advertisement mail of a new product to the mobile phone 1; Acquisition will be described. Haginiwa '847 at [0051] The vending machine 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 [0052] The near field communication function 8 of the mobile phone 1 receives the use identification number "9999" from the vending machine 5, activates the communication management means 19, and determines whether to permit the reception of the use identification number "9999". Request a judgment. Haginiwa '847 at [0053] The communication management unit 19 searches the communication management area 18 using the use identification number "9999". Since "0" indicating permission to receive the application identification number "9999" is set in the communication management area 18, the near-field wireless communication with the vending machine 5 is continued. Haginiwa '847 at [0073] 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 1

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図１】  Haginiwa '847 at Figure 2 【図２】  *See also* 1[b] and 9[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.
16. The mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry." For example: Haginiwa '847 at Abstract

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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 [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 [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 [0016] According to a fifth aspect of the present invention, there is provided the IC card according to the first to fourth aspects, wherein communication enable / disable information for each application identification number stored in the communication management area in response to a user input of the portable information terminal is input. A communication management area changing means capable of adding, changing, and deleting is provided. Haginiwa '847 at [0017] According to a sixth aspect of the present invention, in the IC card according to the first to fifth aspects described above, the communication management means is configured to use the communication identification means based on a use identification number received from a near-field communication wireless function of a peripheral device. The communication management area is searched to determine whether or not to perform communication using the near field communication wireless function indicated by the use identification number. Haginiwa '847 at [0018] According to a seventh aspect of the present invention, in the IC card according to any one of the first to sixth aspects described above, the communication management means includes: With the use identification number and the electronic certificate received from the wireless function for near field communication of the devices present in the vicinity, configured to confirm the presence or absence of unauthorized use in addition to the propriety of communication by the wireless function for near field communication. It is. 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

Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	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] 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 [0073] 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 claim 2 An IC card comprising: The IC card according to claim 1, Haginiwa '847 at Figure 1

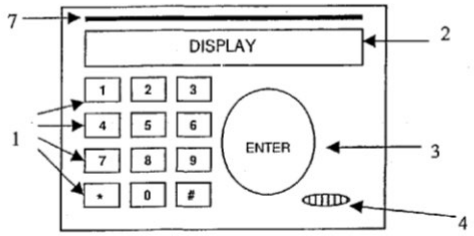
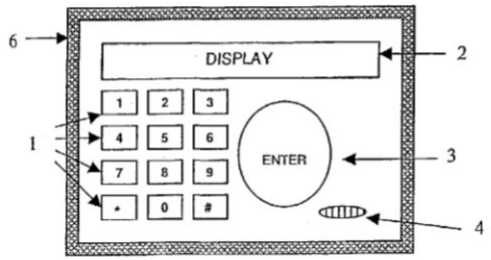
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
	【図１】  Haginiwa '847 at Figure 2 【図２】  *See also* claims 5 and 8 and 9[b] above. To the extent this limitation is not disclosed by Haginiwa '847, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Haginiwa '847, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. *See also* claim 15 above.
17. The mobile phone of claim 15 wherein the single transaction	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.

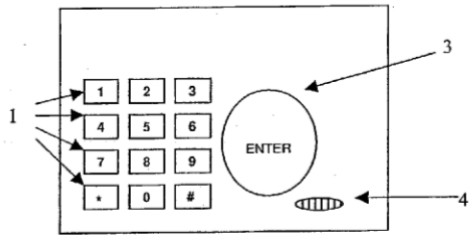
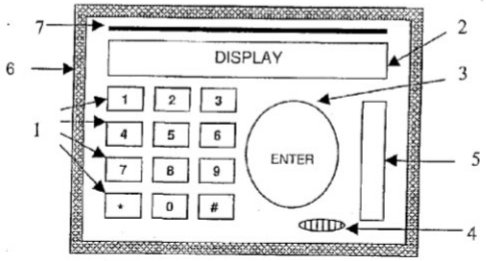
Claim Element	Exemplary Citations to JP2004240847A ("Haginiwa '847")
account numbers have a pre-defined sequence.	*See also* claim 15 above.
18. The mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	Haginiwa '847 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: *See* above at claim 14. 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 15 above.

As demonstrated in the claim charts below, the claims of U.S. Patent No. 9,208,423 ("the '423 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 F and Exhibits F1–F5, 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 '423 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 '423 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.

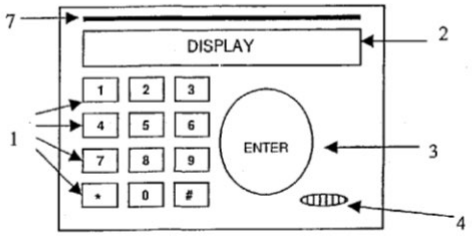
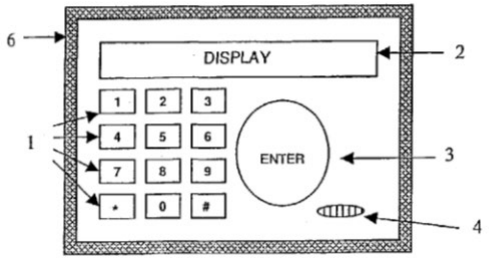
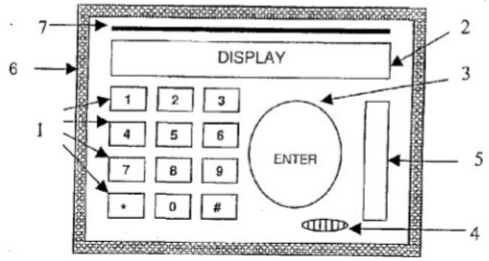
Claim Element	**Exemplary Citations to US20030075610A1 ("Ong '610")**
1[pre]. A mobile phone comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Ong '610 discloses or renders obvious "[a] mobile phone." For example: Ong '610 at [0027] 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.

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

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	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 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.

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

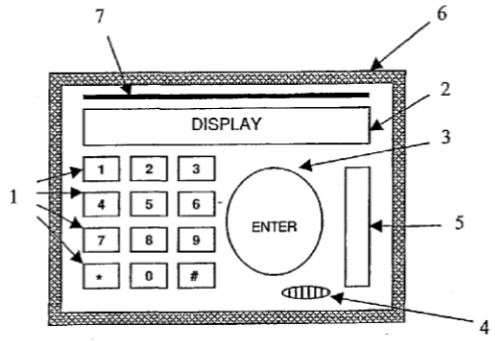
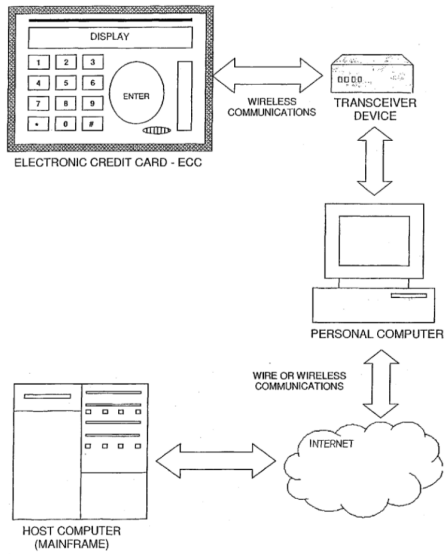
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	FIG. 10 shows a version of the electronic credit card with a keypad 1 forming part of the user verification means, a combination of infra red transmitter receiver 5, radio frequency antenna 7 and induction 6 forming part of the communication 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 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 processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents a single transaction account number.	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 a single transaction account number." For example: Ong '610 at Figure 5.

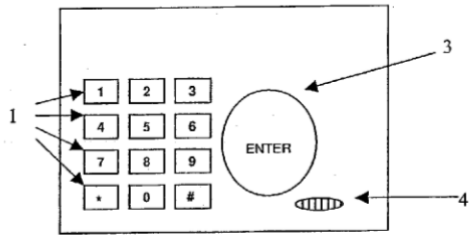
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong '610 at Figure 6 Figure 6: A drawing of ECC physical form covering SAC with PIN control 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 [0018] Preferably, in one embodiment, the unique authorisation code is generated in synchronisation with the transaction station.

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 [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 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 [0045]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	The transfer station must be configured to only continue with the electronic funds transfer transaction with the receipt of the unique authorisation code and account details 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 [0056] Use of the electronic credit card will prevent merchants from using an unauthorised transaction as each transaction can only be generated by a unique transaction provided by the electronic credit card. A merchant cannot generate a unique transaction identifier without an electronic credit card. The electronic credit card verifies the identity of the user before it is activated. The electronic credit card will be disabled if a predetermined number of attempts to gain access to its operation fail and this will prevent fraud in the event that an electronic credit card is stolen. An authorising distributor or other authorised body could re-initialise the electronic credit card through a controlled management system used to issue the electronic credit card. 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.
2. The mobile phone of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card." 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 8

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

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

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

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

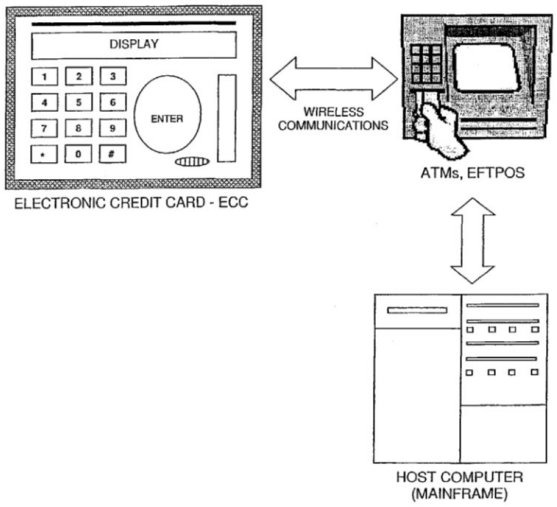
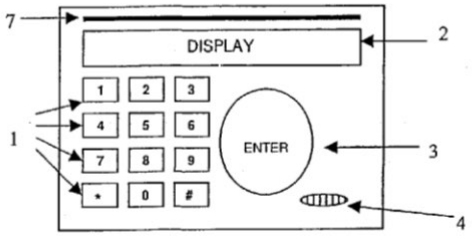
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong '610 at claim 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. *See also* claim 1 above.
3. The mobile phone of claim 1 wherein the single transaction account number represents financial data.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 1 wherein the single transaction account number represents financial data." For example: 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 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 [0045] The transfer station must be configured to only continue with the electronic funds transfer transaction with the receipt of the unique authorisation code and account details Ong '610 at [0056] Use of the electronic credit card will prevent merchants from using an unauthorised transaction as each transaction can only be generated by a unique transaction provided by the electronic credit card. A

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	merchant cannot generate a unique transaction identifier without an electronic credit card. The electronic credit card verifies the identity of the user before it is activated. The electronic credit card will be disabled if a predetermined number of attempts to gain access to its operation fail and this will prevent fraud in the event that an electronic credit card is stolen. An authorising distributor or other authorised body could re-initialise the electronic credit card through a controlled management system used to issue the electronic credit card. 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 phone of claim 3 wherein the financial data comprises credit card data.	Ong '610 discloses or renders obvious "[t]he mobile phone 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:

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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 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 11

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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 phone of claim 1 further comprising smartcard circuitry coupled to the processor.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 1 further comprising smartcard circuitry coupled to 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 a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. 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

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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 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. *See also* claim 1 above.
8, The mobile phone 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 phone of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions." For example: Ong '610 at Figure 3

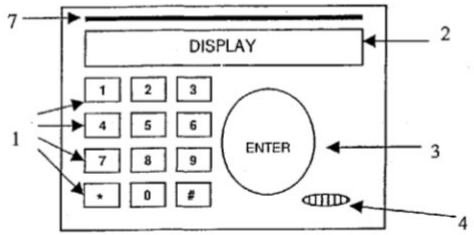
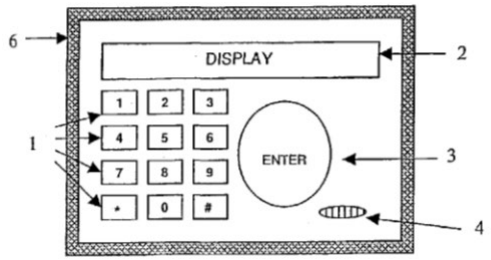
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Figure 3: A drawing of ECC communications link to Teller Machines, ATMs, EFTPOS and Host Computer. Drawing is not to scale.  Ong '610 at Figure 5. Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency 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]

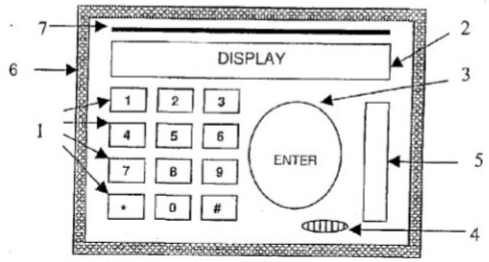
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong '610 at claim 1 a communication means for communicating 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. *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. *See also* claim 1 above.
9[pre]. A mobile phone 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 phone." For example: *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.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
[9b] smartcard circuitry for performing transactions using single transaction account numbers; and	Ong '610 discloses or renders obvious "smartcard circuitry for performing transactions using single transaction account numbers." 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 [0018] Preferably, in one embodiment, the unique authorisation code is generated in synchronisation with the transaction station. 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 [0041]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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 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 [0045] The transfer station must be configured to only continue with the electronic funds transfer transaction with the receipt of the unique authorisation code and account details 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 [0056] Use of the electronic credit card will prevent merchants from using an unauthorised transaction as each transaction can only be generated by a unique transaction provided by the electronic credit card. A merchant cannot generate a unique transaction identifier without an electronic credit card. The electronic credit card verifies the identity of the user before it is activated. The electronic credit card will be disabled

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	if a predetermined number of attempts to gain access to its operation fail and this will prevent fraud in the event that an electronic credit card is stolen. An authorising distributor or other authorised body could re-initialise the electronic credit card through a controlled management system used to issue the electronic credit card. 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 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 5 5. An electronic credit card in accordance with claim 1, wherein the unique authorisation code is generated in synchronisation with the transaction station. 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* [1b] and 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 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

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

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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. 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* [1b] and claim 5 above.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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 phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale 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 [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]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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 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 phone of claim 9 wherein the transactions are financial transactions.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the transactions are financial 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

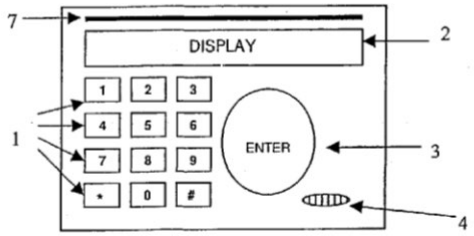
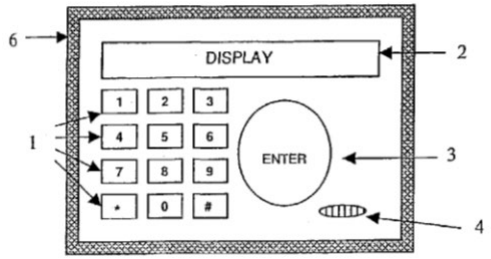
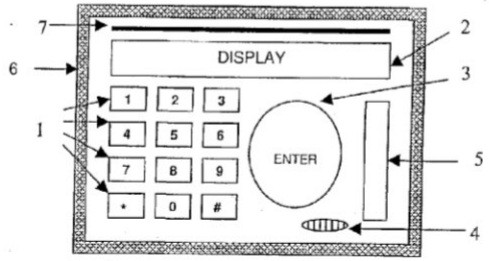
Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (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. 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. *See also* claim 3 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.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
12. The mobile phone 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 phone 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 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.
13. The mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence.	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.
14. The mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: Ong '610 at [0018] Preferably, in one embodiment, the unique authorisation code is generated in synchronisation with the transaction station. 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 [0045] The transfer station must be configured to only continue with the electronic funds transfer transaction with the receipt of the unique authorisation code and account details Ong '610 at [0056]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Use of the electronic credit card will prevent merchants from using an unauthorised transaction as each transaction can only be generated by a unique transaction provided by the electronic credit card. A merchant cannot generate a unique transaction identifier without an electronic credit card. The electronic credit card verifies the identity of the user before it is activated. The electronic credit card will be disabled if a predetermined number of attempts to gain access to its operation fail and this will prevent fraud in the event that an electronic credit card is stolen. An authorising distributor or other authorised body could re-initialise the electronic credit card through a controlled management system used to issue the electronic credit card. Ong '610 at claim 1 a means for generating a unique authorisation code when the user's identity is verified; Ong '610 at claim 5 5. An electronic credit card in accordance with claim 1, wherein the unique authorisation code is generated in synchronisation with the transaction station. 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.
15[pre]. A mobile phone 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 phone." For example: *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.
[15a] 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.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
[15b] circuitry to enable use of single transaction account numbers; and	Ong '610 discloses or renders obvious "circuitry to enable use of single transaction account numbers." For example: Ong '610 at [0018] Preferably, in one embodiment, the unique authorisation code is generated in synchronisation with the transaction station. 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 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 [0045] The transfer station must be configured to only continue with the electronic funds transfer transaction with the receipt of the unique authorisation code and account details Ong '610 at [0056]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	Use of the electronic credit card will prevent merchants from using an unauthorised transaction as each transaction can only be generated by a unique transaction provided by the electronic credit card. A merchant cannot generate a unique transaction identifier without an electronic credit card. The electronic credit card verifies the identity of the user before it is activated. The electronic credit card will be disabled if a predetermined number of attempts to gain access to its operation fail and this will prevent fraud in the event that an electronic credit card is stolen. An authorising distributor or other authorised body could re-initialise the electronic credit card through a controlled management system used to issue the electronic credit card. 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 claim 5 5. An electronic credit card in accordance with claim 1, wherein the unique authorisation code is generated in synchronisation with the transaction station. *See also* [1b] and [9b] and 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.
[15c] a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number.	Ong '610 discloses or renders obvious "a processor coupled to the circuitry to produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number." 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 [0018] Preferably, in one embodiment, the unique authorisation code is generated in synchronisation with the transaction station.

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 [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 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 [0045]

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	The transfer station must be configured to only continue with the electronic funds transfer transaction with the receipt of the unique authorisation code and account details 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 [0056] Use of the electronic credit card will prevent merchants from using an unauthorised transaction as each transaction can only be generated by a unique transaction provided by the electronic credit card. A merchant cannot generate a unique transaction identifier without an electronic credit card. The electronic credit card verifies the identity of the user before it is activated. The electronic credit card will be disabled if a predetermined number of attempts to gain access to its operation fail and this will prevent fraud in the event that an electronic credit card is stolen. An authorising distributor or other authorised body could re-initialise the electronic credit card through a controlled management system used to issue the electronic credit card. 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 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.

Claim Element	Exemplary Citations to US20030075610A1 ("Ong '610")
	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[b] and 9[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.
16. The mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry." 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.

Patent Owner's Ex. 2021
Page 325

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 [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 [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 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 [0045] The transfer station must be configured to only continue with the electronic funds transfer transaction with the receipt of the unique authorisation code and account details 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 [0056] Use of the electronic credit card will prevent merchants from using an unauthorised transaction as each transaction can only be generated by a unique transaction provided by the electronic credit card. A merchant cannot generate a unique transaction identifier without an electronic credit card. The electronic credit card verifies the identity of the user before it is activated. The electronic credit card will be disabled if a predetermined number of attempts to gain access to its operation fail and this will prevent fraud in the event that an electronic credit card is stolen. An authorising distributor or other authorised body could re-initialise the electronic credit card through a controlled management system used to issue the electronic credit card. 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 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 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 and 9[b] 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 15 above.
17. The mobile phone of claim 15 wherein the single transaction account numbers have a pre-defined sequence.	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 15 above.
18. The mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.	Ong '610 discloses or renders obvious "[t]he mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers." For example: *See* above at claim 14. 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 15 above.