

DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 11,270,174

EXHIBIT G

US4791283 (“Burkhardt ’283”), US7917444B1 (“Bursch ’444”), WO2003015043A1 (“Codron ’043”), US20040066273A1 (“Cortina ’273”), US6636833B1 (“Flitcroft ’833”), JP2004240847A (“Haginiwa ’847”), 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. 11,270,174 (“the ’174 patent”) are invalid (a) under 35 U.S.C. § 103 as obvious over each of Burkhardt ’283, Bursch ’444, Codron ’043, Cortina ’273, Flitcroft ’833, Haginiwa ’847, 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 Burkhardt ’283, Bursch ’444, Codron ’043, Cortina ’273, Flitcroft ’833, Haginiwa ’847, 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 G and Exhibits G1–G5, 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 ’174 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 ’174 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.

Claim Element	Exemplary Citations
	Flitcroft '833 at 9:40–63 and 18:25–37. Haginiwa '847 at [0002], [0012], [0020], [0022], [0023], [0041], [0044], [0047], [0050], [0051], and Figure 1. 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. 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.

Claim Element	Exemplary Citations
[1a] a memory to hold transaction data for use in a plurality of transactions;	Cortina '273 at Figure 5, Figure 9, Figure 13, Fig. 22, [0102], [0123], and [0140]. Flitcroft '833 at 9:64–10:19. Haginiwa '847 at Abstract, [0012], [0013]–[0014], [0014], [0026], [0028], [0029], [0030], [0036], [0038], [0047], [0073], [0074], and Figure 2. Hanada '365 at [0007], [0009], and [0019]. Horowitz '542 at Abstract, [0002], [0011], [0012], [0015], [0016], [0025], [0027], claim 1, claim 2, claim 3, claim 5, claim 6, claim 14, claim 15, claim 17, and claim 21. Jo '744 at 1. Kean '986 at [0011], [0027], and [0030]. Keen '200 at [0028]–[0029], [0049], and [0084]. Oishi '373 at [0029]. Sovio '882 at [0045] and [0084]. Yamagata '839 at [0002], [0002]–[0003], [0004], [0026], [0065], [0100], [0100]–[0101], and [0115]. Yu '038 at [0033].
[1b] a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;	Burkhardt '283 at Abstract, Figures 7+8, Figure 9, Figure 10, Figure 11, Figure 12, Figures 13, 1:51–65, 1:66–2:10, 2:21–27, 3:5–17, 3:19–29, 3:30–49, 3:64–66, 4:9–13, 4:17–35, 6:15–22, 6:23–31, 6:52–66, 6:67–7:13, 7:14–29, 8:37–54, 9:2–6, 10:5–9, 10:12–18, 10:25–28, and 10:57–60. Cortina '273 at Abstract, Fig. 1, Figure 16, Fig. 22, [0003], [0012], [0015], [0020], [0022], [0096], [0137], [0140], [0141], [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. Flitcroft '833 at 8:11–29 and 10:26–56. Haginiwa '847 at Abstract, [0040], [0044], [0047], [0051], [0074], and Figure 1. Horowitz '542 at [0011] and [0025]. Jo '744 at 1, 2, 3, 6, and 14. Kean '986 at [0006], [0007], [0011], [0012], [0026], [0030], [0034], claim 2, and claim 24.

Claim Element	Exemplary Citations
	Keen '200 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, [0002], [0003], [0012], [0013], [0026], [0028]–[0029], [0030], [0032], [0063], [0069], [0074], [0076], [0083], [0085], [0086], [0095], [0098], [0106], claim 1, claim 4, and claim 9. Mamba '073 at [0001]. SCAR PT-04002 at 4, 7–8, PayPass Figure (p. 8), 8, ExpressPay Figure (p. 9), 9, 10, Table 1, 22, 23, 24, 37, 38, 39, and 40. Sovio '882 at Abstract, Fig. 1, Fig. 2, [0010], [0017], [0020], [0041], [0043], [0045], [0048], [0049], [0073], [0080], and [0084]. Yamagata '839 at Fig. 1, Figure 15, [0042], [0064], [0107], [0108], [0109], [0110], [0115], [0117], and [0186]. Yoshinaga 2004 at 25 and 26–27. Yu '038 at Fig. 2, Fig. 3, Fig. 4, Fig. 12, Fig. 13, Figure 18, Fig. 19, [0034], [0036], [0039], [0046], [0054]–[0056], [0093], [0096], [0097], claim 2, and claim 20.
[1c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;	Bursch '444 at Fig. 1, Fig. 2, Fig.4A–B, 4:35–49, 6:26–52, and 7:30–49. Codron '043 at Abstract, 2:6–9, 2:19–3:10, 4:1–18, 5:4–23, 6:5–8, 6:19–20, 8:6–10, Fig. 1, and Fig. 2. Flitcroft '833 at Fig. 6, 9:40–63, 11:66–12:23, 16:15–34, 18:25–37, 18:38–44, and 19:35–37. Haginiwa '847 at [0020], [0022], [0024], claim 1, and Figure 1. Hanada '365 at Abstract, [0006], [0007], [0008], [0010], [0011], [0012], [0013], [0014], [0016], [0018], [0019], [0026], [0036], [0039], [0043], [0046], [0047], [0049], [0058], Fig. 1, Fig. 7, Fig. 8, Fig. 9, Fig. 10, and Fig. 11. Horowitz '542 at Figure 2, [0011], [0025], and [0029]. Jo '744 at Abstract, 3, 4, 5, 7, 15, and 16. Mamba '073 at Fig. 1A and Fig. 1B. SCAR PT-04002 at PayPass Figure (p. 8). Sovio '882 at [0035], [0040], [0043], [0044], [0073], and [0078].

Claim Element	Exemplary Citations
	Yoshinaga 2004 at Figure 3. Yu '038 at [0007] and [0039].
[1d] a driver to excite the current carrying conductor; and	Burkhardt '283 at Figures 13, 4:9–13, 4:17–35, and 8:13–36. Keen '200 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, [0002], [0013], [0030], [0058], [0069], [0074], [0076], [0083], [0085], [0086], [0095], [0098], [0106], claim 1, claim 4, and claim 9. Mamba '073 at Abstract, Fig. 2, Fig. 3, Fig. 4, [0008], [0009], [0010], [0011], [0011]–[0012], [0013], [0027], [0030], [0034], [0041], claim 2, claim 3, and claim 5. Sovio '882 at Fig. 2.
[1e] a processor coupled to control the driver.	Burkhardt '283 at Figures 13. Keen '200 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, [0013], [0015], [0028]–[0029], [0030], [0034], [0055], [0058], [0069], [0074], [0076], [0083], [0084], [0085], [0086], [0095], [0098], [0106], claim 1, claim 4, and claim 9. Mamba '073 at Abstract, Fig. 2, Fig. 3, Fig. 4, [0011]–[0012], [0026], [0027], [0030], [0034], [0041], claim 2, claim 3, and claim 5. Sovio '882 at Fig. 2 and [0045]. Yamagata '839 at [0163].
2. The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	Burkhardt '283 at Abstract, Figures 7+8, 3:5–17, 3:19–29, 3:30–49, 3:64–66, 4:9–13, 4:17–35, 6:15–22, 8:37–54, 9:2–6, 10:5–9, 10:12–18, 10:25–28, and 10:57–60. Cortina '273 at [0143]. Flitcroft '833 at 8:11–29 and 10:26–56. Haginiwa '847 at [0040], [0044], [0047], and [0051]. Jo '744 at 2. Kean '986 at Figure 1, [0012], [0021], and [0030].

Claim Element	Exemplary Citations
	SCAR PT-04002 at 4, 8, 9, 10, Table 1, 22, 23, and 24. Sovio '882 at [0010]. Yamagata '839 at [0107], [0109], and [0110]. Yoshinaga 2004 at 25 and 26–27. Yu '038 at Fig. 3, Fig. 4, [0034], [0046], and claim 2.
3. The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	Burkhardt '283 at 3:19–29, 3:30–49, 4:17–35, 6:15–22, and 10:12–18. Cortina '273 at Fig. 4, Fig. 22, [0007], [0016], [0096], [0097], [0178], [0199], [0202], claim 20, and claim 21. Haginiwa '847 at [0040] and [0061]. Jo '744 at 2 and 14. Kean '986 at [0026] and claim 17. Yamagata '839 at Figure 15 and [0186]. Yu '038 at Fig. 13, [0054]–[0056], [0057]–[0058], and claim 5.
4. The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Burkhardt '283 at Abstract, Figures 7+8, 3:5–17, 3:19–29, 3:30–49, 3:64–66, 4:9–13, 4:17–35, 6:15–22, 8:37–54, 9:2–6, 10:5–9, 10:12–18, 10:25–28, and 10:57–60. Cortina '273 at [0143]. Flitcroft '833 at 8:11–29 and 10:26–56. Haginiwa '847 at [0012], [0040], [0044], [0047], and [0051]. Horowitz '542 at Figure 2, Figure 3A, and [0021]. Jo '744 at 2. Kean '986 at Figure 1, [0012], and [0030]. SCAR PT-04002 at 4, 7–8, 8, ExpressPay Figure (p. 9), 9, 10, Table 1, 22, 23, and 24. Sovio '882 at [0010].

Claim Element	Exemplary Citations
	Yamagata '839 at [0110]. Yoshinaga 2004 at 25 and 26–27. Yu '038 at Fig. 3, Fig. 4, [0034], [0036], and [0046].
6. The mobile phone of claim 1 wherein the driver comprises a current driver.	Burkhardt '283 at Figures 13, 3:30–49, 4:17–35, and 8:13–36. Keen '200 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, [0013], [0030], [0058], [0069], [0074], [0076], [0083], [0085], [0086], [0095], [0098], [0106], claim 1, and claim 9. Mamba '073 at Abstract, Fig. 2, Fig. 3, Fig. 4, [0008], [0009], [0010], [0011], [0011]–[0012], [0013], [0026], [0027], [0030], [0034], and [0041]. Sovio '882 at Fig. 2.
7. The mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.	Bursch '444 at Fig. 2. Codron '043 at Abstract, 2:6–9, 2:19–3:10, 4:1–18, 5:4–23, 6:5–8, 6:19–20, 8:6–10, Fig. 1, and Fig. 2. Flitcroft '833 at 9:40–63 and 18:38–44. Haginiwa '847 at [0012], [0020], [0024], claim 1, and Figure 1. Hanada '365 at Abstract, [0007], [0010], [0012], [0014], [0016], [0018], [0019], [0026], [0036], [0039], Fig. 1, Fig. 7, Fig. 8, and Fig. 9. Horowitz '542 at Figure 2, [0011], and [0025]. Jo '744 at Abstract, 7, 15, and 16. Mamba '073 at Fig. 1A and Fig. 1B. Sovio '882 at [0035], [0040], [0043], and [0044]. Yoshinaga 2004 at Figure 3. Yu '038 at [0007], [0033], and [0039].
8. The mobile phone of claim 1 wherein downloaded transaction	Bursch '444 at Abstract, Fig. 1, Fig. 2, Fig.3A–B, Fig.4A–B, 1:6–9, 2:22–32, 2:65–3:9, 3:17–27, 4:1–34, 4:35–49, 5:9–27, 5:28–52, 5:53–60, 5:60–65, 6:26–52, 7:30–49, 7:50–54, and 8:37–42.

Claim Element	Exemplary Citations
data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.	Codron '043 at Abstract, 2:6–9, 2:19–3:10, 5:4–23, 8:6–10, and Fig. 1. Flitcroft '833 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, Fig. 7, Fig. 8, Fig. 9, 4:59–5:4, 5:5–19, 5:20–25, 5:26–48, 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, 13:17–32, 13:40–58, 13:59–66, 14:12–29, 16:15–34, 18:25–37, 18:46–55, and 19:35–37. Haginiwa '847 at [0064] and [0073]. Hanada '365 at Abstract, [0006], [0007], [0008], [0010], [0011], [0012], [0014], [0016], [0026], [0034], [0039], [0043], [0046], [0047], [0049], [0058], Fig. 1, Fig. 2, Fig. 5, Fig. 7, Fig. 8, Fig. 9, Fig. 10, and Fig. 11. Horowitz '542 at [0024], [0025], and [0029]. Jo '744 at 5. Sovio '882 at [0010] and [0084].
9. The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.	Bursch '444 at Abstract, Fig. 1, Fig. 2, Fig.3A–B, Fig.4A–B, 1:6–9, 2:22–32, 2:65–3:9, 3:17–27, 4:1–34, 4:35–49, 5:9–27, 5:28–52, 6:26–52, 7:30–49, 7:50–54, and 8:37–42. Flitcroft '833 at Abstract, Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, Fig. 7, Fig. 8, Fig. 9, 4:59–5:4, 5:20–25, 5:26–48, 6:53–64, 7:37–54, 7:55–8:10, 8:11–29, 8:35–39, 10:26–56, 10:67–11:14, 11:66–12:23, 14:12–29, 16:15–34, 18:25–37, 18:46–55, and 19:35–37. Haginiwa '847 at [0047], [0051], and [0074]. Hanada '365 at [0011], [0012], [0014], [0016], [0018], [0026], [0043], [0046], [0049], [0058], Fig. 1, Fig. 9, and Fig. 11. Horowitz '542 at Figure 3A, [0011], [0013], [0015], [0025], [0027], claim 1, and claim 2. Sovio '882 at [0010] and [0084].

DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 11,270,174

EXHIBIT G1: US20050086171A1 ("Abe '171")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 11,270,174 ("the '174 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 G and Exhibits G1–G5, 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 '174 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.

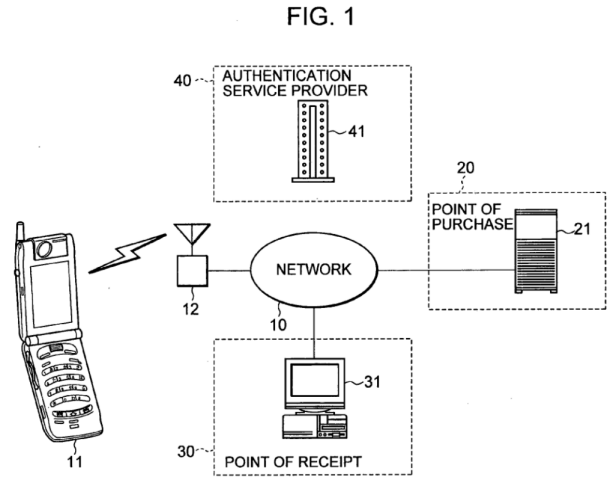
Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '174 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's 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.

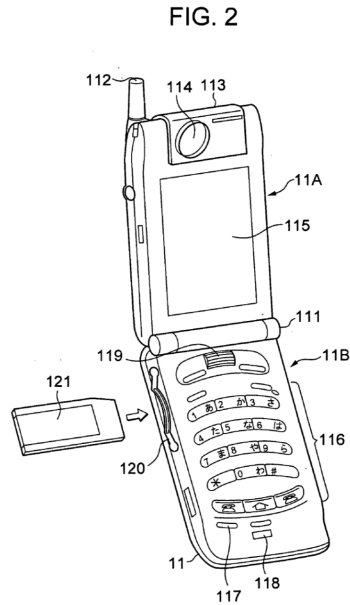
Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)

Abe ’171 at Figure 1



Abe ’171 at Figure 2

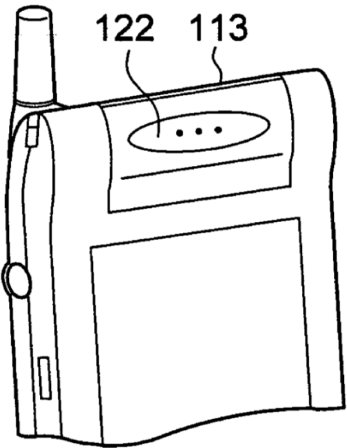


Abe ’171 at Fig. 3

Claim Element

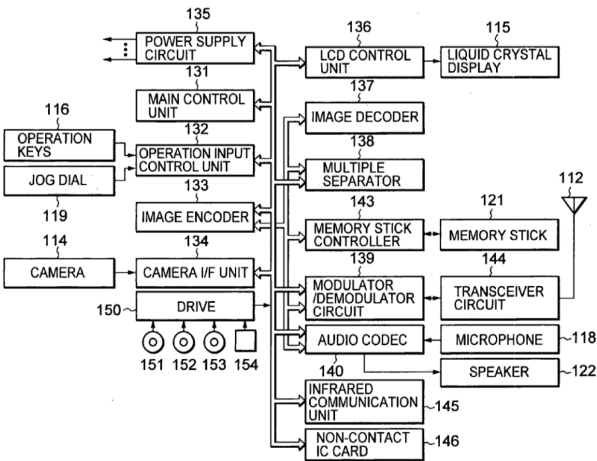
Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 3



Abe ’171 at Figure 4

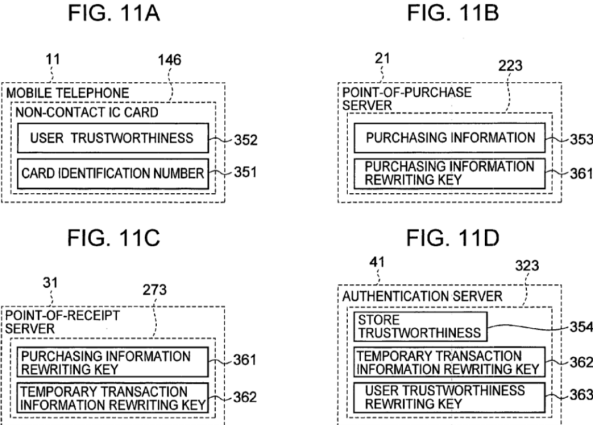
FIG. 4



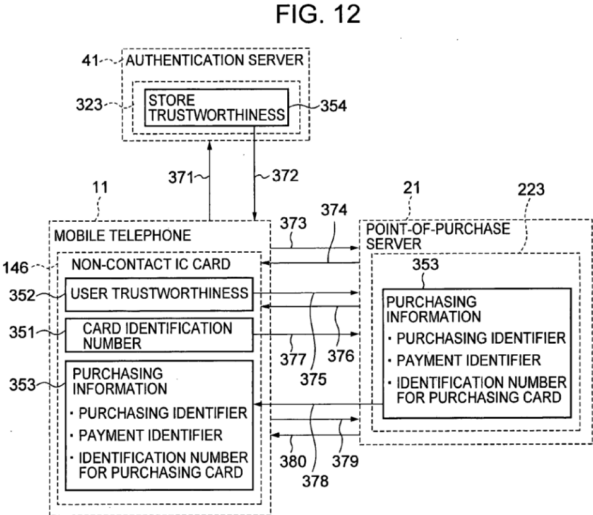
Abe ’171 at Fig.11A–D

Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)



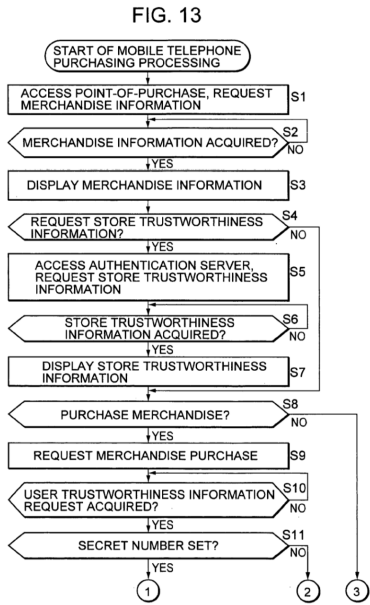
Abe ’171 at Fig. 12



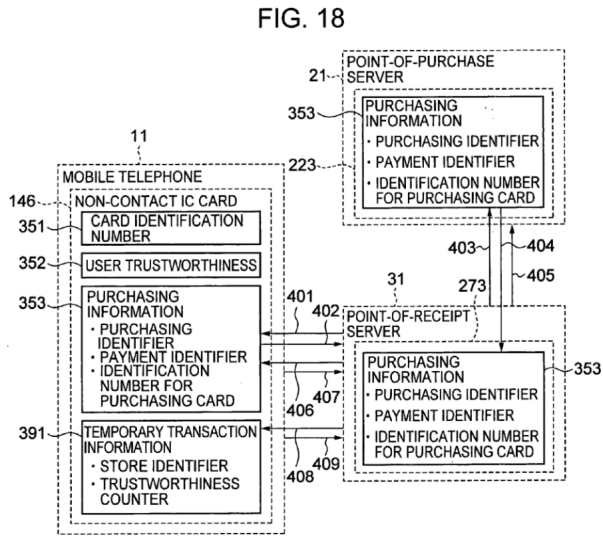
Abe ’171 at Fig. 13

Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)



Abe ’171 at Fig. 18

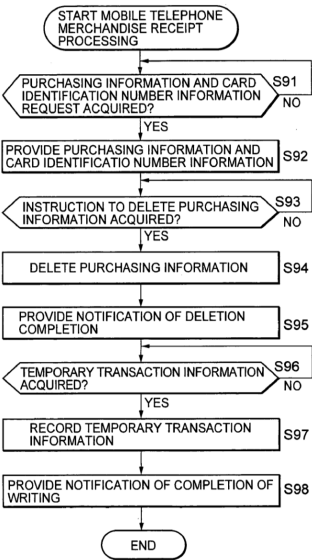


Abe ’171 at Fig. 19

Claim Element

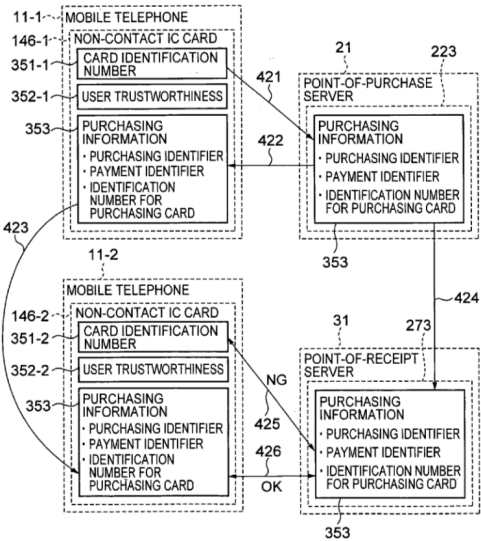
Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 19



Abe ’171 at Fig. 23

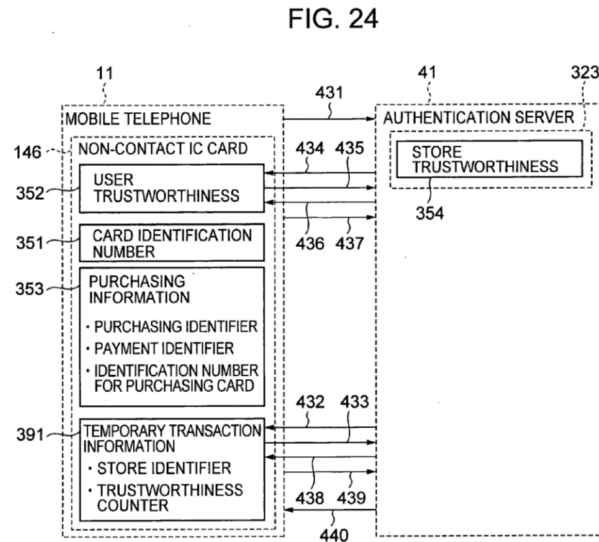
FIG. 23



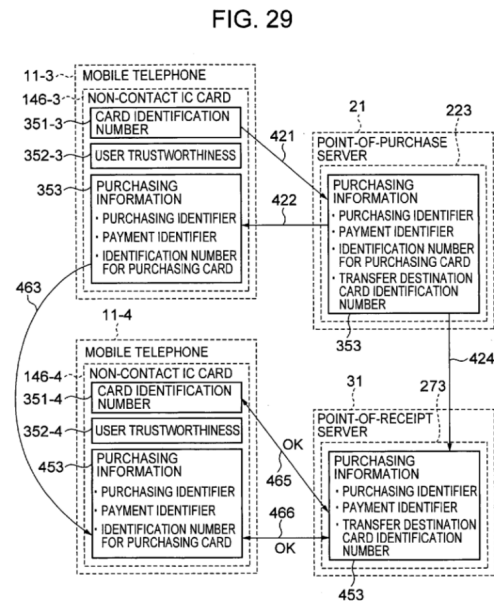
Claim Element

Exemplary Citations to US20050086171A1 ("Abe '171")

Abe '171 at Fig. 24



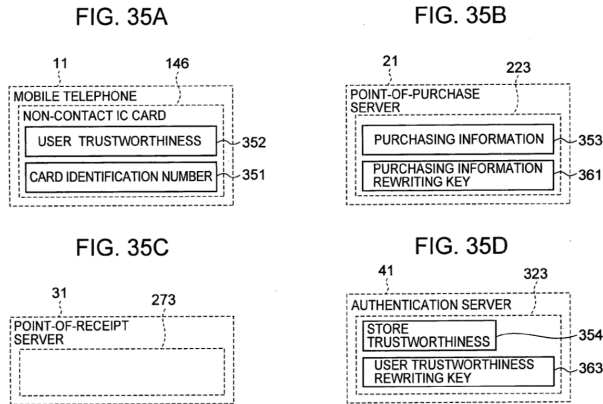
Abe '171 at Fig. 29



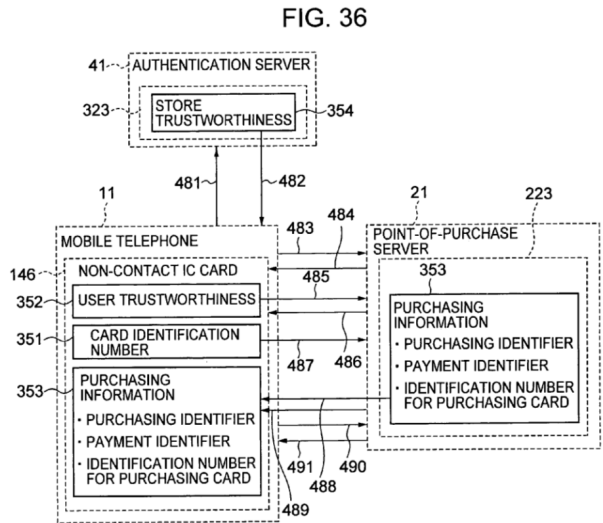
Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)

Abe ’171 at Fig. 35A–D



Abe ’171 at Fig. 36



Abe ’171 at Fig. 37

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	FIG. 37 <pre> graph TD Start([START OF MOBILE TELEPHONE PURCHASING PROCESSING]) --> S311[ACCESS POINT-OF-PURCHASE, REQUEST MERCHANDISE INFORMATION S311] S311 --> S312{MERCHANDISE INFORMATION ACQUIRED? S312} S312 -- NO --> S311 S312 -- YES --> S313[DISPLAY MERCHANDISE INFORMATION S313] S313 --> S314{REQUEST STORE TRUSTWORTHINESS INFORMATION? S314} S314 -- NO --> S313 S314 -- YES --> S315[ACCESS AUTHENTICATION SERVER, REQUEST STORE TRUSTWORTHINESS INFORMATION S315] S315 --> S316{STORE TRUSTWORTHINESS INFORMATION ACQUIRED? S316} S316 -- NO --> S315 S316 -- YES --> S317[DISPLAY STORE TRUSTWORTHINESS INFORMATION S317] S317 --> End((1)) </pre> 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.

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at [0037] FIG. 2 is a view showing an example configuration for the external appearance of the mobile telephone of FIG. 1. Abe ’171 at [0051] FIG. 13 is a flowchart illustrating purchasing processing by a mobile telephone. Abe ’171 at [0051]–[0052] FIG. 14 is a flowchart continuing on from the flowchart of FIG. 13 illustrating purchasing processing by a mobile telephone. Abe ’171 at [0057] FIG. 19 is a flowchart illustrating merchandise receipt processing carried out by a mobile telephone Abe ’171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, 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]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	As shown in FIG. 2, the mobile telephone 11 is constructed from a display unit 11A and main body 11B, capable of being folded up using a central hinge 111. Abe ’171 at [0101] The display unit 11A has an antenna 112 for transmitting and receiving signals that is capable of being pulled out or stored provided at an upper part of a left end. The mobile telephone 11 transmits and receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112. Abe ’171 at [0111] The memory stick 121 is a kind of flash memory card developed by the current applicant, Sony Corporation. This memory stick 121 is an item storing a type of EEPROM (Electrically Erasable and Programmable Read Only Memory) flash memory element constituted by non-volatile memory capable of being rewritten and erased electrically within a small, thin plastic case and is capable of reading and writing various types of data such as images, speech, and music etc. via ten pin terminals. Abe ’171 at [0113] 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-

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	contact IC card functions in the memory stick 121) are connected to a main control unit 131 for providing overall control of each part of the display unit 11A and body 11B via a main bus 141, and the image encoder 133, image decoder 137, multiple separator 138, a memory stick controller 143, the modulator/demodulator circuit 139, and the audio codec 140 are connected via a synchronous bus 142. Abe ’171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. Abe ’171 at [0178] The mobile telephone 11 shown in FIG. 11A holds information for a card identification number 351 and user trustworthiness 352 in the built-in non-contact IC card 146. Abe ’171 at [0202] 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]

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

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	When the non-contact IC card 146 is determined to be in communication range, the CPU 251 advances processing to step S112, controls the CPU 301 of the IC card reader/writer 275, and makes a request to the non-contact IC card 146 of the mobile telephone 11 in the vicinity for the purchasing information 353 and the card identification number information. This processing corresponds to the processing of arrow 401 of FIG. 18. Abe ’171 at [0307] For example, as shown in FIG. 23, when a user of a mobile telephone 11-1 purchases merchandise from the point-of-purchase 20, the point-of-purchase server 21 generates purchasing information 353 (arrow 421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422). Abe ’171 at [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]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	For example, as shown in FIG. 29, when a purchaser mobile telephone 11-3 constituting a mobile telephone used when purchasing merchandise transfers purchasing information 353 stored in a non-contact IC card 146-3 to a transfer destination mobile telephone 11-4, a transfer destination card identification number (i.e. card identification number 351-4) is overwritten (taken to be purchasing information 453) with a purchasing card identification number 353 (i.e. card identification number 351-3) contained in the purchasing information 353, and stored in a non-contact IC card 146-4 of the transfer destination mobile telephone 11-4 (arrow 463). Abe ’171 at [0364] First, in step S231, the main control unit 131 of the purchaser mobile telephone 11-3 makes a request to the point-of-purchase server 21 via the network 10 for permission to transfer the purchasing information 353. 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]

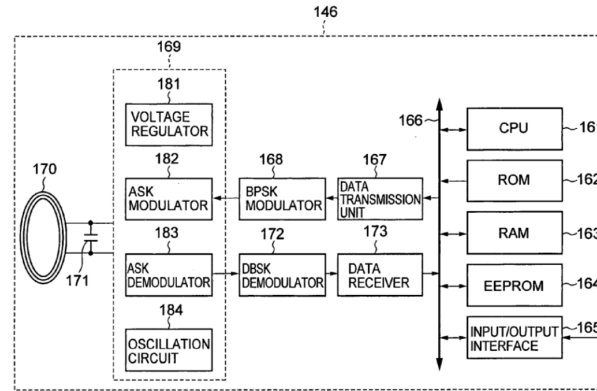
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	As described in the following, the transfer destination mobile telephone 11-4 provided with the purchasing information 453 and the purchasing information rewriting key 361 records the updated purchasing information 453 in the non-contact IC card 146-4 using the acquired purchasing information rewriting key 361. When recording is complete, the purchasing information rewriting key 361 is deleted, and completion of writing is provided to the purchaser mobile telephone 11-3. Abe ’171 at [0395] In step S238 of FIG. 30, the purchaser mobile telephone 11-3 provides the requested card identification number information of the transfer destination to the point-of-purchase server 21. Abe ’171 at [0412]–[0413] 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.

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at [0460] Namely, in step S381, the main control unit 131 of the mobile telephone 11 controls the non-contact IC card 146 so as to determine whether or not a request for card identification number information containing the purchasing information 353 and card identification number 351 has been acquired from the point-of-receipt server 31, and waits until it is determined that acquisition has taken place. Abe ’171 at [0481] In FIG. 47, as with the case in FIG. 24, the mobile telephone 11 accesses the authentication server 41 (arrow 511), but in a point of difference with the case of FIG. 24, the authentication server 41 does not request temporary commercial transaction information, but does request (arrow 512) and acquire (arrow 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] a memory to hold transaction data for use in a plurality of transactions;	Abe ’171 discloses or renders obvious “a memory to hold transaction data for use in a plurality of transactions.” For example: Abe ’171 at Figure 5

Claim Element

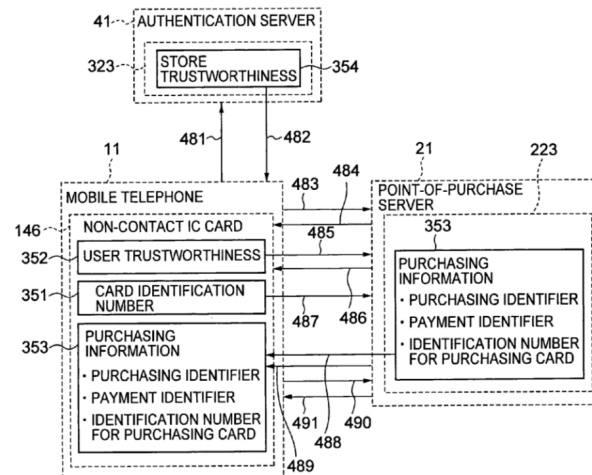
Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 5



Abe ’171 at Fig. 36

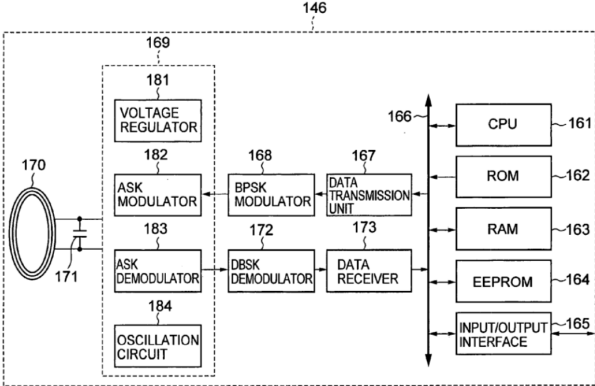
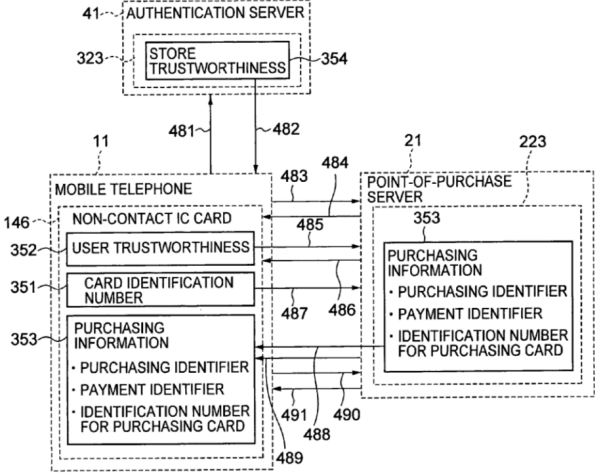
FIG. 36



Abe ’171 at [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

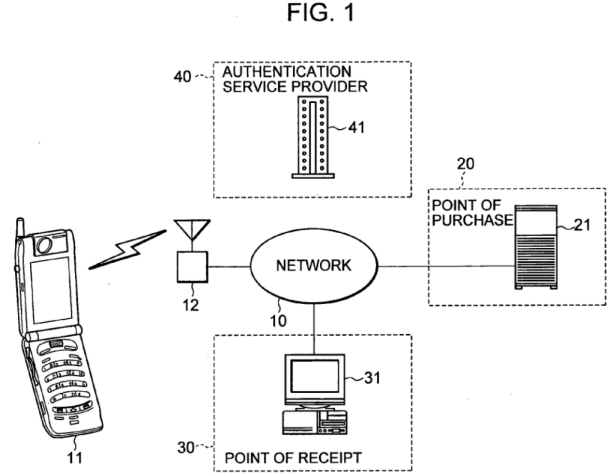
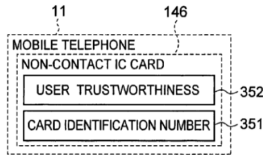
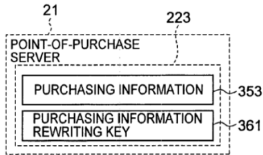
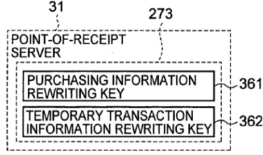
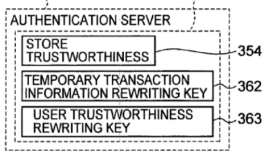
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	being rewritten and erased electrically within a small, thin plastic case and is capable of reading and writing various types of data such as images, speech, and music etc. via ten pin terminals. Abe ’171 at [0116] A power supply circuit 135, operation input control unit 132, image encoder 133, camera interface (I/F) unit 134, LCD control unit 136, multiple separator 138, modulator/demodulator circuit 139, audio codec 140, infrared communication unit 145 and non-contact IC card 146 (in this example, a dedicated non-contact IC card (Felica chip (registered trademark)) is provided but it is also possible to provide non-contact IC card functions in the memory stick 121) are connected to a main control unit 131 for providing overall control of each part of the display unit 11A and body 11B via a main bus 141, and the image encoder 133, image decoder 137, multiple separator 138, a memory stick controller 143, the modulator/demodulator circuit 139, and the audio codec 140 are connected via a synchronous bus 142. Abe ’171 at [0138] A CPU 161 expands a control program stored in ROM 162 into RAM 163, and controls all of the operations of the non-contact IC card 146. For example, when electromagnetic waves radiated from the IC card reader/writer provided at another information processing apparatus are received by an antenna 170, the CPU 161 notifies the IC card reader/writer of a card identification number set at the non-contact IC card 146 in response to this, and processing relating to receiving merchandise is carried out. Abe ’171 at [0147] Electronic money information is stored in the EEPROM 164. The user is then able to settle fees for purchased products and services etc. by utilizing this electronic money. The settlement history is also stored in an EEPROM 164. Abe ’171 at [0153] In the above, the non-contact IC card 146 is built-into the mobile telephone 1 but may also, for example, be installed into the mobile telephone 11 incorporated into the memory stick 121 so as to be controlled by the memory stick controller 143. To the extent this limitation is not disclosed by Abe ’171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe ’171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
[1b] a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;	Abe ’171 discloses or renders obvious “a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions.” For example: Abe ’171 at Figure 5 FIG. 5  Abe ’171 at Fig. 36 FIG. 36  Abe ’171 at [0009]

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

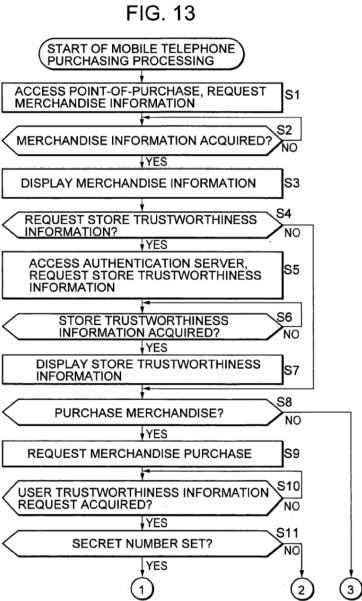
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	receives electromagnetic waves to and from the base station 12 constituting a fixed wireless terminal via the antenna 112. Abe ’171 at [0134] The non-contact IC card 146 may then be brought close to another information processing apparatus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

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

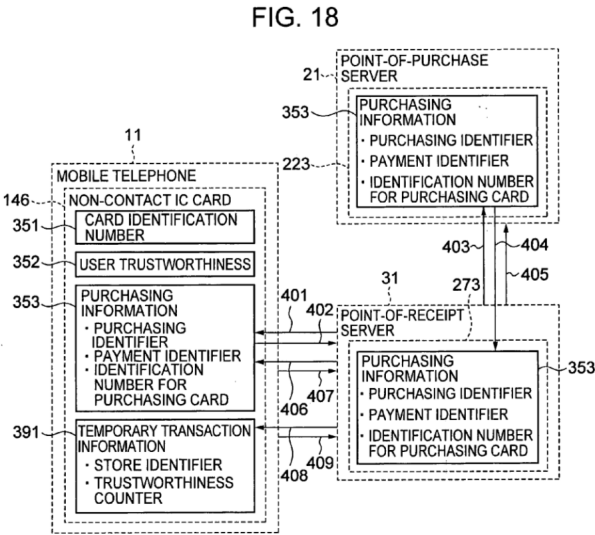
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
[1c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;	Abe ’171 discloses or renders obvious “a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network.” For example: Abe ’171 at Figure 1  FIG. 1 Abe ’171 at Fig.11A–D  FIG. 11A  FIG. 11B  FIG. 11C  FIG. 11D Abe ’171 at Fig. 13

Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)



Abe ’171 at Fig. 18

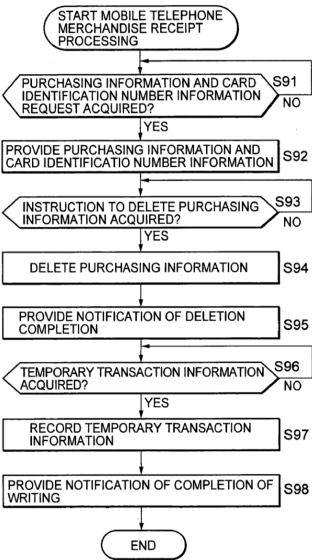


Abe ’171 at Fig. 19

Claim Element

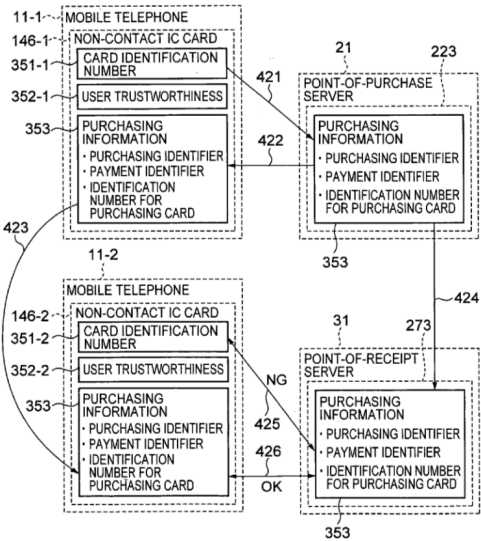
Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 19



Abe ’171 at Fig. 23

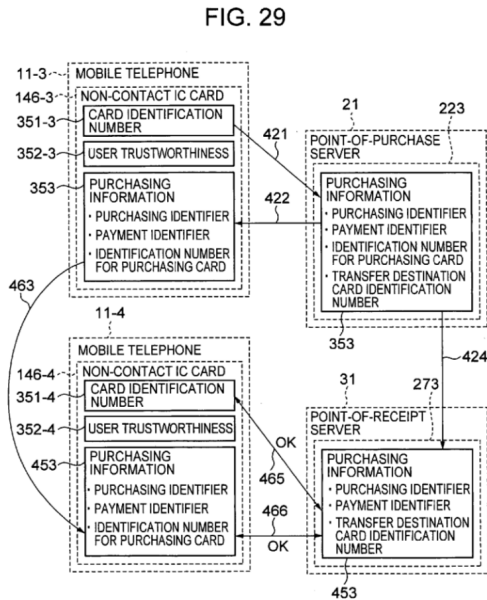
FIG. 23



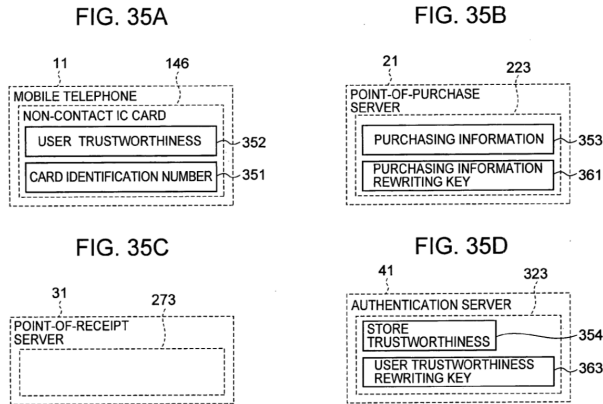
Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)

Abe ’171 at Fig. 29



Abe ’171 at Fig. 35A–D

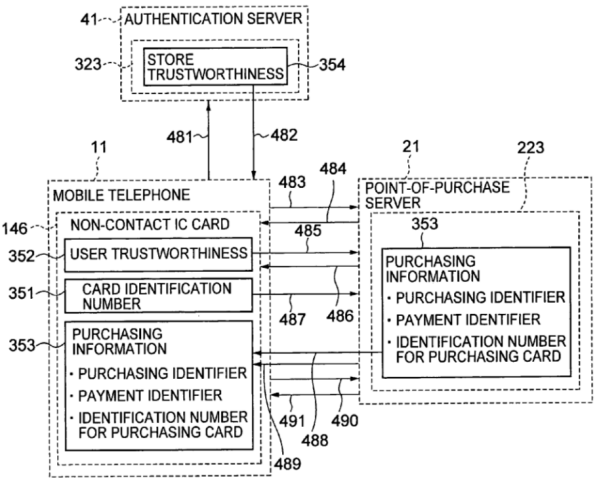


Abe ’171 at Fig. 36

Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 36



Abe ’171 at [0006]

An information processing system of the present invention is characterized by an information communication terminal connected to a network, for holding information relating to a commercial transaction and an information processing apparatus connected to the network, for managing information relating to the commercial transaction, wherein the information communication terminal comprises first acquiring means for acquiring information relating to the commercial transaction from the information processing apparatus during merchandise purchasing, first storage means for storing information relating to the commercial transaction acquired by the first acquiring means, and first providing means for providing information relating to the commercial transaction stored by the first storage means to the information processing apparatus during receipt of merchandise, wherein the information processing apparatus comprises second providing means for providing information relating to the commercial transaction to the information communication terminal during merchandise sales, second storage means for storing information relating to the commercial transaction, second acquiring means for acquiring information relating to the commercial transaction from the information communication terminal during merchandise delivery, and authentication means for authenticating information relating to said commercial transaction acquired by the second acquiring means using information relating to the commercial transaction stored by the second storage means.

Abe ’171 at [0007]

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

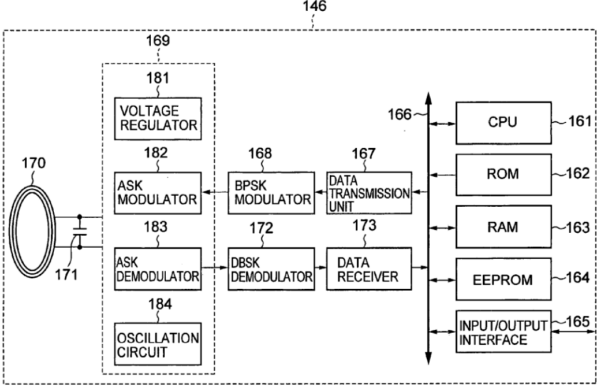
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	relating to the commercial transaction. At the information communication terminal, information relating to the commercial transaction is acquired from the information processing apparatus during merchandise purchasing. Acquired information 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 [0031] A second information processing system of the present invention is characterized by: an information communication terminal connected to a network, for holding information relating to a commercial transaction; a first information processing apparatus connected to said network, for managing information relating to said commercial transaction; and a second information processing apparatus connected to said network, for managing information relating to trustworthiness of a first user constituting a user of said information communication terminal and information relating to trustworthiness of a second user constituting a user of said first information processing apparatus. At the information communication terminal, information relating to trustworthiness of the first user is stored, stored information relating to the trustworthiness of the first user is provided to the first information storage device, information relating to trustworthiness of the second user is acquired from the second information processing apparatus, information relating to a commercial transaction is acquired from the first information processing apparatus, the stored trustworthiness of the first user and acquired information relating to the commercial transaction are provided to the second processing device, and information relating to trustworthiness of the first user updated by the second information processing apparatus is acquired. At the first information processing apparatus, information relating to trustworthiness of the first user is acquired from the information communication terminal and information relating to the commercial transaction is provided to the information communication terminal. At the second information processing apparatus, information relating to the trustworthiness of the second user is stored, stored information relating to the trustworthiness of the second user is provided to the information communication terminal, information relating to the trustworthiness of the first user from the information communication terminal and information relating to the commercial transaction is acquired, information relating to the trustworthiness of the first user and information relating to the trustworthiness of the second user is updated based on the acquired information relating to the commercial transaction, and information relating to the updated first user trustworthiness is provided to the information communication terminal.

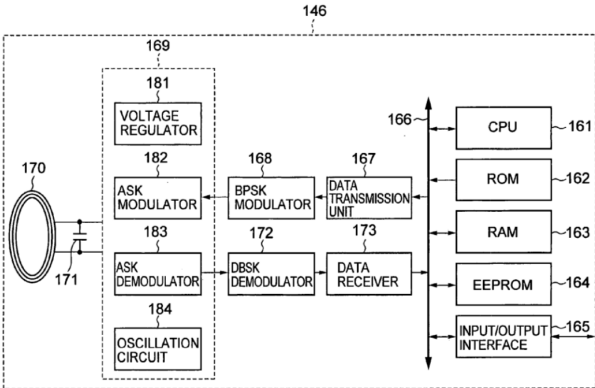
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at [0036] FIG. 1 is a view showing an example configuration for an electronic commercial transaction system to which the present invention is applied. Abe ’171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication 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 [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 [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

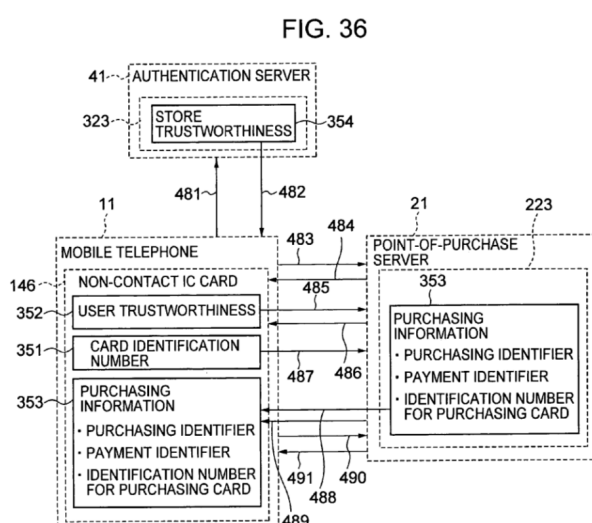
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	network 10, and requests purchasing information. The point-of-purchase server 21 that has acquired this request then provides the requested purchasing information to the mobile telephone 11 as described in the following. Abe ’171 at [0207] When it is determined to request the store trustworthiness information, the main control unit 131 advances the processing to step S5, carries out wireless communication with the closest base station 12 via the antenna 112, accesses the authentication server 41 via the network 10, and requests store trustworthiness information containing the store trustworthiness 354. This processing corresponds to the processing of arrow 371 of FIG. 12. As described in the following, the authentication server 41 generates trustworthiness information containing the store trustworthiness 354 recorded in the storage unit 323 based on this request, and provides this to the mobile telephone 11 via the network 10. Abe ’171 at [0221] In step S25, the main control unit 131 determines whether or not a request for this card identification number information has been acquired, and waits until it is determined that acquisition has taken place. When it is determined that a card identification number information request has been acquired, the main control unit 131 advances processing to step S26, the card identification number 351 is acquired from the non-contact IC card 146, and card identification number information containing this card identification number 351 is provided to the point-of-purchase server 21 via the network 10. This processing corresponds to the processing of arrow 377 of FIG. 12. Abe ’171 at [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 [0248] When purchasing/charging processing is complete, in step S74, the CPU 201 generates purchasing information relating to sale of merchandise on this occasion, and controls the communication unit 224 so that this generated purchasing information is provided to the mobile telephone 11 via the network 10 so as

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	to be stored in the non-contact IC card 146. This processing corresponds to the processing of arrow 378 of FIG. 12. Abe ’171 at [0257] In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance by the point-of-purchase 20. The user then positions the mobile telephone 11 in the vicinity of the IC card reader/writer 275 of the point-of-receipt server 31 installed at the point of receipt 30, and positions the non-contact IC card 146 built-into the mobile telephone 11 in the vicinity of the IC card reader/writer 275. Abe ’171 at [0266] The mobile telephone 11 then records the provided temporary commercial transaction information 391 in the non-contact IC card 146 using the acquired temporary commercial transaction information rewriting key 362. When recording is complete, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362, and provides the notification of completion of writing to the point-of-receipt server 31 (arrow 409) so as to complete processing relating to handing over of the merchandise. Abe ’171 at [0307] For example, as shown in FIG. 23, when a user of a mobile telephone 11-1 purchases merchandise from the point-of-purchase 20, the point-of-purchase server 21 generates purchasing information 353 (arrow 421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422). Abe ’171 at [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 [0376] As described in the following, the point-of-purchase server 21 that has acquired the card identification number information of the transfer destination updates the purchasing information 353 using the card identification number 351-4 contained in the acquired card identification number information, generates purchasing information 453 containing the card identification number 351-4, and provides this to the purchaser mobile telephone 11-3 together with the purchasing information rewriting key 361. Abe ’171 at [0481] In FIG. 47, as with the case in FIG. 24, the mobile telephone 11 accesses the authentication server 41 (arrow 511), but in a point of difference with the case of FIG. 24, the authentication server 41 does not request temporary commercial transaction information, but does request (arrow 512) and acquire (arrow 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 claim 25 an information communication terminal connected to a network, for holding information relating to a commercial transaction; Abe ’171 at claim 26 26. An information communication terminal, connected to a network, for communicating with a first information processing apparatus, characterized by: Abe ’171 at claim 27 27. An information communication terminal, connected to a network, for communicating with a first information processing apparatus, characterized by:

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at claim 30 30. An information communication terminal, connected to a network, for communicating with a first information processing apparatus, characterized by: To the extent this limitation is not disclosed by Abe ’171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe ’171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] a driver to excite the current carrying conductor; and	Abe ’171 discloses or renders obvious “a driver to excite the current carrying conductor.” For example: Abe ’171 at Figure 5 FIG. 5  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]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	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. 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.
[1e] a processor coupled to control the driver.	Abe ’171 discloses or renders obvious “a processor coupled to control the driver.” For example: Abe ’171 at Figure 5 FIG. 5  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.

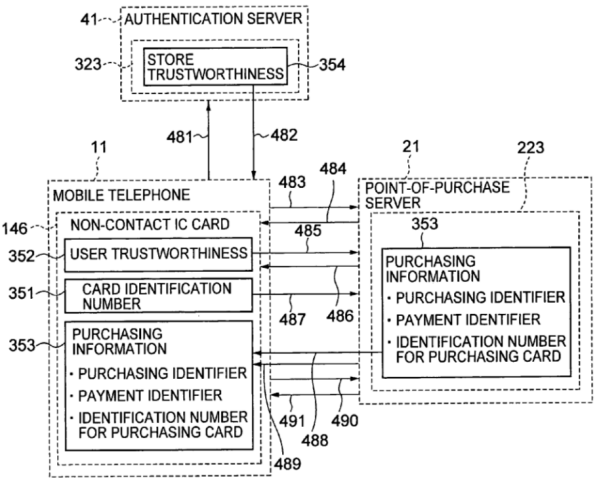
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	To the extent this limitation is not disclosed by Abe ’171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe ’171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	Abe ’171 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.” For example: Abe ’171 at Fig. 36  Abe ’171 at [0092] In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10.

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	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). 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. <i>See also</i> claim 1 above.
3. The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	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. <i>See also</i> claim 1 above.
4. The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Abe ’171 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.” For example: Abe ’171 at Fig. 36

Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 36

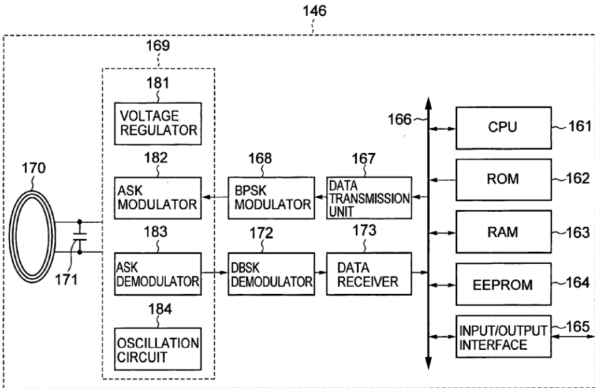


Abe ’171 at [0092]

In FIG. 1, a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10 to which the base station 12 is connected typified by, for example, the Internet, etc. Further, a point-of-purchase server 21 installed at a point-of-purchase 20 constituted by a store where a user of the mobile telephone 11 orders merchandise via the network 10, a point-of-receipt server 31 installed at a point of receipt 30 constituted by a store where the merchandise purchased by the user of the mobile telephone 11 is received, and an authentication server 41 providing basic services installed at an authentication service provider 40 for managing trustworthiness relating to commercial transactions between the user of the mobile telephone 11 and the store 20 using these basic services are connected to the network 10.

Abe ’171 at [0093]

The mobile telephone 11 is operated by the user so as to carry out wireless communication with the nearest base station 12, access the point-of-purchase server 21 via the network 10, and carry out merchandise purchasing processing. The mobile telephone 11 is operated by the user so as to access the authentication server 41 of the authentication service provider 40, trustworthiness of the point-of-purchase 20 is acquired, and this is provided to the user to enable a determination to be made as to whether or not to purchase the merchandise (product).

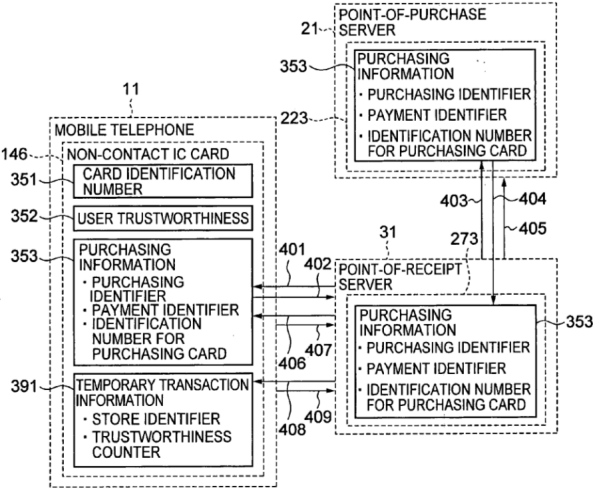
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	To the extent this limitation is not disclosed by Abe ’171, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Abe ’171, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
6. The mobile phone of claim 1 wherein the driver comprises a current driver.	Abe ’171 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the driver comprises a current driver.” For example: Abe ’171 at Figure 5 FIG. 5  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]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	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. <i>See also 1[d] above.</i> 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. <i>See also claim 1 above.</i>
7. The mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.	Abe ’171 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.” For example: Abe ’171 at Fig. 13 <pre> graph TD Start([START OF MOBILE TELEPHONE PURCHASING PROCESSING]) --> S1[ACCESS POINT-OF-PURCHASE, REQUEST MERCHANDISE INFORMATION S1] S1 --> S2{MERCHANDISE INFORMATION ACQUIRED? S2} S2 -- YES --> S3[DISPLAY MERCHANDISE INFORMATION S3] S2 -- NO --> C2((2)) S3 --> S4{REQUEST STORE TRUSTWORTHINESS INFORMATION? S4} S4 -- YES --> S5[ACCESS AUTHENTICATION SERVER, REQUEST STORE TRUSTWORTHINESS INFORMATION S5] S4 -- NO --> C2 S5 --> S6{STORE TRUSTWORTHINESS INFORMATION ACQUIRED? S6} S6 -- YES --> S7[DISPLAY STORE TRUSTWORTHINESS INFORMATION S7] S6 -- NO --> C2 S7 --> S8{PURCHASE MERCHANDISE? S8} S8 -- YES --> S9[REQUEST MERCHANDISE PURCHASE S9] S8 -- NO --> C2 S9 --> S10{USER TRUSTWORTHINESS INFORMATION REQUEST ACQUIRED? S10} S10 -- YES --> S11{SECRET NUMBER SET? S11} S10 -- NO --> C2 S11 -- YES --> C1((1)) S11 -- NO --> C3((3)) </pre> Abe ’171 at Fig. 18

Claim Element

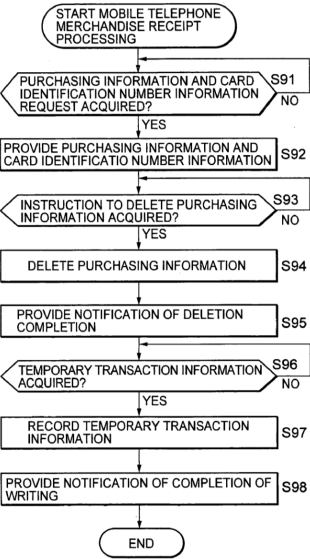
Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 18



Abe ’171 at Fig. 19

FIG. 19



Abe ’171 at [0030]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	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 [0031] A second information processing system of the present invention is characterized by: an information communication terminal connected to a network, for holding information relating to a commercial transaction; a first information processing apparatus connected to said network, for managing information relating to said commercial transaction; and a second information processing apparatus connected to said network, for managing information relating to trustworthiness of a first user constituting a user of said information communication terminal and information relating to trustworthiness of a second user constituting a user of said first information processing apparatus. At the information communication terminal, information relating to trustworthiness of the first user is stored, stored information relating to the trustworthiness of the first user is provided to the first information storage device, information relating to trustworthiness of the second user is acquired from the second information processing apparatus, information relating to a commercial transaction is acquired from the first information processing apparatus, the stored trustworthiness of the first user and acquired information relating to the commercial transaction are provided to the second processing device, and information relating to trustworthiness of the first user updated by the second information processing apparatus is acquired. At the first information processing apparatus, information relating to trustworthiness of the first user is acquired from the information communication terminal and information relating to the commercial transaction is provided to the information communication terminal. At the second information processing apparatus, information relating to the trustworthiness of the second user is stored, stored information relating to the trustworthiness of the second user is provided to the information communication terminal, information relating to the trustworthiness of the first user from the information communication terminal and information relating to the commercial transaction is acquired, information relating to the trustworthiness

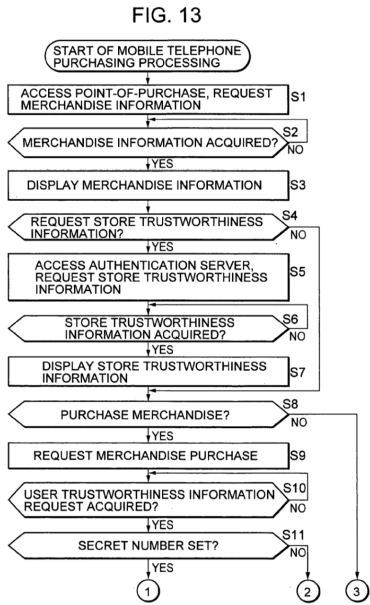
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	of the first user and information relating to the trustworthiness of the second user is updated based on the acquired information relating to the commercial transaction, and information relating to the updated first user trustworthiness is provided to the information communication terminal. Abe ’171 at [0036] FIG. 1 is a view showing an example configuration for an electronic commercial transaction system to which the present invention is applied. Abe ’171 at [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 [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 [0207]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	When it is determined to request the store trustworthiness information, the main control unit 131 advances the processing to step S5, carries out wireless communication with the closest base station 12 via the antenna 112, accesses the authentication server 41 via the network 10, and requests store trustworthiness information containing the store trustworthiness 354. This processing corresponds to the processing of arrow 371 of FIG. 12. As described in the following, the authentication server 41 generates trustworthiness information containing the store trustworthiness 354 recorded in the storage unit 323 based on this request, and provides this to the mobile telephone 11 via the network 10. 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 [0248] When purchasing/charging processing is complete, in step S74, the CPU 201 generates purchasing information relating to sale of merchandise on this occasion, and controls the communication unit 224 so that this generated purchasing information is provided to the mobile telephone 11 via the network 10 so as to be stored in the non-contact IC card 146. This processing corresponds to the processing of arrow 378 of FIG. 12. Abe ’171 at [0257] In order to receive the purchased merchandise, the user of the mobile telephone 11 that has purchased the merchandise as described above goes to either the nearest point of receipt 30 or to a point of receipt 30 designated in advance by the point-of-purchase 20. The user then positions the mobile telephone 11 in the vicinity of the IC card reader/writer 275 of the point-of-receipt server 31 installed at the point of receipt 30, and positions the non-contact IC card 146 built-into the mobile telephone 11 in the vicinity of the IC card reader/writer 275. Abe ’171 at [0266] The mobile telephone 11 then records the provided temporary commercial transaction information 391 in the non-contact IC card 146 using the acquired temporary commercial transaction information rewriting key 362. When recording is complete, the mobile telephone 11 deletes the temporary commercial

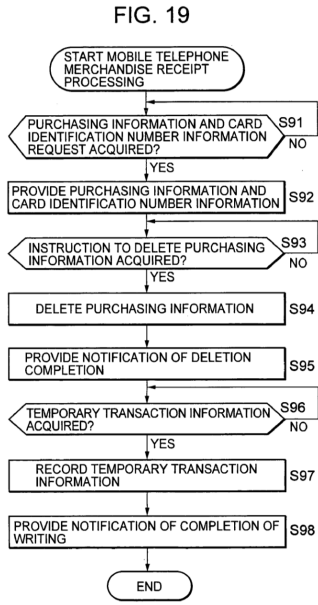
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	transaction information rewriting key 362, and provides the notification of completion of writing to the point-of-receipt server 31 (arrow 409) so as to complete processing relating to handing over of the merchandise. Abe ’171 at [0360] 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). 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. <i>See also</i> claim 1 above.
8. The mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.	Abe ’171 discloses or renders obvious “[t]he mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.” For example: Abe ’171 at Fig. 13

Claim Element

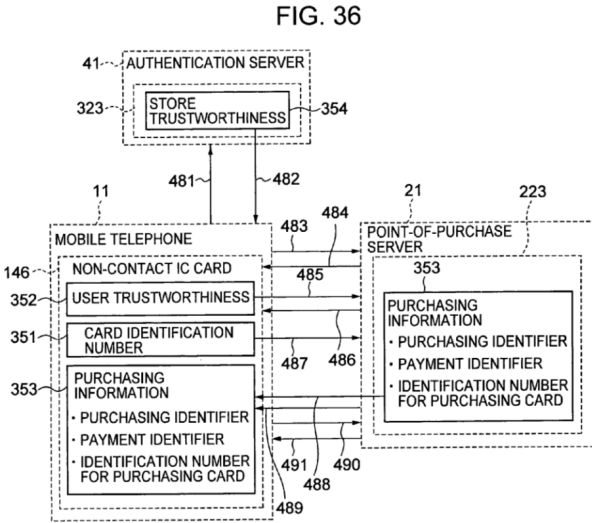
Exemplary Citations to US20050086171A1 (“Abe ’171”)



Abe ’171 at Fig. 19



Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at Fig. 23 FIG. 23 Abe ’171 at Fig. 24 FIG. 24

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at Fig. 36  Abe ’171 at [0057] FIG. 19 is a flowchart illustrating merchandise receipt processing carried out by a mobile telephone Abe ’171 at [0207] When it is determined to request the store trustworthiness information, the main control unit 131 advances the processing to step S5, carries out wireless communication with the closest base station 12 via the antenna 112, accesses the authentication server 41 via the network 10, and requests store trustworthiness information containing the store trustworthiness 354. This processing corresponds to the processing of arrow 371 of FIG. 12. As described in the following, the authentication server 41 generates trustworthiness information containing the store trustworthiness 354 recorded in the storage unit 323 based on this request, and provides this to the mobile telephone 11 via the network 10. 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

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

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422). Abe ’171 at [0313] 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 [0315] The mobile telephone 11 then deletes the temporary commercial transaction information 391 using the acquired temporary commercial transaction information rewriting key 362 and notifies the authentication server 41 when this is complete (arrow 439). The authentication server 41 notified of deletion of the temporary commercial transaction information 391 then provides notification of processing completion to the mobile telephone 11 (arrow 440) and ends processing relating to updating of the trustworthiness information. 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 [0331] When it is determined that a temporary commercial transaction information deletion instruction has been acquired (the temporary commercial transaction information rewriting key 362 has been acquired), the main control unit 131 advances the processing to step S183, and the temporary commercial transaction information 391 stored in the non-contact IC card 146 is deleted using the acquired temporary commercial transaction information rewriting key 362. Abe ’171 at [0332] The main control unit 131 that has deleted the temporary commercial transaction information 391 stored in the non-contact IC card 146 then advances processing to step S184, deletes the temporary commercial transaction information rewriting key 362, and provides deletion completion notification to the authentication server 41. This processing corresponds to the arrow 439 of FIG. 24.

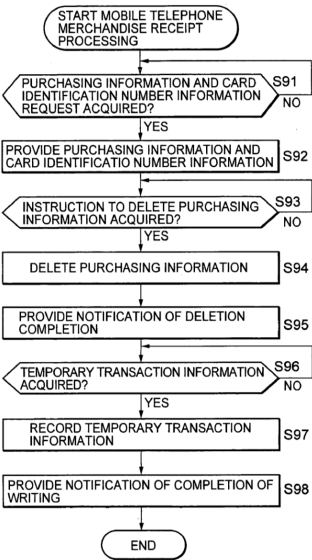
Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at [0347] The main control unit 131 of the mobile telephone 11 that has acquired the user trustworthiness information then updates the user trustworthiness 352 stored in the non-contact IC card 146 and provides this to the authentication 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 [0376] As described in the following, the point-of-purchase server 21 that has acquired the card identification number information of the transfer destination updates the purchasing information 353 using the card identification number 351-4 contained in the acquired card identification number information, generates purchasing information 453 containing the card identification number 351-4, and provides this to the purchaser mobile telephone 11-3 together with the purchasing information rewriting key 361. Abe ’171 at [0420] In the above, a description is given where the point-of-receipt server 31 of the point of receipt 30 holds the purchasing information rewriting key 361, with the purchasing information 353 stored in the non-contact IC card 146 being deleted after delivery of the merchandise. However, the present invention is by no means limited in this respect, and this electronic commercial transaction system may be simplified by not having the point-of-receipt server 31 delete the purchasing information.

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	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 claim 32 deleting means for deleting information relating to said first information processing apparatus stored by said storage means using said key information acquired by said fourth acquiring means. 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. <i>See also</i> claim 1 above.
9. The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.	Abe ’171 discloses or renders obvious “[t]he mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.” For example: Abe ’171 at Fig. 19

Claim Element

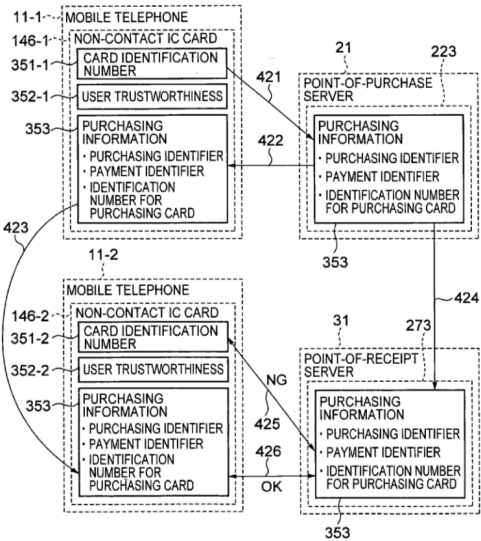
Exemplary Citations to US20050086171A1 (“Abe ’171”)

FIG. 19



Abe ’171 at Fig. 23

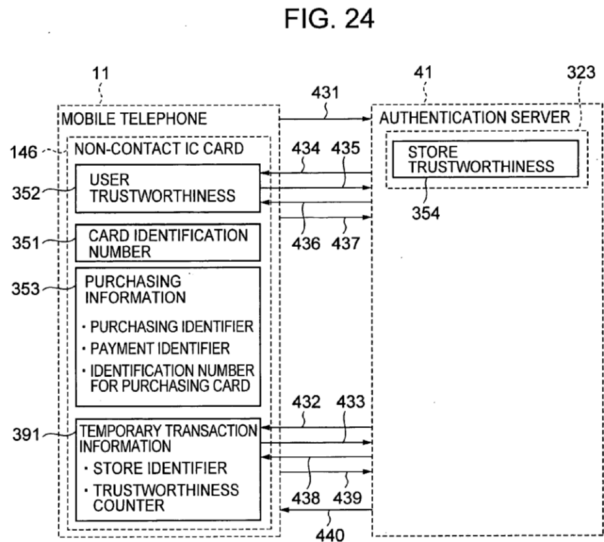
FIG. 23



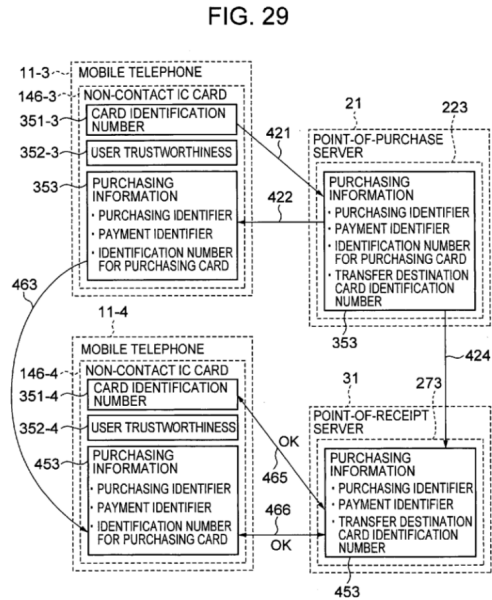
Claim Element

Exemplary Citations to US20050086171A1 (“Abe ’171”)

Abe ’171 at Fig. 24



Abe ’171 at Fig. 29



Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	Abe ’171 at [0057] FIG. 19 is a flowchart illustrating merchandise receipt processing carried out by a mobile telephone 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 [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 [0307] For example, as shown in FIG. 23, when a user of a mobile telephone 11-1 purchases merchandise from the point-of-purchase 20, the point-of-purchase server 21 generates purchasing information 353 (arrow 421) using a card identification number 351-1 allotted to the non-contact IC card 146-1 of the mobile telephone 11-1 and provides this to the non-contact IC card 146 (arrow 422). Abe ’171 at [0315] The mobile telephone 11 then deletes the temporary commercial transaction information 391 using the acquired temporary commercial transaction information rewriting key 362 and notifies the authentication server 41 when this is complete (arrow 439). The authentication server 41 notified of deletion of the temporary commercial transaction information 391 then provides notification of processing completion to the mobile telephone 11 (arrow 440) and ends processing relating to updating of the trustworthiness information. Abe ’171 at [0319]

Claim Element	Exemplary Citations to US20050086171A1 (“Abe ’171”)
	The authentication server 41 that has accessed the mobile telephone 11 then, as described in the following, requests temporary commercial transaction information 391 stored in the non-contact IC card 146 of the mobile telephone 11. Abe ’171 at [0347] The main control unit 131 of the mobile telephone 11 that has acquired the user trustworthiness information then updates the user trustworthiness 352 stored in the non-contact IC card 146 and provides this to the authentication server 41 using the processing of step S181 of FIG. 26. Abe ’171 at [0360] For example, as shown in FIG. 29, when a purchaser mobile telephone 11-3 constituting a mobile telephone used when purchasing merchandise transfers purchasing information 353 stored in a non-contact IC card 146-3 to a transfer destination mobile telephone 11-4, a transfer destination card identification number (i.e. card identification number 351-4) is overwritten (taken to be purchasing information 453) with a purchasing card identification number 353 (i.e. card identification number 351-3) contained in the purchasing information 353, and stored in a non-contact IC card 146-4 of the transfer destination mobile telephone 11-4 (arrow 463). Abe ’171 at [0376] As described in the following, the point-of-purchase server 21 that has acquired the card identification number information of the transfer destination updates the purchasing information 353 using the card identification number 351-4 contained in the acquired card identification number information, generates purchasing information 453 containing the card identification number 351-4, and provides this to the purchaser mobile telephone 11-3 together with the purchasing information rewriting key 361. Abe ’171 at [0420] In the above, a description is given where the point-of-receipt server 31 of the point of receipt 30 holds the purchasing information rewriting key 361, with the purchasing information 353 stored in the non-contact IC card 146 being deleted after delivery of the merchandise. However, the present invention is by no means limited in this respect, and this electronic commercial transaction system may be simplified by not having the point-of-receipt server 31 delete the purchasing information. Abe ’171 at claim 35 a generating step for generating information relating to said commercial transaction during product sales;

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. <i>See also</i> claim 1 above.

DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 11,270,174

EXHIBIT G2: US20040133787A1 ("Doughty '787")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 11,270,174 ("the '174 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 G and Exhibits G1–G5, 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 '174 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 '174 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] a memory to hold transaction data for use in a plurality of transactions;	Doughty ’787 discloses or renders obvious “a memory to hold transaction data for use in a plurality of transactions.” For example: Doughty ’787 at Abstract The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty ’787 at Fig. 3

Claim Element

Exemplary Citations to US20040133787A1 (“Doughty ’787”)

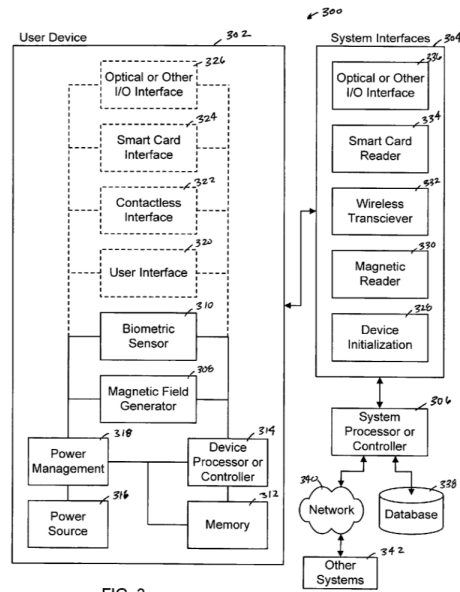


FIG. 3

Doughty ’787 at Figure 11

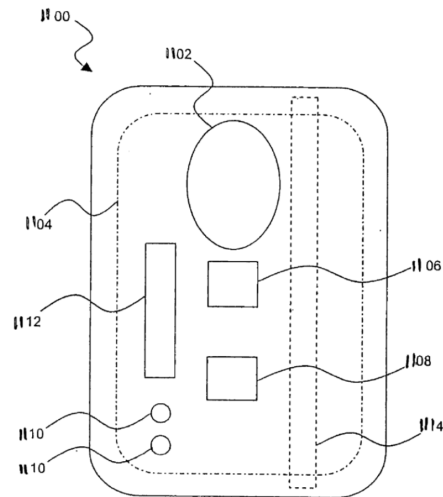


Fig. 11

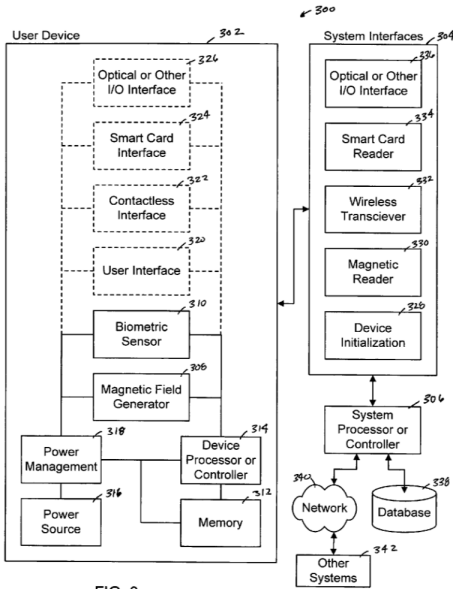
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at [0008]–[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner. Doughty ’787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty ’787 at [0039]

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

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified. Doughty ’787 at [0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication. Doughty ’787 at [0046] 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.

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at [0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card. Doughty ’787 at [0065] The ASIC 1106 is a custom integrated circuit chip developed for use in the device 1100. The ASIC 1106 includes Random Access Memory (“RAM”) which may be used for temporarily storing a current fingerprint analog detected by the fingerprint sensor 1102 and for temporarily storing intermediate results of processing calculations (e.g., fingerprint comparisons, etc.). The ASIC 1106 may also include non-volatile memory (e.g., Flash memory or EEPROM) to store and retrieve one or more fingerprint template analogs that are used for comparison against the current fingerprint analog. 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 claim 1 a memory disposed within the substrate; Doughty ’787 at claim 1 a processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified; and Doughty ’787 at claim 26 26. The apparatus as recited in claim 1, wherein the processor and the memory are integrated into a single integrated circuit. Doughty ’787 at claim 60 60. A system comprising: one or more user devices, each user device comprising a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate, a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified, and a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor; one or more system interfaces operable to communicate with the user device; and a system processor communicably coupled to the one or more system interfaces. Doughty ’787 at claim 88 88. The system as recited in claim 60, wherein the device processor and the memory are integrated into a single integrated circuit.

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 current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;	Doughty ’787 discloses or renders obvious “a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions.” For example: Doughty ’787 at Fig. 3  FIG. 3 Doughty ’787 at Fig. 5B

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	FIG. 5B Doughty ’787 at Figure 9 Fig. 9 Doughty ’787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe. Doughty ’787 at [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 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]

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

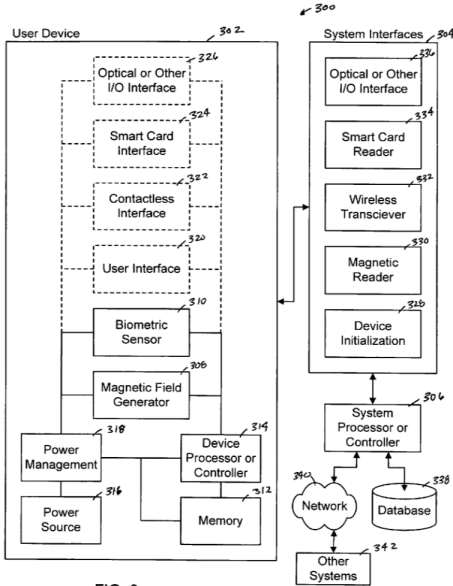
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 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 [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

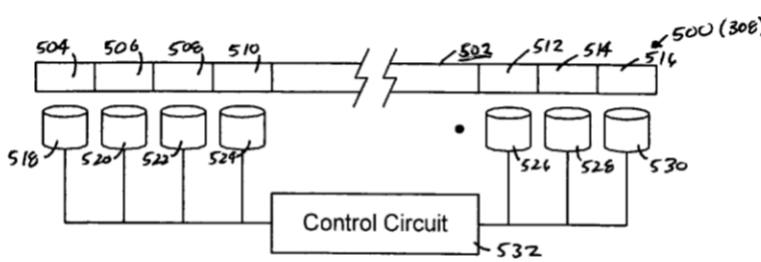
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 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 material that can be read by standard magnetic card readers when such binary code is applied in accordance with ISO standards. 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

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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 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

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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. 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 [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 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.
[1c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;	Doughty ’787 discloses or renders obvious “a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network.” For example: Doughty ’787 at Fig. 3  FIG. 3 Doughty ’787 at [0047] The one or more system interfaces 304 may include a device initialization interface 328, a magnetic reader 330, a wireless communications interface (transceiver) 332, a smart card reader 334, or an optical or other input/output interface 336. The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly, depending on the desired application and implementation. Other non-system interfaces may include a battery recharger, personal computer interface or personal data assistant (PDA). The one or more system interfaces 304 are communicably coupled to a system processor or controller 306, which in turn may be communicably coupled to a database 338 or one or more remote

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	systems or computers 342 via network 340. Network 340 may be a local area network or wide area network, such as the Internet. Doughty ’787 at [0062] It is understood that many different reader/writer configurations may be used. For example, the reader/writer device 902 may be in communication with other devices or with a network. Furthermore, the reader/writer device 902 may be in communication with other devices or with a network. Furthermore, the reader/writer device 902 may include the RF power source, or they may be separate devices. For the purposes of clarity, the reader/writer device 902 of the present invention example includes the RF power source, although alternate sources of RF power may be used. Doughty ’787 at claim 63 63. The system as recited in claim 60, further comprising one or more remote computers communicably coupled to the system processor via a network. To the extent this limitation is not disclosed by Doughty ’787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty ’787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] a driver to excite the current carrying conductor; and	Doughty ’787 discloses or renders obvious “a driver to excite the current carrying conductor.” For example: 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 [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

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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. 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.
[1e] a processor coupled to control the driver.	Doughty ’787 discloses or renders obvious “a processor coupled to control the driver.” 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”)

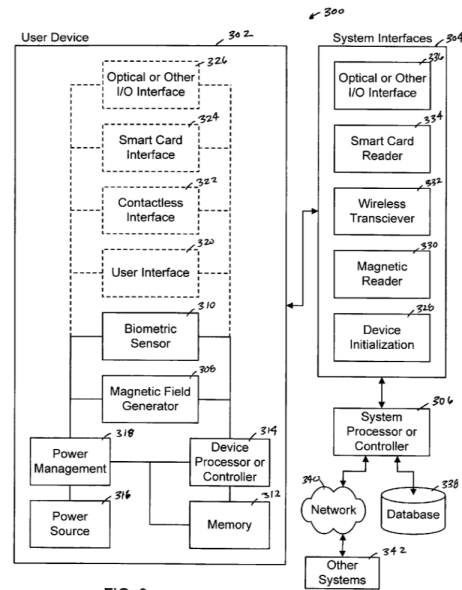


FIG. 3

Doughty ’787 at Fig. 5A

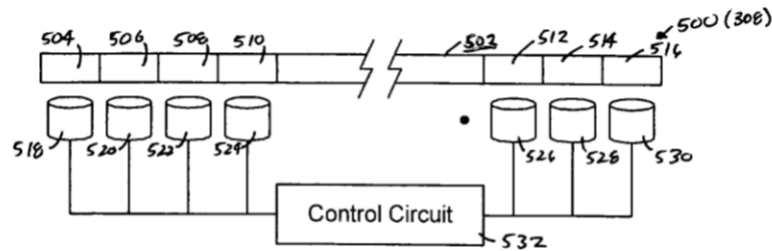


FIG. 5A

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 [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

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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 [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. 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 represents a point-of-sale transaction.	Doughty ’787 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.” For example: Doughty ’787 at [0008] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty ’787 at [0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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 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

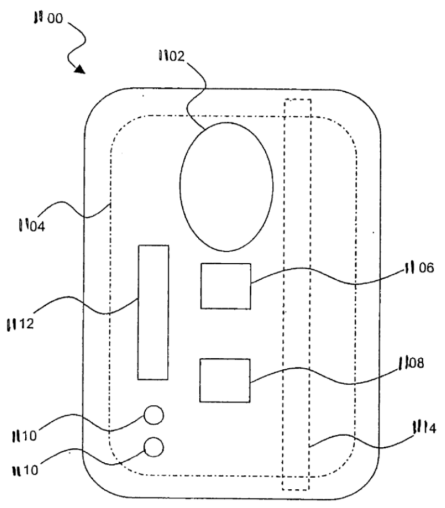
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not 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 [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. 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,

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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 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.

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at claim 53 53. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty ’787 at claim 57 57. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader. Doughty ’787 at claim 64 64. The system as recited in claim 60, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. To the extent this limitation is not disclosed by Doughty ’787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty ’787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
3. The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	Doughty ’787 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.” For example: Doughty ’787 at [0021]–[0022] FIG. 7 is a flow chart of an exemplary authentication method for using a device in accordance with the present invention Doughty ’787 at [0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at [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 [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

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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 [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 claim 22 22. The apparatus as recited in claim 1, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card. Doughty ’787 at claim 51 51. The computer program as recited in claim 46, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. To the extent this limitation is not disclosed by Doughty ’787, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Doughty ’787, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.

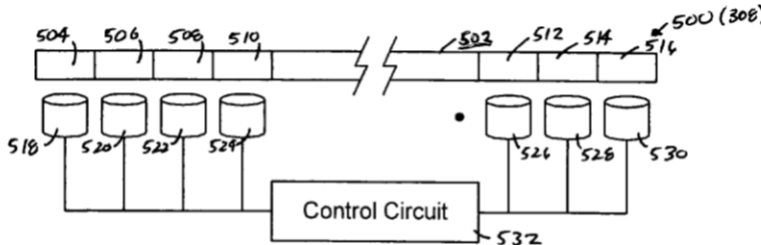
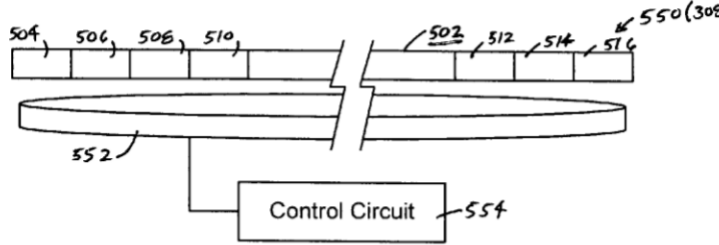
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
4. The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Doughty ’787 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.” For example: Doughty ’787 at Figure 11  Fig. 11 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]

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices. Doughty ’787 at [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 [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.

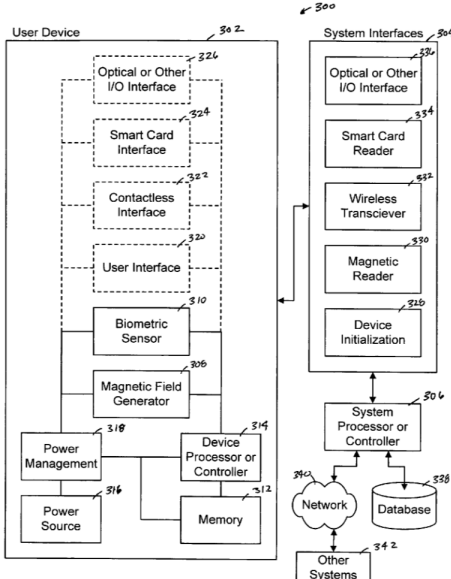
Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at [0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information 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 [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.

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	Doughty ’787 at [0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an “electronic purse” functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip. Doughty ’787 at [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 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.

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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. <i>See also</i> claim 1 above.
6. The mobile phone of claim 1 wherein the driver comprises a current driver.	Doughty ’787 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the driver comprises a current driver.” For example:

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 [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. <i>See also</i> 1[d] 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. <i>See also</i> claim 1 above.
7. The mobile phone of claim 1 wherein the network is one of a	Doughty ’787 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.” For example:

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
cellular network or a wireless local area network.	Doughty ’787 at Fig. 3  FIG. 3 Doughty ’787 at [0047] The one or more system interfaces 304 may include a device initialization interface 328, a magnetic reader 330, a wireless communications interface (transceiver) 332, a smart card reader 334, or an optical or other input/output interface 336. The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly, depending on the desired application and implementation. Other non-system interfaces may include a battery recharger, personal computer interface or personal data assistant (PDA). The one or more system interfaces 304 are communicably coupled to a system processor or controller 306, which in turn may be communicably coupled to a database 338 or one or more remote systems or computers 342 via network 340. Network 340 may be a local area network or wide area network, such as the Internet. Doughty ’787 at claim 63 63. The system as recited in claim 60, further comprising one or more remote computers communicably coupled to the system processor via a network.

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. <i>See also</i> claim 1 above.
8. The mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.	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. <i>See also</i> claim 1 above.
9. The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.	Doughty ’787 discloses or renders obvious “[t]he mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.” For example: 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.

Claim Element	Exemplary Citations to US20040133787A1 (“Doughty ’787”)
	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 [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 [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.

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. <i>See also</i> claim 1 above.

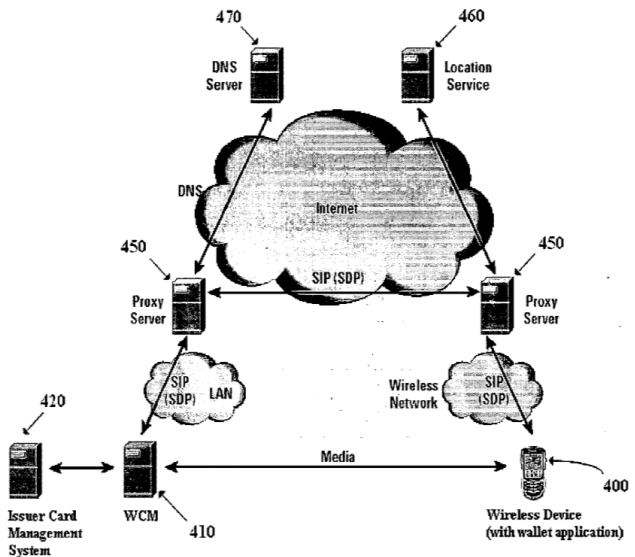
DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 11,270,174

EXHIBIT G3: US20060165060A1 ("Dua '060")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 11,270,174 ("the '174 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Dua '060 and (b) under 35 U.S.C. § 103(a) as obvious over Dua '060 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 G and Exhibits G1–G5, 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 '174 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 '174 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 US20060165060A1 ("Dua '060")
1[pre]. A mobile phone comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Dua '060 discloses or renders obvious "[a] mobile phone." For example: Dua '060 at Fig. 1

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at Fig. 3  Dua ’060 at Fig. 5

Claim Element

Exemplary Citations to US20060165060A1 (“Dua ’060”)

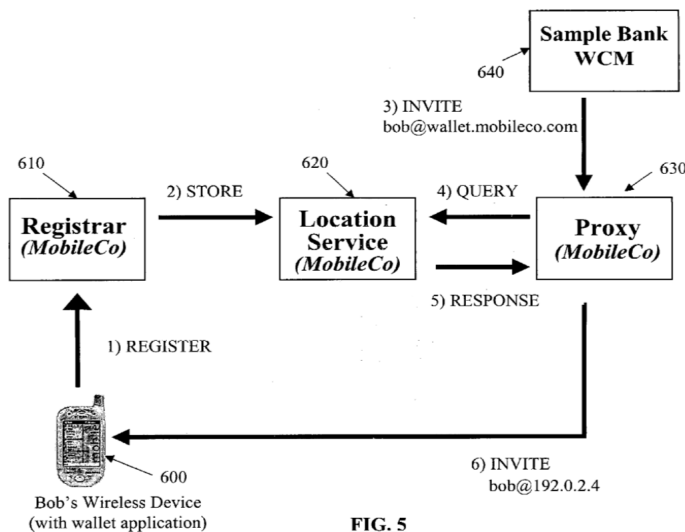


FIG. 5

Dua ’060 at Fig. 6A–B

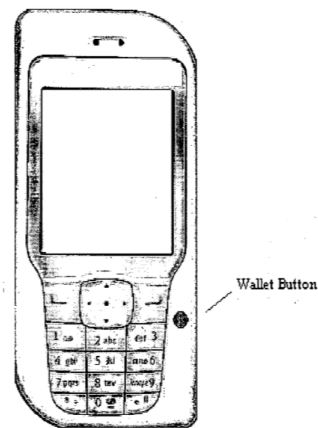


FIG. 6(a)

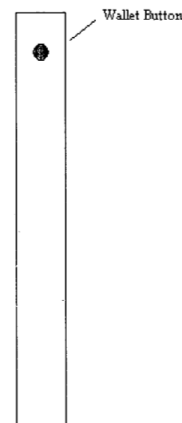
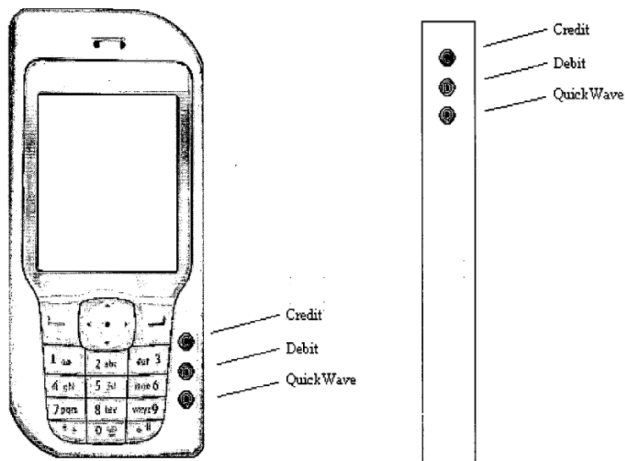


FIG. 6(b)

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at Fig. 7A–B  FIG. 7(a) shows a mobile phone with three buttons on the right side labeled Credit, Debit, and QuickWave. FIG. 7(b) shows a vertical device with three buttons labeled Credit, Debit, and QuickWave. <u>FIG. 7(a)</u> <u>FIG. 7(b)</u> Dua ’060 at [0023] It is a still further object of the present invention to provide for the secure importation of financial and other personal information into wireless devices. Dua ’060 at [0026] These and other objects of the present invention are obtained through the use of a novel system and methodology for conducting financial and other transactions requiring authorization. According to the methodology of the present invention, credentials may be selectively issued by issuers such as credit card companies, banks, and merchants to consumers permitting the specific consumer to conduct a transaction according to the authorization given as reflected by the credential or set of credentials. The preferred mechanism for controlling and distributing credentials according to the present invention is through one or more publicly accessible networks such as the Internet wherein the system design and operating characteristics are in conformance with the standards and other specific requirements of the chosen network or set of networks. According to a preferred embodiment of the invention, credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network. The user

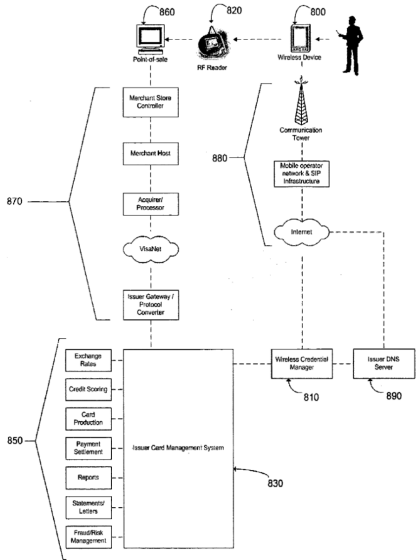
Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale (POS) terminal. Dua ’060 at [0039] Although FIG. 1 shows only a single wireless device 200 it will be readily understood that in deploying the present invention, credential issuers obtain the ability to selectively control credentials held by a practically unlimited number of wireless devices. The teachings of the present invention illustrate techniques for ensuring that the proper credentials are made available only to the proper wireless device or set of wireless devices. Various addressing and other techniques are used in the present invention to ensure secure control over the distribution of credentials to the wireless devices. Dua ’060 at [0041] As stated above, the present invention preferably involves the distribution of credentials to a “wireless device”. As used herein, wireless device 200 is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter. Preferably, wireless device 200 has a display screen and a key pad for alphanumeric and special character data input. It is further preferred that wireless device 200 has processing and secure storage capabilities allowing it to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically. Wireless device 200 also preferably has an integrated short-range communication capability for transmitting confidential information and exchanging other data between the wallet application and an external reader that is in proximity to the wireless device. Dua ’060 at [0046] WCM 110 provides for the secure Internet delivery of electronic credentials to wireless device 200 which is loaded with a wallet application. WCM 110 provides a secure and robust means of issuing, canceling, and managing electronic credentials on wireless devices via the Internet. WCM 110 leverages existing Internet protocols and technologies, making it easy for issuers to integrate with their existing systems, and alleviating the need to establish direct links with multiple mobile operators. Dua ’060 at [0048] According to the teachings of the present invention, an E.164 phone number is used to target a user's wallet application on Internet-enabled wireless device 200 for the delivery of credentials and confidential data, including but not limited to credit card, debit card, ATM card, loyalty card, driver's license,

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	electronic ticket, coupons and other information. In addition, an E.164 phone number is used according to the present invention to target a user's wallet application residing on wireless device 200 for the remote cancellation or updating of credentials. Also, E.164 phone numbers may be used as described herein to make person-to-person, person-to-company, or company-to-company electronic payments or fund transfers using wireless device 200. Although a preferred embodiment, this invention is not necessarily limited to the use of E.164 phone numbers. Rather, the use of URIs and other address types that are capable of being translated to an Internet address is also possible for the purposes mentioned above. Dua ’060 at [0053] In order to take advantage of ENUM, the mobile telephone number must first be assigned to a user by a telecom operator for services. The number can then be registered for one or more ENUM services. For example, a subscriber might wish to install a wallet application on wireless device 200 and register the telephone number as the identifier for the wallet application. Multiple issuers can in turn deliver payment methods, identification, or other types of electronic credentials to the wallet application on the wireless device 200 via the Internet using the phone number as the destination address. Additionally, that subscriber might wish to register an e-mail address or fax number to be associated with the same phone number. However the user chooses to set up these services, the information for the registered services, including the wallet application, is saved in NAPTR (Naming Authority Pointer) Resource Records. Dua ’060 at [0057] Turning now to FIG. 2, an overview of the credential issuance process of the present invention, in a preferred embodiment thereof, is now described. The credential issuance process begins with WCM 110 receiving a request from the issuer's card or user management system 120 to issue electronic credentials to an individual user (see step 310). The request is forwarded to WCM 110 along with the user's mobile (E.164) number, the credentials to be issued, encryption keys, and other information contained in the Personalization File for the specific request. The Personalization File may be a batch file that contains numerous records of credentials that are to be issued to individuals on their wireless device 200, or could be a separate file record for each credential to be issued. In another embodiment, the Personalization File is transmitted to WCM 110 by issuer personalization server 130 which is in communication with issuer cardholder system 120. Issuer personalization server communicates with personalization bureau server 140 which is typically maintained by the personalization bureau. Dua ’060 at [0126]

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Now that a general description of the methodology and components of the present invention has been provided, the following discussion provides examples of the use of the SIP protocol for issuing, canceling and updating credentials on a wireless device according to the teachings of the present invention. Dua ’060 at [0128] FIG. 4 shows a typical example of a SIP message exchange between a credential issuer (named herein Sample Bank) and a fictitious mobile user named Bob. (Each message is labeled with the letter “F” and a number for reference by the text.) In this example, SIP signaling functionality embedded in the Wireless Credential Manager (WCM) 510 is used to issue Bob a Sample Bank MasterCard on his SIP-enabled mobile device 500 via the Internet. Also shown are two SIP proxy servers that act on behalf of Sample Bank and Bob's mobile operator (MobileCo) to facilitate session establishment. This typical arrangement is often referred to as the “SIP trapezoid” as shown by the geometric shape of the dotted lines in FIG. 4. Dua ’060 at [0179] The media session between the Sample Bank WCM 510 and the wallet application on Bob's SIP enabled mobile phone 500 has now begun, and they can send data packets using the format to which they agreed in the exchange of SDP. In general, the end-to-end data packets take a different path from the SIP signaling messages. Dua ’060 at [0295] A wireless device loaded with the wallet application may come with some pre-loaded extensions. Extensions may reside on the device memory, in an embedded smart card, in a removable storage media, or on a remote server, securely accessible through the wallet application protocols. An extension may communicate with the user, may exchange information with remote servers or it may use other elements of the device hardware or software. Dua ’060 at [0315] In a local—or proximity—environment, the consumer is in the vicinity of a reader device that is connected to a point-of-sale (POS) terminal or some other type of computer system. Most day-to-day proximity transactions today use a card or token with information encoded in a variety of media types including magnetic stripe, bar code, chip, and embossed or printed data. A mobile device with a wallet application can serve as a replacement for single-purpose cards and tokens. During a proximity transaction, the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF). For example, a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	waved slowly in close proximity to a reader device to facilitate a transaction. Similarly, a wireless device that uses infra-red to transact with a reader requires that the user point the infra-red beam to a reader device. Dua ’060 at [0317] In a personal environment, mobile transactions are conducted on the user interface of another device and augmented by security, connectivity, information, and other functionality provided by the user's wireless device. For example, during a transaction—a point-of-sale device may establish secure connectivity with the user's wireless device and poll it for a list of user-defined payment methods that the user can select from using the user-interface of the POS system. The implication is that the user's wireless device can act as a repository of information that can be securely accessed by another device during a transaction. Dua ’060 at [0417] Assume that a wireless user has an electronic Sample Bank MasterCard credit card stored in the wallet application that is setup for OTA PIN validation. The user selects the electronic card for use in a proximity transaction at a grocery store, and the credential information is transmitted to a reader via RF as described earlier. The POS at the grocery store will switch the transaction to its central host, which in turn will recognize that this is a MasterCard credit card and switch it to the MasterCard network (either directly or through an acquirer/processor depending on configuration). MasterCard in turn switches the authorization request to Sample Bank which is the card issuer. Sample Bank's gateway receives the authorization request, and passes the transaction to its card management system for approval. The card management system checks the account status using the normal validation process it follows for credit card authorizations. One of the novel aspects of the present invention is that Sample Bank has implemented a new credit card product with OTA PIN verification. As such, a flag in the credit card customer account record signals to the credit card management system that an authorization approval can not be sent back to the retailer POS until an Over-the-Air PIN verification is completed. Dua ’060 at [0433] Receipts from a merchant can be sent to the user's wallet application on the wireless device via several methods as discussed herein. Under one design, the user's E.164 phone number for the wireless device is transmitted to the merchant with the credential information during an RF transaction. The wallet application would have the ability to learn the E.164 phone number of the device on which it operates through the device's operating system, or directly from the SIM card which may contain certain device settings and attributes like the E.164 number. A phone number field would be specified in the credential transmission record that is transmitted from the wireless device to the POS reader (or to a server in the

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	case of a remote transaction). Under this embodiment, the merchant's system receives the E.164 phone number of the device that initiated the transaction. The merchant could use the number in conjunction with a WCM deployed at the merchant's site to issue digital receipts to the wallet application. The merchant would have a WCM setup to interface with its central transaction processing system. The retailer's transaction processing system would temporarily hold the E.164 number received with the credential during an authorization request that originated at the POS. Dua ’060 at claim 1 1. A method for issuing a credential to a wireless device comprising the steps of: Dua ’060 at claim 44 44. The method of claim 1 wherein said wireless device is a mobile phone. Dua ’060 at claim 79 79. The system of claim 50 wherein said wireless device is a mobile phone. Dua ’060 at claim 92 2. The wireless device of claim 91 wherein said wireless device comprises a wireless telephone. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] a memory to hold transaction data for use in a plurality of transactions;	Dua ’060 discloses or renders obvious “a memory to hold transaction data for use in a plurality of transactions.” For example: Dua ’060 at [0041] As stated above, the present invention preferably involves the distribution of credentials to a “wireless device”. As used herein, wireless device 200 is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter. Preferably, wireless device 200 has a display screen and a key pad for alphanumeric and special character data input. It is further preferred that wireless device 200 has processing and secure storage capabilities allowing it to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically. Wireless device 200 also preferably has an integrated short-range

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	communication capability for transmitting confidential information and exchanging other data between the wallet application and an external reader that is in proximity to the wireless device. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;	Dua ’060 discloses or renders obvious “a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions.” For example: Dua ’060 at Figure 8  FIG. 8 Dua ’060 at [0009] A contactless smart card requires only close proximity to a reader. Both the reader and the card have antennas and it is via this contactless link that the two communicate via radio frequency (RF) when in close proximity. Most contactless cards typically receive power for on-card electronic functions via this electromagnetic signal. The range is typically two to three inches for non-battery powered cards, and this is ideal for applications such as mass transit which requires a very fast card interface.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at [0011] As stated, RF communication is used in connection with both contactless and hybrid smart cards. RF and Radio Frequency Identification (RFID) technologies come in a variety of forms, each of which may be tailored for use in different types of environments. These technologies differ in, for example, the frequency bands they employ, which in turn influences the rate of data transfer between the tag and reader. Consequently, different data transfer rate requirements influence the types of solutions that RFID services can and should be expected to provide. RFID technology is typically used for POS payments, electronic toll collection, access control, and numerous other applications. Dua ’060 at [0013] American Express, MasterCard, and Visa have agreed on a single contactless payment standard in the United States, ISO/IEC 14443, and are implementing a contactless payment approach that leverages the existing payments infrastructure. As a result, merchants can easily add a contactless RF reader to their existing POS systems and immediately begin accepting contactless payment. MasterCard and Visa have also been working jointly over the last few years to develop specifications that define a set of requirements for security and interoperability between chip cards and terminals on a global basis, regardless of the manufacturer, the financial institution, or where the card is used. Dua ’060 at [0016] Common short-range communications network standards defined by the International Electrical and Electronic Engineers association (IEEE) include 802.11a, 802.11b, and 802.11g. Many mobile devices employ these IEEE network standards to establish wireless LAN (WLAN) connectivity. Various other short-range technologies currently in use for device-to-device communication include Bluetooth and infra-red. One major short-range infra-red (IR) communications network protocol is defined by the Infra-red Device Association (IrDA), and is known as the IrDA standard. Wireless devices with integrated RFID proximity chips or Near Field Communication (NFC) technology may also provide users the ability to transfer information to a reader device. Dua ’060 at [0290] For example, when a subway contactless stored value card is waved in front of a reader at the turnstile, the electronic balance is automatically debited from the onboard chip. The rules that govern the functioning of that stored value program and the card's interaction with an external RF reader, are all programmed into the onboard chip.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at [0291] In the case of a magnetic-stripe credit card, the card is swiped in a POS terminal and magnetically encoded information on tracks 1 and 2 are read and captured by the reader. The data in turn is used to authorize the transaction with the card issuer. Dua ’060 at [0293] These are just a few examples of the types of credentials that can be issued to and stored within the wallet application. Implementing electronic versions of these credentials in the wallet application creates different operating and processing requirements for each credential. Consider the requirements associated with implementing the subway stored value credential through the wallet platform. The logic required to operate the subway stored value credential, the unique message format for communication between the wireless device and a RF reader at the turnstile, unique display messages, an over-the-air reload tool, and other features associated with the stored value credential that a user might see on the wireless device—all need to be programmed into the wallet application. These types of requirements are embodied in mini-programs that operate within the wallet application called “extensions” since they “extend” the capability of the wallet application in order to handle new features and capabilities that are specific to an issuer's credential. These extensions allow credentials to be used in a controlled way through specific issuer-defined functions. Dua ’060 at [0315] In a local—or proximity—environment, the consumer is in the vicinity of a reader device that is connected to a point-of-sale (POS) terminal or some other type of computer system. Most day-to-day proximity transactions today use a card or token with information encoded in a variety of media types including magnetic stripe, bar code, chip, and embossed or printed data. A mobile device with a wallet application can serve as a replacement for single-purpose cards and tokens. During a proximity transaction, the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF). For example, a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be waved slowly in close proximity to a reader device to facilitate a transaction. Similarly, a wireless device that uses infra-red to transact with a reader requires that the user point the infra-red beam to a reader device. Dua ’060 at [0317]

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	In a personal environment, mobile transactions are conducted on the user interface of another device and augmented by security, connectivity, information, and other functionality provided by the user's wireless device. For example, during a transaction—a point-of-sale device may establish secure connectivity with the user's wireless device and poll it for a list of user-defined payment methods that the user can select from using the user-interface of the POS system. The implication is that the user's wireless device can act as a repository of information that can be securely accessed by another device during a transaction. Dua ’060 at [0318] The wallet application will support peer-to-peer connectivity to a device in close proximity. Connectivity between the wireless device and the reader/POS terminal could be made via 802.11a/b/g, Bluetooth, or other RF protocols. Connectivity could initially be established by exchanging encryption keys via RFID that allow the devices to establish connectivity via an alternate channel securely so no other device can listen in to the communication. Keys could also initially be exchanged via infra-red technology. Dua ’060 at [0336] Payment Methods—Credit, debit/ATM, stored value, electronic check, and RFID payment methods may be registered with the wallet application Dua ’060 at [0353] Several features of this invention serve to minimize the key strokes a user has to make in searching for, selecting, and transmitting a credential to a reader. One such feature of this invention is the use of a credential-specific “reader key”. The key is sent with an electronic credential record to a wireless device during the issuance process. The same reader key is programmed in all reader devices employed by an organization. In the case of an RFID reader, the key is transmitted from the reader to the wireless device's RFID chip during a proximity transaction. The receipt of the key by the RFID chip in the wireless device may initiate the automatic launch of the wallet application resident on the device, and the transfer of the key to the application. The key is subsequently received by the wallet application and is used as a search string by the application to locate a specific credential for transmission back to the reader via the device's RF capability. Dua ’060 at [0354] The “reader key” is especially useful to organizations that are both issuers of electronic credentials and also acceptors of those credentials. An example would be a grocery chain that has a WCM for issuing electronic loyalty cards to mobile devices, and is also setup to accept those credentials via RFID readers installed at POS terminals in its stores. The grocery chain would program the reader key into all its RF

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	readers so that the key is transmitted during a proximity transaction to the RFID chip embedded in a wireless device. During the issuance process of a digital loyalty card, the grocery chain sends the reader key along with the loyalty credential to an end-user's wireless device. The wallet application stores the “reader key” with the electronic credential to which it is linked. When transmitted to the wireless device from the reader, the key is used by the wallet application as a search string for locating the linked credential. If a matching key is found within the wallet application, the corresponding loyalty information will be transmitted to the reader from the wireless device via RF. Dua ’060 at [0382] Because of the sensitive nature of information stored in the wallet application, user's want to ensure that they have complete control over the transmission of information to an external reader such as at a retail point-of-sale. This is especially important for wireless devices that have an embedded RFID chip for short-range transmission. While RFID cards automatically exchange information with a reader when held in close proximity, users require a greater sense of control when using an RFID-enabled wireless device that contains multiple pieces of confidential information. Dua ’060 at [0392] According to this embodiment, a user could use the “Wallet Settings” functionality in the wallet application to link his favorite/preferred credit card to button 1, and his favorite/preferred debit/ATM card to button 2. Button 3, labeled above as “QuickWave”, allows a user to transmit any PIN-less designated credential that has a “reader key” associated with it to a reader during a transaction. Dua ’060 at [0395] Pressing buttons 1 or 2, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click “OK” to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click “OK” to initiate PIN verification, and upon positive confirmation be prompted to hold down either button 1 or 2 while placing the device in close proximity to a reader. The press/release or hold down scenarios would also apply to button 3. Dua ’060 at [0405] As can be seen in FIG. 8, a first transmission path of an electronic credit card authorization request 870 includes, for example, a merchant store controller and merchant host system, an acquirer/processor network, a private network such as VisaNet, and a issuer gateway. Using these components, point of sale terminal 860, via RF reader 820 can be used to capture and transmit an electronic credential from a wireless device for online authorization. The second transmission path as shown in FIG. 8 is via WCM

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	810 using the Internet and wireless link 880 and issuer DNS server 890 and is used to deliver a PIN request to wireless device 800 and to receive a user-input response from wireless device 800. Dua ’060 at [0417] Assume that a wireless user has an electronic Sample Bank MasterCard credit card stored in the wallet application that is setup for OTA PIN validation. The user selects the electronic card for use in a proximity transaction at a grocery store, and the credential information is transmitted to a reader via RF as described earlier. The POS at the grocery store will switch the transaction to its central host, which in turn will recognize that this is a MasterCard credit card and switch it to the MasterCard network (either directly or through an acquirer/processor depending on configuration). MasterCard in turn switches the authorization request to Sample Bank which is the card issuer. Sample Bank's gateway receives the authorization request, and passes the transaction to its card management system for approval. The card management system checks the account status using the normal validation process it follows for credit card authorizations. One of the novel aspects of the present invention is that Sample Bank has implemented a new credit card product with OTA PIN verification. As such, a flag in the credit card customer account record signals to the credit card management system that an authorization approval can not be sent back to the retailer POS until an Over-the-Air PIN verification is completed. Dua ’060 at [0433] Receipts from a merchant can be sent to the user's wallet application on the wireless device via several methods as discussed herein. Under one design, the user's E.164 phone number for the wireless device is transmitted to the merchant with the credential information during an RF transaction. The wallet application would have the ability to learn the E.164 phone number of the device on which it operates through the device's operating system, or directly from the SIM card which may contain certain device settings and attributes like the E.164 number. A phone number field would be specified in the credential transmission record that is transmitted from the wireless device to the POS reader (or to a server in the case of a remote transaction). Under this embodiment, the merchant's system receives the E.164 phone number of the device that initiated the transaction. The merchant could use the number in conjunction with a WCM deployed at the merchant's site to issue digital receipts to the wallet application. The merchant would have a WCM setup to interface with its central transaction processing system. The retailer's transaction processing system would temporarily hold the E.164 number received with the credential during an authorization request that originated at the POS. Dua ’060 at claim 20 20. The method of claim 1 wherein said credential comprises a credit card account.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;	Dua ’060 discloses or renders obvious “a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network.” For example: Dua ’060 at Abstract A novel system and methodology for conducting financial and other transactions using a wireless device. Credentials may be selectively issued by issuers such as credit card companies, banks, and merchants to consumers permitting the specific consumer to conduct a transaction according to the authorization given as reflected by the credential or set of credentials. The preferred mechanism for controlling and distributing credentials according to the present invention is through one or more publicly accessible networks such as the Internet wherein the system design and operating characteristics are in conformance with the standards and other specific requirements of the chosen network or set of networks. Credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale terminal. Dua ’060 at Fig. 1

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at Fig. 3 Dua ’060 at Fig. 4

Claim Element

Exemplary Citations to US20060165060A1 (“Dua ’060”)

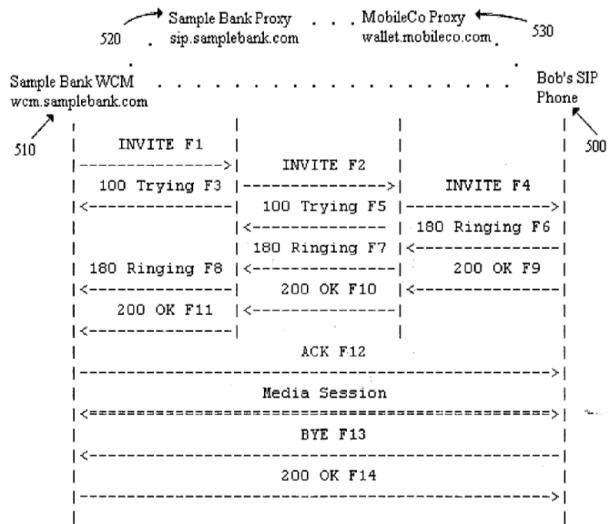


FIG. 4

Dua ’060 at Fig. 5

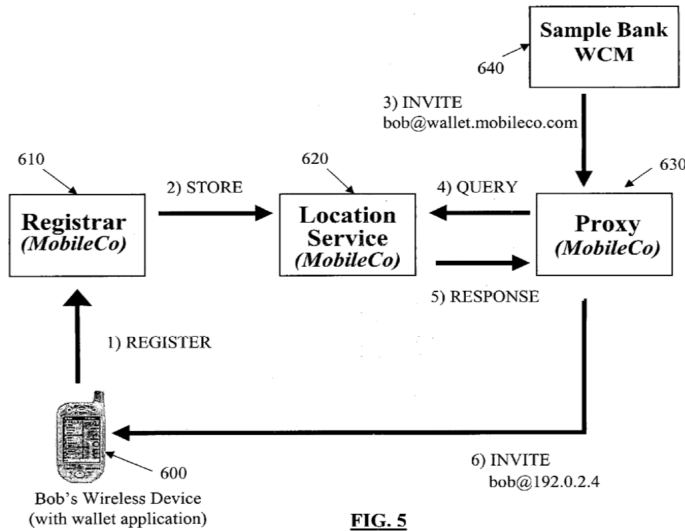
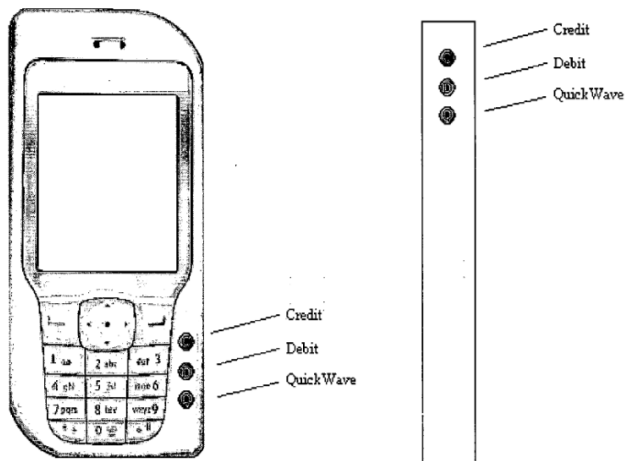
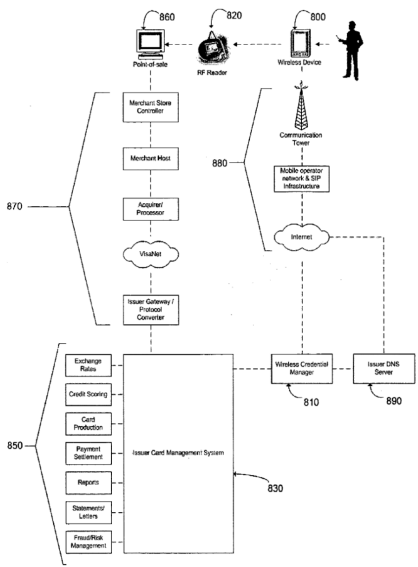


FIG. 5

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at Fig. 7A–B  FIG. 7(a) shows a mobile phone with a screen and a keypad. Three buttons on the right side of the keypad are labeled 'Credit', 'Debit', and 'QuickWave'. FIG. 7(b) shows a vertical strip with three buttons labeled 'Credit', 'Debit', and 'QuickWave'. <u>FIG. 7(a)</u> <u>FIG. 7(b)</u> Dua ’060 at Figure 8

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	 FIG. 8 Dua ’060 at [0016] Common short-range communications network standards defined by the International Electrical and Electronic Engineers association (IEEE) include 802.11a, 802.11b, and 802.11g. Many mobile devices employ these IEEE network standards to establish wireless LAN (WLAN) connectivity. Various other short-range technologies currently in use for device-to-device communication include Bluetooth and infra-red. One major short-range infra-red (IR) communications network protocol is defined by the Infra-red Device Association (IrDA), and is known as the IrDA standard. Wireless devices with integrated RFID proximity chips or Near Field Communication (NFC) technology may also provide users the ability to transfer information to a reader device. Dua ’060 at [0026] These and other objects of the present invention are obtained through the use of a novel system and methodology for conducting financial and other transactions requiring authorization. According to the methodology of the present invention, credentials may be selectively issued by issuers such as credit card companies, banks, and merchants to consumers permitting the specific consumer to conduct a transaction according to the authorization given as reflected by the credential or set of credentials. The preferred mechanism for controlling and distributing credentials according to the present invention is through one

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	or more publicly accessible networks such as the Internet wherein the system design and operating characteristics are in conformance with the standards and other specific requirements of the chosen network or set of networks. According to a preferred embodiment of the invention, credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale (POS) terminal. Dua ’060 at [0038] A general discussion of the present invention is now provided and is thereafter followed by a detailed description of each of the components and functions of the invention according to specific preferred embodiments. FIG. 1 is an overall system diagram illustrating some of the key components of the credential distribution system of the present invention in a preferred embodiment thereof. The ultimate goal of the present invention is to securely, accurately and rapidly distribute credentials to the proper wireless devices based upon the actions of credential issuers. It is also important that these credential issuers have the ability to securely, accurately and rapidly update credentials as required. In furtherance of this, wireless credential manager 110 of the present invention functions to manage, distribute and update credentials so that they are contained as desired in a wallet software application running on wireless device 200. A set of components 100 collectively comprise a subsystem capable of, among other things, causing the issuance of a credential to wireless device 200 according to the teachings of the present invention. Dua ’060 at [0040] In a preferred embodiment of the present invention, distribution of credentials is made via a transmission initiated by Issuer Cardholder System 120 to Wireless Credential Manager 110 which causes the credential or set of credentials to be transmitted to wireless device 200 via the Internet and/or one or more alternative public or private networks. Based upon the specific addressing schemes employed herein, the credential may then ultimately make its way to the targeted wireless device via an over-the-air wireless link. Dua ’060 at [0041] As stated above, the present invention preferably involves the distribution of credentials to a “wireless device”. As used herein, wireless device 200 is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter. Preferably, wireless device 200 has a display screen and a key pad for

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	alphanumeric and special character data input. It is further preferred that wireless device 200 has processing and secure storage capabilities allowing it to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically. Wireless device 200 also preferably has an integrated short-range communication capability for transmitting confidential information and exchanging other data between the wallet application and an external reader that is in proximity to the wireless device. Dua ’060 at [0043] Wireless Credential Manager (WCM) 110 maintains, controls and distributes credentials in accordance with the teachings herein. In a preferred embodiment, WCM 110 is able to interface with a payment, identification, and/or other existing user management or card management systems such as issuer cardholder system 120. An issuer representative may interface with issuer cardholder system 120 through the use of customer care terminal 150. The process for issuing a credential according to the present invention may be initiated manually by an issuer representative via terminal 150. Alternatively, the customer himself may initiate the process through interactive voice response (IVR) system 160 by calling in through wireline phone 165 via PSTN network 170. Dua ’060 at [0044] Other alternatives for initiating the process include the use of computer via the requesting party's ISP 178, the Internet 180 and through the issuer's web server 182 to issuer cardholder system 120. Still another alternative for initiating the credential issuing process is through wireless device 200 via mobile operator network 155, SIP proxy 157, Internet 180 and issuer's web server 182. The wireless device used to initiate the credential issuance process may be either the device to receive the credential or another wireless device. Dua ’060 at [0046] WCM 110 provides for the secure Internet delivery of electronic credentials to wireless device 200 which is loaded with a wallet application. WCM 110 provides a secure and robust means of issuing, canceling, and managing electronic credentials on wireless devices via the Internet. WCM 110 leverages existing Internet protocols and technologies, making it easy for issuers to integrate with their existing systems, and alleviating the need to establish direct links with multiple mobile operators. Dua ’060 at [0048] According to the teachings of the present invention, an E.164 phone number is used to target a user's wallet application on Internet-enabled wireless device 200 for the delivery of credentials and confidential

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	data, including but not limited to credit card, debit card, ATM card, loyalty card, driver's license, electronic ticket, coupons and other information. In addition, an E.164 phone number is used according to the present invention to target a user's wallet application residing on wireless device 200 for the remote cancellation or updating of credentials. Also, E.164 phone numbers may be used as described herein to make person-to-person, person-to-company, or company-to-company electronic payments or fund transfers using wireless device 200. Although a preferred embodiment, this invention is not necessarily limited to the use of E.164 phone numbers. Rather, the use of URIs and other address types that are capable of being translated to an Internet address is also possible for the purposes mentioned above. Dua ’060 at [0050] The use of ENUM presupposes the collection of these records into a central or hierarchical service. According to a preferred embodiment, the resolved Internet address is used to establish secure real-time communication between WCM 110 and the wallet application on wireless device 200 using the Session Initiation Protocol (SIP) (for example, according to the RFC 3261 standard) to transfer encrypted credentials. The issuer WCM 110 may also be used to update credentials or update the status of credentials on wireless device 200. WCM 110 may also be used to authenticate a mobile user's identity in real-time during a transaction. While the use of SIP for such purposes is preferred, alternative application protocols may be used in lieu of SIP while still remaining within the spirit and scope of the present invention. Dua ’060 at [0053] In order to take advantage of ENUM, the mobile telephone number must first be assigned to a user by a telecom operator for services. The number can then be registered for one or more ENUM services. For example, a subscriber might wish to install a wallet application on wireless device 200 and register the telephone number as the identifier for the wallet application. Multiple issuers can in turn deliver payment methods, identification, or other types of electronic credentials to the wallet application on the wireless device 200 via the Internet using the phone number as the destination address. Additionally, that subscriber might wish to register an e-mail address or fax number to be associated with the same phone number. However the user chooses to set up these services, the information for the registered services, including the wallet application, is saved in NAPTR (Naming Authority Pointer) Resource Records. Dua ’060 at [0055] According to the present invention, electronic credentials may be issued to a wallet application on a wireless device 200 held (owned, rented or otherwise controlled) by a user that already has a physical card or token-based credential. For example, an existing bank customer that has a magnetic-stripe credit card

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	may also request a digital card for use with the wallet application on his or her wireless device 200. The bank customer could request the new credential over the phone by first validating his or her identity with the issuer, by logging into the issuer's secure web site using a valid username and password, or in person at a branch. Dua ’060 at [0056] Credentials may alternatively be issued to a wireless device held by a user that is applying for a new credential for the first time. For example, a user may be applying for a credit card for the first time, and may wish to only request the credential on his or her mobile phone. According to the teachings of this invention, credential issuers may request from applicants (e.g. over the telephone) a properly formatted E.164 phone number in order to target the delivery of credential(s) to a wallet application on wireless device 200. The request for a E.164 wireless device number on an application for a credit card, debit card, ATM card, loyalty card, driver's license, security pass, coupons, certificates, or other credential type is made by the issuer. The E.164 phone number may be obtained on paper, via a web-based application, via an electronic kiosk, via telephone or it may be captured through other means. Dua ’060 at [0057] Turning now to FIG. 2, an overview of the credential issuance process of the present invention, in a preferred embodiment thereof, is now described. The credential issuance process begins with WCM 110 receiving a request from the issuer's card or user management system 120 to issue electronic credentials to an individual user (see step 310). The request is forwarded to WCM 110 along with the user's mobile (E.164) number, the credentials to be issued, encryption keys, and other information contained in the Personalization File for the specific request. The Personalization File may be a batch file that contains numerous records of credentials that are to be issued to individuals on their wireless device 200, or could be a separate file record for each credential to be issued. In another embodiment, the Personalization File is transmitted to WCM 110 by issuer personalization server 130 which is in communication with issuer cardholder system 120. Issuer personalization server communicates with personalization bureau server 140 which is typically maintained by the personalization bureau. Dua ’060 at [0102] SIP is based on an HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular method, or function, on the server and at least one response. SIP uses most of the header fields, encoding rules, and status codes of HTTP. This provides a readable text-based format for displaying information. SIP incorporates the use of Session Description Protocol (SDP), which defines

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	session content using a set of types similar to those used in Multipurpose Internet Mail Extensions (MIME). Technically, SIP will function across both IPv4 and IPv6 networks. Dua ’060 at [0104] The present invention, in a preferred embodiment provides for using some of the SIP-network infrastructure that mobile operators will have in place to deliver credentials from SIP-based Wireless Credential Manager (WCM) 110 at an issuer site to a SIP-based wallet application on a wireless device 200. The system disclosed herein is designed to interoperate with mobile 2.5G, 3G, and Wi-Fi networks among others. Dua ’060 at [0107] FIG. 3 illustrates some of the SIP components, their relationship to one another and the protocols that are employed. A user agent acting as a client (in this case the issuer WCM 410 which is in communication with issuer card management system 420) uses SIP to set up a session with a user agent that acts as a server (in this case a wallet application operating on user's wireless device 400). The session initiation dialogue uses SIP and involves one or more proxy servers to forward requests and responses between the two user agents. The user agents also make use of the SDP, which is used to describe the media session. Dua ’060 at [0126] Now that a general description of the methodology and components of the present invention has been provided, the following discussion provides examples of the use of the SIP protocol for issuing, canceling and updating credentials on a wireless device according to the teachings of the present invention. Dua ’060 at [0128] FIG. 4 shows a typical example of a SIP message exchange between a credential issuer (named herein Sample Bank) and a fictitious mobile user named Bob. (Each message is labeled with the letter “F” and a number for reference by the text.) In this example, SIP signaling functionality embedded in the Wireless Credential Manager (WCM) 510 is used to issue Bob a Sample Bank MasterCard on his SIP-enabled mobile device 500 via the Internet. Also shown are two SIP proxy servers that act on behalf of Sample Bank and Bob's mobile operator (MobileCo) to facilitate session establishment. This typical arrangement is often referred to as the “SIP trapezoid” as shown by the geometric shape of the dotted lines in FIG. 4. Dua ’060 at [0129] WCM 510 may initiate communication with a wallet application on Bob's wireless device 500 through a SIP proxy server on MobileCo's network that also handles voice, instant messaging, and other services.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at [0155] Since WCM 510 does not know the location of Bob or the SIP server in the mobileco.com domain, WCM 510 sends the INVITE to the SIP server that serves Sample Bank's domain, samplebank.com. The address of the Sample Bank SIP server (sip.samplebank.com) could have been configured in WCM 510, or it could have been discovered by DHCP, for example. It should be noted that for illustrative purposes the SIP proxy functionality was shown as a being a separate server from WCM 510; in reality the proxy functionality is a part of WCM 510. The proxy component of WCM 510 is an important aspect of this system and the overall methodology. Dua ’060 at [0179] The media session between the Sample Bank WCM 510 and the wallet application on Bob's SIP enabled mobile phone 500 has now begun, and they can send data packets using the format to which they agreed in the exchange of SDP. In general, the end-to-end data packets take a different path from the SIP signaling messages. Dua ’060 at [0180] The established session may initially be used to exchange encryption keys and/or other security information. Subsequent to that, the issuer's system will authenticate the mobile user's identity in real-time to ensure that the person on the receiving end is in fact the person that requested the digital credential. The authentication process can be accomplished by the issuer system prompting the user for some cardholder or accountholder authentication information contained within its system, that only the rightful accountholder would have. The user would see such a request for information within the wallet application screen on the device display. This could include a request for such information such as an existing card account number, card expiration date, cardholder name, mother's maiden name, billing address, social security number, account balance, transaction history, driver's license number, or business identification. The issuer could also request a special code or PIN that was mailed to the user in advance of the issuance as a means to further validate identity and ensure non-repudiation. Some of the input information individually, or a combination of certain input information could be used as a decryption key for a credential that is transmitted to the wireless device. Subsequent to the issuer's system validating the user's identity in real-time, the WCM 510 will transmit the credential to the wallet application. Dua ’060 at [0295] A wireless device loaded with the wallet application may come with some pre-loaded extensions. Extensions may reside on the device memory, in an embedded smart card, in a removable storage media,

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	or on a remote server, securely accessible through the wallet application protocols. An extension may communicate with the user, may exchange information with remote servers or it may use other elements of the device hardware or software. Dua ’060 at [0296] Credit card associations/networks may develop a software extension for the wallet application that governs the interaction between the RFID chip embedded in a wireless device and a reader terminal. A modified version of the “MasterCard Proximity Chip Payment—Online Profile” and the “Visa Specification for Financial Messaging for Contactless Payment” could be embodied in a software extension for the wallet application. The use of such an extension for facilitating credit card transactions using the wallet application is an important part of the present invention. The provisioning of such an extension to a wireless device using a valid E.164 number of URI is also possible. The same extensions could be used by multiple issuing banks. Dua ’060 at [0297] The actual account information or personal information that is transmitted by the issuer to the wallet application is referred to as the “credential”. The actual credential record that is transmitted to the wallet application by the issuer may contain some of the following information: Dua ’060 at [0323] In a remote—or online—environment, transactions are conducted with a remote server over a wireless network. For example, a remote transaction using a wireless device can be conducted over the Internet with a browser on the wireless device. In such transactions, the wireless device's user interface (UI) is of paramount importance. The UI must relay all relevant information to maintain the user's trust and ensure usability of the services. Remote transactions range from online purchases and banking to more impulsive activities like downloading digital content. Dua ’060 at [0347] If a credential is received by the wallet application containing a primary and/or secondary category that does not yet exist in the credential tree, the wallet application will add the primary and/or secondary category automatically before linking the credential to it. Dua ’060 at [0402] Other credential issuers may issue a credential to a wireless device, require the wallet PIN with every transaction, but also prompt the user for an issuer PIN (or PIN set with the issuer) on the POS terminal

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	during each transaction. The POS terminal may know to prompt for a PIN based on a card BIN number for example. Dua ’060 at [0405] As can be seen in FIG. 8, a first transmission path of an electronic credit card authorization request 870 includes, for example, a merchant store controller and merchant host system, an acquirer/processor network, a private network such as VisaNet, and a issuer gateway. Using these components, point of sale terminal 860, via RF reader 820 can be used to capture and transmit an electronic credential from a wireless device for online authorization. The second transmission path as shown in FIG. 8 is via WCM 810 using the Internet and wireless link 880 and issuer DNS server 890 and is used to deliver a PIN request to wireless device 800 and to receive a user-input response from wireless device 800. Dua ’060 at [0408] After the issuer's card management system 830 has validated that the account is in good status and is qualified for “approval”, a PIN request is generated by the system and sent to WCM 810 via a real-time interface along with information relating to the transaction and certain account information. (If the account is not in good status or does not qualify for an “approval”, a denial message would be sent through the network(s) to the origination point.) The PIN request message sent to WCM 810 should include fields such as the name of the organization that originated the authorization request, location ID from where the request originated (e.g. a store address), date/time of authorization request, transaction amount being authorized (or purpose of transaction if a non-financial transaction), transaction ID, last four digits of account number, credential type (e.g. Visa Credit Card), issuer name, and the E.164 mobile phone number retrieved from the credential holder's account (in Application Unique String format as defined earlier). There must be a valid E.164 mobile phone number in the account record in order to enable OTA PIN verification with a credential. Dua ’060 at [0422] Under another embodiment of this invention, the dual network processing path utilized for transactions involving OTA PIN verification as described above, could be used to prompt a user for certain preference information on his wireless device 800 during a transaction. For example, Sample Bank may create an innovative payment product (herein called the “Wallet Account”) that links together multiple payment accounts such as a credit account, a debit account, and a stored value account under a single account number. The Wallet Account number could utilize a Visa, MasterCard, American Express, Discover, Diners, or other network/association Bank Identification Number (BIN) range that allows Wallet Account transactions to be authorized by a retailer's POS systems the way credit/debit card transactions are 870.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	When a Wallet Account transaction reaches Sample Bank's Card Management System 830 for authorization, Sample Bank's system 830 will discern that the account number corresponds to a valid Wallet Account which has a credit, debit, and stored value account linked. Using the user's E.164 number stored in Sample Bank's Card Management System 830, the Card Management System will send a message to the user's wireless device 800 to request a PIN (as described earlier) and to ask the user to specify his choice of using one of the linked credit, debit, or stored value accounts for completing the transaction. This request for payment preference traverses the same network path as the OTA PIN verification request described earlier, and traverses the Internet and mobile operator network 880. Based on the user's payment preference input into wireless device 800, Sample Bank's Card Management System 830 can authorize and apply the transaction to the appropriate account. This example illustrates that requests for user preferences or other information during a transaction can traverse a completely different network path (comprised of one or more networks) than the original online authorization via one network path (comprised of one or more networks). Also illustrated is the fact that OTA PIN requests can be coupled with requests for user preferences or other information. Dua ’060 at [0453] During the setup process of the wallet application, a mobile operator will issue a unique “mobile operator key” to each wallet application device. The key is stored in the wallet application, and is used by the operator to reset the wallet application remotely in the event that the device is lost/stolen, and to manage other wallet settings like (SIP proxy server addresses, DNS server addresses, etc). Dua ’060 at [0494] Credentials will be issued to the wireless device in the manner previously described in this document with only a slight modification to where the credentials actually get stored. When an issuer's WCM opens a peer-to-peer SIP connection with the wallet application on the wireless device, the wallet application will have an open connection maintained to the secure storage service. Any credentials that are issued to the wireless device will be transparently transmitted to the storage service where they will reside. The connection between the wallet application and the storage service could utilize an application protocol such as HTTP, SIP, or others. Any data transmitted to the storage service will be registered with the wallet application first; the registration of credentials, personal information, and other confidential data within the wallet application allows the wallet application to display headers for information in storage without having to retrieve it online; the registration process also allows the wallet application to call specific data from storage based on the assigned registration ID for the data object in storage. Dua ’060 at claim 1

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	(b) accepting a routable address associated with said request, said routable address being routable over a data network; Dua ’060 at claim 1 (c) accepting data associated with said credential; and Dua ’060 at claim 49 (d) means for issuing said credential to said wireless device through a transmission path comprising a data network and a wireless link. Dua ’060 at claim 50 50. A system for transmitting a credential from an issuer to a wireless device comprising: Dua ’060 at claim 50 (b) a network for transmitting said credential to said wireless device, said network further comprising a non-wireless network portion and a wireless network portion; Dua ’060 at claim 89 89. The system of claim 50 further comprising an RF reader and an issuer account management system, wherein said wireless device operates to transmit credential information to said RF reader and said RF reader transmits said credential information to said issuer account management system through a first network path and, in response to said transmission, a PIN request is transmitted by said issuer account management system to said wireless device through a second network path. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] a driver to excite the current carrying conductor; and	To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1e] a processor coupled to control the driver.	To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
2. The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	Dua ’060 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.” For example: Dua ’060 at Figure 8 FIG. 8 Dua ’060 at [0011] As stated, RF communication is used in connection with both contactless and hybrid smart cards. RF and Radio Frequency Identification (RFID) technologies come in a variety of forms, each of which may be tailored for use in different types of environments. These technologies differ in, for example, the frequency bands they employ, which in turn influences the rate of data transfer between the tag and reader. Consequently, different data transfer rate requirements influence the types of solutions that RFID services can and should be expected to provide. RFID technology is typically used for POS payments, electronic toll collection, access control, and numerous other applications. Dua ’060 at [0013] American Express, MasterCard, and Visa have agreed on a single contactless payment standard in the United States, ISO/IEC 14443, and are implementing a contactless payment approach that leverages the existing payments infrastructure. As a result, merchants can easily add a contactless RF reader to their existing POS systems and immediately begin accepting contactless payment. MasterCard and Visa have

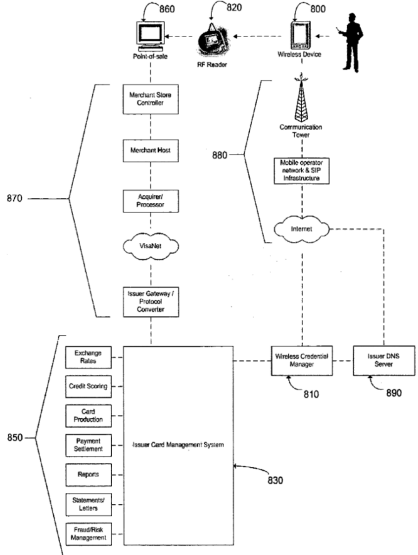
Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	also been working jointly over the last few years to develop specifications that define a set of requirements for security and interoperability between chip cards and terminals on a global basis, regardless of the manufacturer, the financial institution, or where the card is used. Dua ’060 at [0290] For example, when a subway contactless stored value card is waved in front of a reader at the turnstile, the electronic balance is automatically debited from the onboard chip. The rules that govern the functioning of that stored value program and the card's interaction with an external RF reader, are all programmed into the onboard chip. Dua ’060 at [0293] These are just a few examples of the types of credentials that can be issued to and stored within the wallet application. Implementing electronic versions of these credentials in the wallet application creates different operating and processing requirements for each credential. Consider the requirements associated with implementing the subway stored value credential through the wallet platform. The logic required to operate the subway stored value credential, the unique message format for communication between the wireless device and a RF reader at the turnstile, unique display messages, an over-the-air reload tool, and other features associated with the stored value credential that a user might see on the wireless device—all need to be programmed into the wallet application. These types of requirements are embodied in mini-programs that operate within the wallet application called “extensions” since they “extend” the capability of the wallet application in order to handle new features and capabilities that are specific to an issuer's credential. These extensions allow credentials to be used in a controlled way through specific issuer-defined functions. Dua ’060 at [0315] In a local—or proximity—environment, the consumer is in the vicinity of a reader device that is connected to a point-of-sale (POS) terminal or some other type of computer system. Most day-to-day proximity transactions today use a card or token with information encoded in a variety of media types including magnetic stripe, bar code, chip, and embossed or printed data. A mobile device with a wallet application can serve as a replacement for single-purpose cards and tokens. During a proximity transaction, the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF). For example, a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be waved slowly in close proximity to a reader device to facilitate a transaction. Similarly, a wireless device

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	that uses infra-red to transact with a reader requires that the user point the infra-red beam to a reader device. Dua ’060 at [0317] In a personal environment, mobile transactions are conducted on the user interface of another device and augmented by security, connectivity, information, and other functionality provided by the user's wireless device. For example, during a transaction—a point-of-sale device may establish secure connectivity with the user's wireless device and poll it for a list of user-defined payment methods that the user can select from using the user-interface of the POS system. The implication is that the user's wireless device can act as a repository of information that can be securely accessed by another device during a transaction. Dua ’060 at [0336] Payment Methods—Credit, debit/ATM, stored value, electronic check, and RFID payment methods may be registered with the wallet application Dua ’060 at [0353] Several features of this invention serve to minimize the key strokes a user has to make in searching for, selecting, and transmitting a credential to a reader. One such feature of this invention is the use of a credential-specific “reader key”. The key is sent with an electronic credential record to a wireless device during the issuance process. The same reader key is programmed in all reader devices employed by an organization. In the case of an RFID reader, the key is transmitted from the reader to the wireless device's RFID chip during a proximity transaction. The receipt of the key by the RFID chip in the wireless device may initiate the automatic launch of the wallet application resident on the device, and the transfer of the key to the application. The key is subsequently received by the wallet application and is used as a search string by the application to locate a specific credential for transmission back to the reader via the device's RF capability. Dua ’060 at [0395] Pressing buttons 1 or 2, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click “OK” to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click “OK” to initiate PIN verification, and upon positive confirmation be prompted to hold down either button 1 or 2 while placing the device in close proximity to a reader. The press/release or hold down scenarios would also apply to button 3. Dua ’060 at [0405]

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	As can be seen in FIG. 8, a first transmission path of an electronic credit card authorization request 870 includes, for example, a merchant store controller and merchant host system, an acquirer/processor network, a private network such as VisaNet, and a issuer gateway. Using these components, point of sale terminal 860, via RF reader 820 can be used to capture and transmit an electronic credential from a wireless device for online authorization. The second transmission path as shown in FIG. 8 is via WCM 810 using the Internet and wireless link 880 and issuer DNS server 890 and is used to deliver a PIN request to wireless device 800 and to receive a user-input response from wireless device 800. Dua ’060 at [0417] Assume that a wireless user has an electronic Sample Bank MasterCard credit card stored in the wallet application that is setup for OTA PIN validation. The user selects the electronic card for use in a proximity transaction at a grocery store, and the credential information is transmitted to a reader via RF as described earlier. The POS at the grocery store will switch the transaction to its central host, which in turn will recognize that this is a MasterCard credit card and switch it to the MasterCard network (either directly or through an acquirer/processor depending on configuration). MasterCard in turn switches the authorization request to Sample Bank which is the card issuer. Sample Bank's gateway receives the authorization request, and passes the transaction to its card management system for approval. The card management system checks the account status using the normal validation process it follows for credit card authorizations. One of the novel aspects of the present invention is that Sample Bank has implemented a new credit card product with OTA PIN verification. As such, a flag in the credit card customer account record signals to the credit card management system that an authorization approval can not be sent back to the retailer POS until an Over-the-Air PIN verification is completed. Dua ’060 at [0433] Receipts from a merchant can be sent to the user's wallet application on the wireless device via several methods as discussed herein. Under one design, the user's E.164 phone number for the wireless device is transmitted to the merchant with the credential information during an RF transaction. The wallet application would have the ability to learn the E.164 phone number of the device on which it operates through the device's operating system, or directly from the SIM card which may contain certain device settings and attributes like the E.164 number. A phone number field would be specified in the credential transmission record that is transmitted from the wireless device to the POS reader (or to a server in the case of a remote transaction). Under this embodiment, the merchant's system receives the E.164 phone number of the device that initiated the transaction. The merchant could use the number in conjunction with a WCM deployed at the merchant's site to issue digital receipts to the wallet application. The merchant would have a WCM setup to interface with its central transaction processing system. The

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	retailer's transaction processing system would temporarily hold the E.164 number received with the credential during an authorization request that originated at the POS. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
3. The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	Dua ’060 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.” For example: Dua ’060 at [0011] As stated, RF communication is used in connection with both contactless and hybrid smart cards. RF and Radio Frequency Identification (RFID) technologies come in a variety of forms, each of which may be tailored for use in different types of environments. These technologies differ in, for example, the frequency bands they employ, which in turn influences the rate of data transfer between the tag and reader. Consequently, different data transfer rate requirements influence the types of solutions that RFID services can and should be expected to provide. RFID technology is typically used for POS payments, electronic toll collection, access control, and numerous other applications. Dua ’060 at [0293] These are just a few examples of the types of credentials that can be issued to and stored within the wallet application. Implementing electronic versions of these credentials in the wallet application creates different operating and processing requirements for each credential. Consider the requirements associated with implementing the subway stored value credential through the wallet platform. The logic required to operate the subway stored value credential, the unique message format for communication between the wireless device and a RF reader at the turnstile, unique display messages, an over-the-air reload tool, and other features associated with the stored value credential that a user might see on the wireless device—all need to be programmed into the wallet application. These types of requirements are embodied in mini-programs that operate within the wallet application called “extensions” since they “extend” the capability of the wallet application in order to handle new features and capabilities that are specific to an issuer's credential. These extensions allow credentials to be used in a controlled way through specific issuer-defined functions. Dua ’060 at [0338]

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Membership Cards—Personal memberships to video rental stores, libraries, and other organizations Dua ’060 at [0339] Access Cards—Electronic keys for offices, apartments, parking garages, cars, and other secure facilities Dua ’060 at [0340] E-Tickets & Passes—Electronic tickets for sporting events, concerts, shows, transportation, and other purposes may be issued to the wallet application. Dua ’060 at [0417] Assume that a wireless user has an electronic Sample Bank MasterCard credit card stored in the wallet application that is setup for OTA PIN validation. The user selects the electronic card for use in a proximity transaction at a grocery store, and the credential information is transmitted to a reader via RF as described earlier. The POS at the grocery store will switch the transaction to its central host, which in turn will recognize that this is a MasterCard credit card and switch it to the MasterCard network (either directly or through an acquirer/processor depending on configuration). MasterCard in turn switches the authorization request to Sample Bank which is the card issuer. Sample Bank's gateway receives the authorization request, and passes the transaction to its card management system for approval. The card management system checks the account status using the normal validation process it follows for credit card authorizations. One of the novel aspects of the present invention is that Sample Bank has implemented a new credit card product with OTA PIN verification. As such, a flag in the credit card customer account record signals to the credit card management system that an authorization approval can not be sent back to the retailer POS until an Over-the-Air PIN verification is completed. Dua ’060 at claim 27 27. The method of claim 1 wherein said credential comprises a security access card. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
4. The mobile phone of claim 1 wherein the time-varying magnetic	Dua ’060 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.” For example:

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
field represents a credit card transaction.	Dua ’060 at Figure 8  FIG. 8 Dua ’060 at [0011] As stated, RF communication is used in connection with both contactless and hybrid smart cards. RF and Radio Frequency Identification (RFID) technologies come in a variety of forms, each of which may be tailored for use in different types of environments. These technologies differ in, for example, the frequency bands they employ, which in turn influences the rate of data transfer between the tag and reader. Consequently, different data transfer rate requirements influence the types of solutions that RFID services can and should be expected to provide. RFID technology is typically used for POS payments, electronic toll collection, access control, and numerous other applications. Dua ’060 at [0013] American Express, MasterCard, and Visa have agreed on a single contactless payment standard in the United States, ISO/IEC 14443, and are implementing a contactless payment approach that leverages the existing payments infrastructure. As a result, merchants can easily add a contactless RF reader to their existing POS systems and immediately begin accepting contactless payment. MasterCard and Visa have also been working jointly over the last few years to develop specifications that define a set of

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	requirements for security and interoperability between chip cards and terminals on a global basis, regardless of the manufacturer, the financial institution, or where the card is used. Dua ’060 at [0290] For example, when a subway contactless stored value card is waved in front of a reader at the turnstile, the electronic balance is automatically debited from the onboard chip. The rules that govern the functioning of that stored value program and the card's interaction with an external RF reader, are all programmed into the onboard chip. Dua ’060 at [0293] These are just a few examples of the types of credentials that can be issued to and stored within the wallet application. Implementing electronic versions of these credentials in the wallet application creates different operating and processing requirements for each credential. Consider the requirements associated with implementing the subway stored value credential through the wallet platform. The logic required to operate the subway stored value credential, the unique message format for communication between the wireless device and a RF reader at the turnstile, unique display messages, an over-the-air reload tool, and other features associated with the stored value credential that a user might see on the wireless device—all need to be programmed into the wallet application. These types of requirements are embodied in mini-programs that operate within the wallet application called “extensions” since they “extend” the capability of the wallet application in order to handle new features and capabilities that are specific to an issuer's credential. These extensions allow credentials to be used in a controlled way through specific issuer-defined functions. Dua ’060 at [0315] In a local—or proximity—environment, the consumer is in the vicinity of a reader device that is connected to a point-of-sale (POS) terminal or some other type of computer system. Most day-to-day proximity transactions today use a card or token with information encoded in a variety of media types including magnetic stripe, bar code, chip, and embossed or printed data. A mobile device with a wallet application can serve as a replacement for single-purpose cards and tokens. During a proximity transaction, the wireless device can transmit payment, identification, or other confidential information to a reader using the short-range transmission capability of the wireless device (e.g. RF). For example, a wireless device loaded with a wallet application, that also has an integrated RFID chip can simply be waved slowly in close proximity to a reader device to facilitate a transaction. Similarly, a wireless device that uses infra-red to transact with a reader requires that the user point the infra-red beam to a reader device.

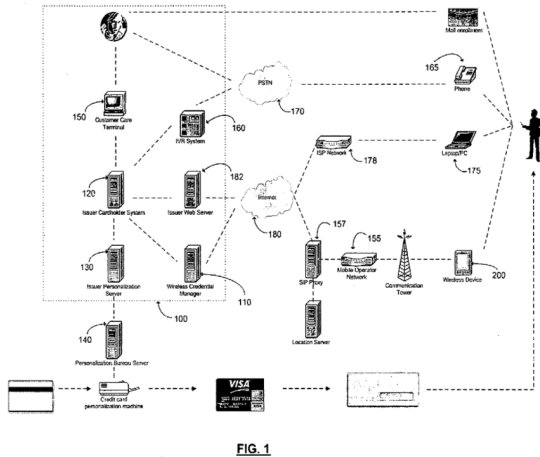
Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at [0317] In a personal environment, mobile transactions are conducted on the user interface of another device and augmented by security, connectivity, information, and other functionality provided by the user's wireless device. For example, during a transaction—a point-of-sale device may establish secure connectivity with the user's wireless device and poll it for a list of user-defined payment methods that the user can select from using the user-interface of the POS system. The implication is that the user's wireless device can act as a repository of information that can be securely accessed by another device during a transaction. Dua ’060 at [0336] Payment Methods—Credit, debit/ATM, stored value, electronic check, and RFID payment methods may be registered with the wallet application Dua ’060 at [0353] Several features of this invention serve to minimize the key strokes a user has to make in searching for, selecting, and transmitting a credential to a reader. One such feature of this invention is the use of a credential-specific “reader key”. The key is sent with an electronic credential record to a wireless device during the issuance process. The same reader key is programmed in all reader devices employed by an organization. In the case of an RFID reader, the key is transmitted from the reader to the wireless device's RFID chip during a proximity transaction. The receipt of the key by the RFID chip in the wireless device may initiate the automatic launch of the wallet application resident on the device, and the transfer of the key to the application. The key is subsequently received by the wallet application and is used as a search string by the application to locate a specific credential for transmission back to the reader via the device's RF capability. Dua ’060 at [0392] According to this embodiment, a user could use the “Wallet Settings” functionality in the wallet application to link his favorite/preferred credit card to button 1, and his favorite/preferred debit/ATM card to button 2. Button 3, labeled above as “QuickWave”, allows a user to transmit any PIN-less designated credential that has a “reader key” associated with it to a reader during a transaction. Dua ’060 at [0395] Pressing buttons 1 or 2, may prompt the user to input a PIN before RF communication can be enabled. As such, a user may be required to input a PIN and click “OK” to enable RF communication for a 30 second window. Alternatively, the user may be required to input his PIN, click “OK” to initiate PIN verification,

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	and upon positive confirmation be prompted to hold down either button 1 or 2 while placing the device in close proximity to a reader. The press/release or hold down scenarios would also apply to button 3. Dua ’060 at [0405] As can be seen in FIG. 8, a first transmission path of an electronic credit card authorization request 870 includes, for example, a merchant store controller and merchant host system, an acquirer/processor network, a private network such as VisaNet, and a issuer gateway. Using these components, point of sale terminal 860, via RF reader 820 can be used to capture and transmit an electronic credential from a wireless device for online authorization. The second transmission path as shown in FIG. 8 is via WCM 810 using the Internet and wireless link 880 and issuer DNS server 890 and is used to deliver a PIN request to wireless device 800 and to receive a user-input response from wireless device 800. Dua ’060 at [0417] Assume that a wireless user has an electronic Sample Bank MasterCard credit card stored in the wallet application that is setup for OTA PIN validation. The user selects the electronic card for use in a proximity transaction at a grocery store, and the credential information is transmitted to a reader via RF as described earlier. The POS at the grocery store will switch the transaction to its central host, which in turn will recognize that this is a MasterCard credit card and switch it to the MasterCard network (either directly or through an acquirer/processor depending on configuration). MasterCard in turn switches the authorization request to Sample Bank which is the card issuer. Sample Bank's gateway receives the authorization request, and passes the transaction to its card management system for approval. The card management system checks the account status using the normal validation process it follows for credit card authorizations. One of the novel aspects of the present invention is that Sample Bank has implemented a new credit card product with OTA PIN verification. As such, a flag in the credit card customer account record signals to the credit card management system that an authorization approval can not be sent back to the retailer POS until an Over-the-Air PIN verification is completed. Dua ’060 at [0433] Receipts from a merchant can be sent to the user's wallet application on the wireless device via several methods as discussed herein. Under one design, the user's E.164 phone number for the wireless device is transmitted to the merchant with the credential information during an RF transaction. The wallet application would have the ability to learn the E.164 phone number of the device on which it operates through the device's operating system, or directly from the SIM card which may contain certain device settings and attributes like the E.164 number. A phone number field would be specified in the credential transmission record that is transmitted from the wireless device to the POS reader (or to a server in the

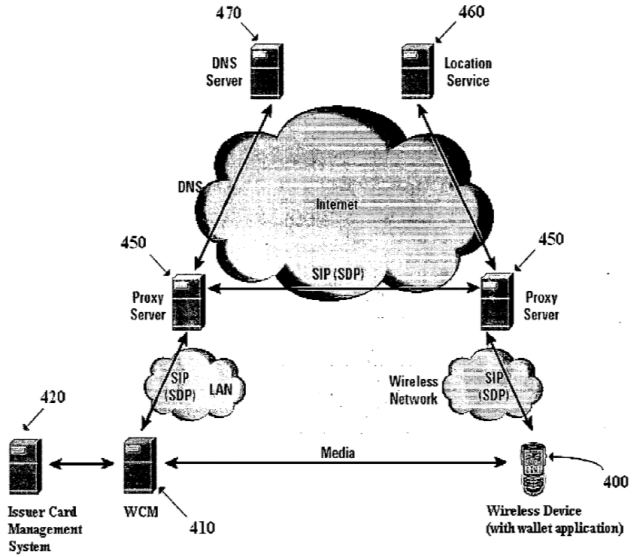
Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	case of a remote transaction). Under this embodiment, the merchant's system receives the E.164 phone number of the device that initiated the transaction. The merchant could use the number in conjunction with a WCM deployed at the merchant's site to issue digital receipts to the wallet application. The merchant would have a WCM setup to interface with its central transaction processing system. The retailer's transaction processing system would temporarily hold the E.164 number received with the credential during an authorization request that originated at the POS. Dua ’060 at claim 20 20. The method of claim 1 wherein said credential comprises a credit card account. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
6. The mobile phone of claim 1 wherein the driver comprises a current driver.	To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
7. The mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.	Dua ’060 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.” For example: Dua ’060 at Fig. 1

Claim Element

Exemplary Citations to US20060165060A1 (“Dua ’060”)



Dua ’060 at Fig. 3



Claim Element

Exemplary Citations to US20060165060A1 (“Dua ’060”)

Dua ’060 at Fig. 4

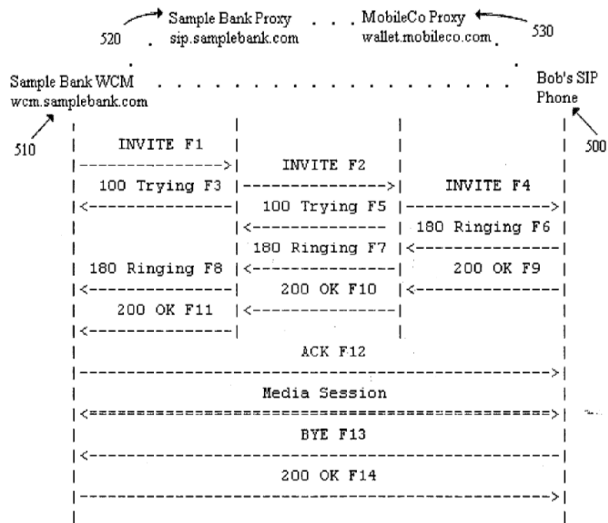


FIG. 4

Dua ’060 at Fig. 5

Claim Element

Exemplary Citations to US20060165060A1 (“Dua ’060”)

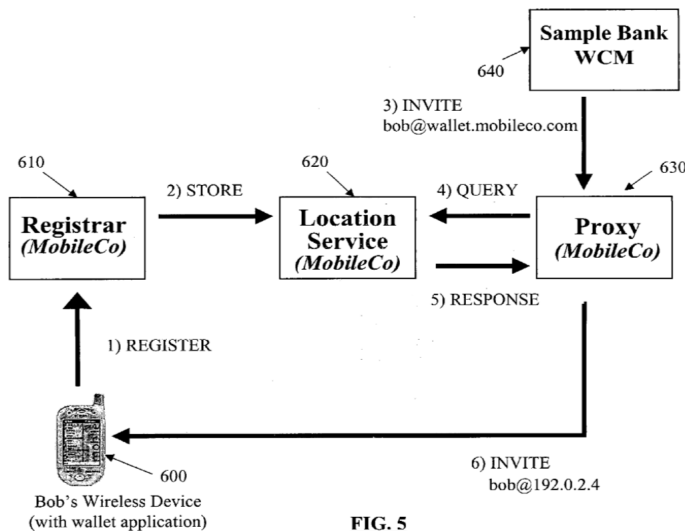


FIG. 5

Dua ’060 at Figure 8

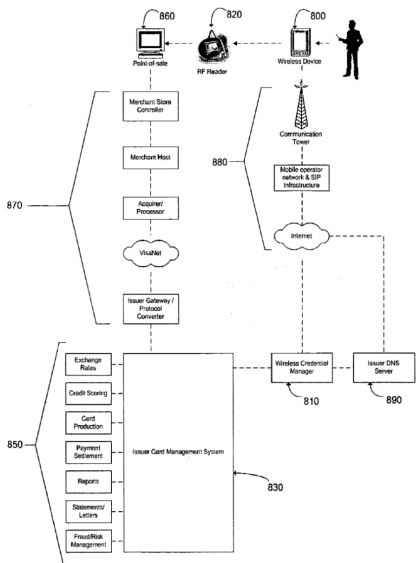


FIG. 8

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at [0016] Common short-range communications network standards defined by the International Electrical and Electronic Engineers association (IEEE) include 802.11a, 802.11b, and 802.11g. Many mobile devices employ these IEEE network standards to establish wireless LAN (WLAN) connectivity. Various other short-range technologies currently in use for device-to-device communication include Bluetooth and infra-red. One major short-range infra-red (IR) communications network protocol is defined by the Infra-red Device Association (IrDA), and is known as the IrDA standard. Wireless devices with integrated RFID proximity chips or Near Field Communication (NFC) technology may also provide users the ability to transfer information to a reader device. Dua ’060 at [0026] These and other objects of the present invention are obtained through the use of a novel system and methodology for conducting financial and other transactions requiring authorization. According to the methodology of the present invention, credentials may be selectively issued by issuers such as credit card companies, banks, and merchants to consumers permitting the specific consumer to conduct a transaction according to the authorization given as reflected by the credential or set of credentials. The preferred mechanism for controlling and distributing credentials according to the present invention is through one or more publicly accessible networks such as the Internet wherein the system design and operating characteristics are in conformance with the standards and other specific requirements of the chosen network or set of networks. According to a preferred embodiment of the invention, credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale (POS) terminal. Dua ’060 at [0040] In a preferred embodiment of the present invention, distribution of credentials is made via a transmission initiated by Issuer Cardholder System 120 to Wireless Credential Manager 110 which causes the credential or set of credentials to be transmitted to wireless device 200 via the Internet and/or one or more alternative public or private networks. Based upon the specific addressing schemes employed herein, the credential may then ultimately make its way to the targeted wireless device via an over-the-air wireless link. Dua ’060 at [0041]

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	As stated above, the present invention preferably involves the distribution of credentials to a “wireless device”. As used herein, wireless device 200 is preferably a device that is capable of wirelessly connecting to the Internet using network protocols such as GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH or other relevant protocols developed hereinafter. Preferably, wireless device 200 has a display screen and a key pad for alphanumeric and special character data input. It is further preferred that wireless device 200 has processing and secure storage capabilities allowing it to host and operate a wallet application capable of receiving, storing, managing and transmitting multiple payment, identification, and other confidential information electronically. Wireless device 200 also preferably has an integrated short-range communication capability for transmitting confidential information and exchanging other data between the wallet application and an external reader that is in proximity to the wireless device. Dua ’060 at [0043] Wireless Credential Manager (WCM) 110 maintains, controls and distributes credentials in accordance with the teachings herein. In a preferred embodiment, WCM 110 is able to interface with a payment, identification, and/or other existing user management or card management systems such as issuer cardholder system 120. An issuer representative may interface with issuer cardholder system 120 through the use of customer care terminal 150. The process for issuing a credential according to the present invention may be initiated manually by an issuer representative via terminal 150. Alternatively, the customer himself may initiate the process through interactive voice response (IVR) system 160 by calling in through wireline phone 165 via PSTN network 170. Dua ’060 at [0044] Other alternatives for initiating the process include the use of computer via the requesting party's ISP 178, the Internet 180 and through the issuer's web server 182 to issuer cardholder system 120. Still another alternative for initiating the credential issuing process is through wireless device 200 via mobile operator network 155, SIP proxy 157, Internet 180 and issuer's web server 182. The wireless device used to initiate the credential issuance process may be either the device to receive the credential or another wireless device. Dua ’060 at [0048] According to the teachings of the present invention, an E.164 phone number is used to target a user's wallet application on Internet-enabled wireless device 200 for the delivery of credentials and confidential data, including but not limited to credit card, debit card, ATM card, loyalty card, driver's license, electronic ticket, coupons and other information. In addition, an E.164 phone number is used according to

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	the present invention to target a user's wallet application residing on wireless device 200 for the remote cancellation or updating of credentials. Also, E.164 phone numbers may be used as described herein to make person-to-person, person-to-company, or company-to-company electronic payments or fund transfers using wireless device 200. Although a preferred embodiment, this invention is not necessarily limited to the use of E.164 phone numbers. Rather, the use of URIs and other address types that are capable of being translated to an Internet address is also possible for the purposes mentioned above. Dua ’060 at [0050] The use of ENUM presupposes the collection of these records into a central or hierarchical service. According to a preferred embodiment, the resolved Internet address is used to establish secure real-time communication between WCM 110 and the wallet application on wireless device 200 using the Session Initiation Protocol (SIP) (for example, according to the RFC 3261 standard) to transfer encrypted credentials. The issuer WCM 110 may also be used to update credentials or update the status of credentials on wireless device 200. WCM 110 may also be used to authenticate a mobile user's identity in real-time during a transaction. While the use of SIP for such purposes is preferred, alternative application protocols may be used in lieu of SIP while still remaining within the spirit and scope of the present invention. Dua ’060 at [0055] According to the present invention, electronic credentials may be issued to a wallet application on a wireless device 200 held (owned, rented or otherwise controlled) by a user that already has a physical card or token-based credential. For example, an existing bank customer that has a magnetic-stripe credit card may also request a digital card for use with the wallet application on his or her wireless device 200. The bank customer could request the new credential over the phone by first validating his or her identity with the issuer, by logging into the issuer's secure web site using a valid username and password, or in person at a branch. Dua ’060 at [0056] Credentials may alternatively be issued to a wireless device held by a user that is applying for a new credential for the first time. For example, a user may be applying for a credit card for the first time, and may wish to only request the credential on his or her mobile phone. According to the teachings of this invention, credential issuers may request from applicants (e.g. over the telephone) a properly formatted E.164 phone number in order to target the delivery of credential(s) to a wallet application on wireless device 200. The request for a E.164 wireless device number on an application for a credit card, debit card, ATM card, loyalty card, driver's license, security pass, coupons, certificates, or other credential type is

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	made by the issuer. The E.164 phone number may be obtained on paper, via a web-based application, via an electronic kiosk, via telephone or it may be captured through other means. Dua ’060 at [0102] SIP is based on an HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular method, or function, on the server and at least one response. SIP uses most of the header fields, encoding rules, and status codes of HTTP. This provides a readable text-based format for displaying information. SIP incorporates the use of Session Description Protocol (SDP), which defines session content using a set of types similar to those used in Multipurpose Internet Mail Extensions (MIME). Technically, SIP will function across both IPv4 and IPv6 networks. Dua ’060 at [0104] The present invention, in a preferred embodiment provides for using some of the SIP-network infrastructure that mobile operators will have in place to deliver credentials from SIP-based Wireless Credential Manager (WCM) 110 at an issuer site to a SIP-based wallet application on a wireless device 200. The system disclosed herein is designed to interoperate with mobile 2.5G, 3G, and Wi-Fi networks among others. Dua ’060 at [0108] The proxy servers 450 may also act as redirect servers as needed. If redirection is done, the proxy server 450 needs to consult the location service database 460, which may or may not be colocated with the proxy server 450. The Domain Name System (DNS) 470 is also an important part of SIP operation. Typically, a user agent client (UAC) makes a request using the domain name of the user agent server (UAS), rather than an IP address. Proxy server 450 thus needs to consult DNS server 470 to find a proxy server 450 for the target domain. Dua ’060 at [0128] FIG. 4 shows a typical example of a SIP message exchange between a credential issuer (named herein Sample Bank) and a fictitious mobile user named Bob. (Each message is labeled with the letter “F” and a number for reference by the text.) In this example, SIP signaling functionality embedded in the Wireless Credential Manager (WCM) 510 is used to issue Bob a Sample Bank MasterCard on his SIP-enabled mobile device 500 via the Internet. Also shown are two SIP proxy servers that act on behalf of Sample Bank and Bob's mobile operator (MobileCo) to facilitate session establishment. This typical arrangement is often referred to as the “SIP trapezoid” as shown by the geometric shape of the dotted lines in FIG. 4.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at [0129] WCM 510 may initiate communication with a wallet application on Bob's wireless device 500 through a SIP proxy server on MobileCo's network that also handles voice, instant messaging, and other services. Dua ’060 at [0155] Since WCM 510 does not know the location of Bob or the SIP server in the mobileco.com domain, WCM 510 sends the INVITE to the SIP server that serves Sample Bank's domain, samplebank.com. The address of the Sample Bank SIP server (sip.samplebank.com) could have been configured in WCM 510, or it could have been discovered by DHCP, for example. It should be noted that for illustrative purposes the SIP proxy functionality was shown as a being a separate server from WCM 510; in reality the proxy functionality is a part of WCM 510. The proxy component of WCM 510 is an important aspect of this system and the overall methodology. Dua ’060 at [0323] In a remote—or online—environment, transactions are conducted with a remote server over a wireless network. For example, a remote transaction using a wireless device can be conducted over the Internet with a browser on the wireless device. In such transactions, the wireless device's user interface (UI) is of paramount importance. The UI must relay all relevant information to maintain the user's trust and ensure usability of the services. Remote transactions range from online purchases and banking to more impulsive activities like downloading digital content. Dua ’060 at [0422] Under another embodiment of this invention, the dual network processing path utilized for transactions involving OTA PIN verification as described above, could be used to prompt a user for certain preference information on his wireless device 800 during a transaction. For example, Sample Bank may create an innovative payment product (herein called the “Wallet Account”) that links together multiple payment accounts such as a credit account, a debit account, and a stored value account under a single account number. The Wallet Account number could utilize a Visa, MasterCard, American Express, Discover, Diners, or other network/association Bank Identification Number (BIN) range that allows Wallet Account transactions to be authorized by a retailer's POS systems the way credit/debit card transactions are 870. When a Wallet Account transaction reaches Sample Bank's Card Management System 830 for authorization, Sample Bank's system 830 will discern that the account number corresponds to a valid Wallet Account which has a credit, debit, and stored value account linked. Using the user's E.164 number stored in Sample Bank's Card Management System 830, the Card Management System will send a

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	message to the user's wireless device 800 to request a PIN (as described earlier) and to ask the user to specify his choice of using one of the linked credit, debit, or stored value accounts for completing the transaction. This request for payment preference traverses the same network path as the OTA PIN verification request described earlier, and traverses the Internet and mobile operator network 880. Based on the user's payment preference input into wireless device 800, Sample Bank's Card Management System 830 can authorize and apply the transaction to the appropriate account. This example illustrates that requests for user preferences or other information during a transaction can traverse a completely different network path (comprised of one or more networks) than the original online authorization via one network path (comprised of one or more networks). Also illustrated is the fact that OTA PIN requests can be coupled with requests for user preferences or other information. Dua ’060 at claim 1 (b) accepting a routable address associated with said request, said routable address being routable over a data network; Dua ’060 at claim 49 (d) means for issuing said credential to said wireless device through a transmission path comprising a data network and a wireless link. Dua ’060 at claim 53 53. The system of claim 50 wherein said non-wireless portion of said network is a private data network Dua ’060 at claim 89 89. The system of claim 50 further comprising an RF reader and an issuer account management system, wherein said wireless device operates to transmit credential information to said RF reader and said RF reader transmits said credential information to said issuer account management system through a first network path and, in response to said transmission, a PIN request is transmitted by said issuer account management system to said wireless device through a second network path. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
8. The mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.	Dua ’060 discloses or renders obvious “[t]he mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.” For example: Dua ’060 at [0026] These and other objects of the present invention are obtained through the use of a novel system and methodology for conducting financial and other transactions requiring authorization. According to the methodology of the present invention, credentials may be selectively issued by issuers such as credit card companies, banks, and merchants to consumers permitting the specific consumer to conduct a transaction according to the authorization given as reflected by the credential or set of credentials. The preferred mechanism for controlling and distributing credentials according to the present invention is through one or more publicly accessible networks such as the Internet wherein the system design and operating characteristics are in conformance with the standards and other specific requirements of the chosen network or set of networks. According to a preferred embodiment of the invention, credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network. The user holding the credential may then use the handheld device to conduct the authorized transaction or set of transactions via, for example, a short range wireless link with a point-of-sale (POS) terminal. Dua ’060 at [0046] WCM 110 provides for the secure Internet delivery of electronic credentials to wireless device 200 which is loaded with a wallet application. WCM 110 provides a secure and robust means of issuing, canceling, and managing electronic credentials on wireless devices via the Internet. WCM 110 leverages existing Internet protocols and technologies, making it easy for issuers to integrate with their existing systems, and alleviating the need to establish direct links with multiple mobile operators. Dua ’060 at [0048] According to the teachings of the present invention, an E.164 phone number is used to target a user's wallet application on Internet-enabled wireless device 200 for the delivery of credentials and confidential data, including but not limited to credit card, debit card, ATM card, loyalty card, driver's license, electronic ticket, coupons and other information. In addition, an E.164 phone number is used according to the present invention to target a user's wallet application residing on wireless device 200 for the remote cancellation or updating of credentials. Also, E.164 phone numbers may be used as described herein to make person-to-person, person-to-company, or company-to-company electronic payments or fund transfers using wireless device 200. Although a preferred embodiment, this invention is not necessarily

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	limited to the use of E.164 phone numbers. Rather, the use of URIs and other address types that are capable of being translated to an Internet address is also possible for the purposes mentioned above. Dua ’060 at [0050] The use of ENUM presupposes the collection of these records into a central or hierarchical service. According to a preferred embodiment, the resolved Internet address is used to establish secure real-time communication between WCM 110 and the wallet application on wireless device 200 using the Session Initiation Protocol (SIP) (for example, according to the RFC 3261 standard) to transfer encrypted credentials. The issuer WCM 110 may also be used to update credentials or update the status of credentials on wireless device 200. WCM 110 may also be used to authenticate a mobile user's identity in real-time during a transaction. While the use of SIP for such purposes is preferred, alternative application protocols may be used in lieu of SIP while still remaining within the spirit and scope of the present invention. Dua ’060 at [0053] In order to take advantage of ENUM, the mobile telephone number must first be assigned to a user by a telecom operator for services. The number can then be registered for one or more ENUM services. For example, a subscriber might wish to install a wallet application on wireless device 200 and register the telephone number as the identifier for the wallet application. Multiple issuers can in turn deliver payment methods, identification, or other types of electronic credentials to the wallet application on the wireless device 200 via the Internet using the phone number as the destination address. Additionally, that subscriber might wish to register an e-mail address or fax number to be associated with the same phone number. However the user chooses to set up these services, the information for the registered services, including the wallet application, is saved in NAPTR (Naming Authority Pointer) Resource Records. Dua ’060 at [0055] According to the present invention, electronic credentials may be issued to a wallet application on a wireless device 200 held (owned, rented or otherwise controlled) by a user that already has a physical card or token-based credential. For example, an existing bank customer that has a magnetic-stripe credit card may also request a digital card for use with the wallet application on his or her wireless device 200. The bank customer could request the new credential over the phone by first validating his or her identity with the issuer, by logging into the issuer's secure web site using a valid username and password, or in person at a branch. Dua ’060 at [0056]

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Credentials may alternatively be issued to a wireless device held by a user that is applying for a new credential for the first time. For example, a user may be applying for a credit card for the first time, and may wish to only request the credential on his or her mobile phone. According to the teachings of this invention, credential issuers may request from applicants (e.g. over the telephone) a properly formatted E.164 phone number in order to target the delivery of credential(s) to a wallet application on wireless device 200. The request for a E.164 wireless device number on an application for a credit card, debit card, ATM card, loyalty card, driver's license, security pass, coupons, certificates, or other credential type is made by the issuer. The E.164 phone number may be obtained on paper, via a web-based application, via an electronic kiosk, via telephone or it may be captured through other means. Dua ’060 at [0057] Turning now to FIG. 2, an overview of the credential issuance process of the present invention, in a preferred embodiment thereof, is now described. The credential issuance process begins with WCM 110 receiving a request from the issuer's card or user management system 120 to issue electronic credentials to an individual user (see step 310). The request is forwarded to WCM 110 along with the user's mobile (E.164) number, the credentials to be issued, encryption keys, and other information contained in the Personalization File for the specific request. The Personalization File may be a batch file that contains numerous records of credentials that are to be issued to individuals on their wireless device 200, or could be a separate file record for each credential to be issued. In another embodiment, the Personalization File is transmitted to WCM 110 by issuer personalization server 130 which is in communication with issuer cardholder system 120. Issuer personalization server communicates with personalization bureau server 140 which is typically maintained by the personalization bureau. Dua ’060 at [0059] In the case where a user already has one or more credentials from the issuer, such as a magnetic-stripe credit card, and wishes to supplement the card with a digital version of the credential on his or her wireless device 200, the issuer can provide the user with a digital credential linked to the same magnetic-stripe account, but that bears a different account number. Dua ’060 at [0060] The full account number of the electronic credential issued to wireless device 200 may not be visible to the user through the wallet application (discussed later), since the credential may have been issued for “device present” transactions only as may be the case with certain credit cards that are issued. Account numbers and other information could also be partially masked for security reasons with other credential types. In all such cases, the issuer may specify in the security characteristics such as the visibility of

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	account numbers or other information in the Personalization File. For example, the issuer may specify that the wallet application should only make the last four digits of the account number visible to the user on wireless device 200. Dua ’060 at [0179] The media session between the Sample Bank WCM 510 and the wallet application on Bob's SIP enabled mobile phone 500 has now begun, and they can send data packets using the format to which they agreed in the exchange of SDP. In general, the end-to-end data packets take a different path from the SIP signaling messages. Dua ’060 at [0295] A wireless device loaded with the wallet application may come with some pre-loaded extensions. Extensions may reside on the device memory, in an embedded smart card, in a removable storage media, or on a remote server, securely accessible through the wallet application protocols. An extension may communicate with the user, may exchange information with remote servers or it may use other elements of the device hardware or software. Dua ’060 at [0297] The actual account information or personal information that is transmitted by the issuer to the wallet application is referred to as the “credential”. The actual credential record that is transmitted to the wallet application by the issuer may contain some of the following information: Dua ’060 at [0319] One advantage of establishing peer-to-peer connectivity with a POS terminal is that it allows for a bi-directional exchange of data where a user may be prompted on his wireless device for various types of preferences, questions, or other data input in sequence. Transactions where there is a stream of data that goes in both directions can benefit from this type of peer-to-peer session using any number of protocols. Dua ’060 at [0347] If a credential is received by the wallet application containing a primary and/or secondary category that does not yet exist in the credential tree, the wallet application will add the primary and/or secondary category automatically before linking the credential to it. Dua ’060 at [0408]

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	After the issuer's card management system 830 has validated that the account is in good status and is qualified for “approval”, a PIN request is generated by the system and sent to WCM 810 via a real-time interface along with information relating to the transaction and certain account information. (If the account is not in good status or does not qualify for an “approval”, a denial message would be sent through the network(s) to the origination point.) The PIN request message sent to WCM 810 should include fields such as the name of the organization that originated the authorization request, location ID from where the request originated (e.g. a store address), date/time of authorization request, transaction amount being authorized (or purpose of transaction if a non-financial transaction), transaction ID, last four digits of account number, credential type (e.g. Visa Credit Card), issuer name, and the E.164 mobile phone number retrieved from the credential holder's account (in Application Unique String format as defined earlier). There must be a valid E.164 mobile phone number in the account record in order to enable OTA PIN verification with a credential. Dua ’060 at [0453] During the setup process of the wallet application, a mobile operator will issue a unique “mobile operator key” to each wallet application device. The key is stored in the wallet application, and is used by the operator to reset the wallet application remotely in the event that the device is lost/stolen, and to manage other wallet settings like (SIP proxy server addresses, DNS server addresses, etc). Dua ’060 at [0494] Credentials will be issued to the wireless device in the manner previously described in this document with only a slight modification to where the credentials actually get stored. When an issuer's WCM opens a peer-to-peer SIP connection with the wallet application on the wireless device, the wallet application will have an open connection maintained to the secure storage service. Any credentials that are issued to the wireless device will be transparently transmitted to the storage service where they will reside. The connection between the wallet application and the storage service could utilize an application protocol such as HTTP, SIP, or others. Any data transmitted to the storage service will be registered with the wallet application first; the registration of credentials, personal information, and other confidential data within the wallet application allows the wallet application to display headers for information in storage without having to retrieve it online; the registration process also allows the wallet application to call specific data from storage based on the assigned registration ID for the data object in storage. Dua ’060 at claim 50 50. A system for transmitting a credential from an issuer to a wireless device comprising:

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	Dua ’060 at claim 75 75. The system of claim 50 wherein said issued credential comprises a credential record including at least one account number associated with said issued credential. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
9. The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.	Dua ’060 discloses or renders obvious “[t]he mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.” For example: Dua ’060 at [0056] Credentials may alternatively be issued to a wireless device held by a user that is applying for a new credential for the first time. For example, a user may be applying for a credit card for the first time, and may wish to only request the credential on his or her mobile phone. According to the teachings of this invention, credential issuers may request from applicants (e.g. over the telephone) a properly formatted E.164 phone number in order to target the delivery of credential(s) to a wallet application on wireless device 200. The request for a E.164 wireless device number on an application for a credit card, debit card, ATM card, loyalty card, driver's license, security pass, coupons, certificates, or other credential type is made by the issuer. The E.164 phone number may be obtained on paper, via a web-based application, via an electronic kiosk, via telephone or it may be captured through other means. Dua ’060 at [0057] Turning now to FIG. 2, an overview of the credential issuance process of the present invention, in a preferred embodiment thereof, is now described. The credential issuance process begins with WCM 110 receiving a request from the issuer's card or user management system 120 to issue electronic credentials to an individual user (see step 310). The request is forwarded to WCM 110 along with the user's mobile (E.164) number, the credentials to be issued, encryption keys, and other information contained in the Personalization File for the specific request. The Personalization File may be a batch file that contains numerous records of credentials that are to be issued to individuals on their wireless device 200, or could be a separate file record for each credential to be issued. In another embodiment, the Personalization File is transmitted to WCM 110 by issuer personalization server 130 which is in communication with issuer

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	cardholder system 120. Issuer personalization server communicates with personalization bureau server 140 which is typically maintained by the personalization bureau. Dua ’060 at [0059] In the case where a user already has one or more credentials from the issuer, such as a magnetic-stripe credit card, and wishes to supplement the card with a digital version of the credential on his or her wireless device 200, the issuer can provide the user with a digital credential linked to the same magnetic-stripe account, but that bears a different account number. Dua ’060 at [0060] The full account number of the electronic credential issued to wireless device 200 may not be visible to the user through the wallet application (discussed later), since the credential may have been issued for “device present” transactions only as may be the case with certain credit cards that are issued. Account numbers and other information could also be partially masked for security reasons with other credential types. In all such cases, the issuer may specify in the security characteristics such as the visibility of account numbers or other information in the Personalization File. For example, the issuer may specify that the wallet application should only make the last four digits of the account number visible to the user on wireless device 200. Dua ’060 at [0297] The actual account information or personal information that is transmitted by the issuer to the wallet application is referred to as the “credential”. The actual credential record that is transmitted to the wallet application by the issuer may contain some of the following information: Dua ’060 at [0408] After the issuer's card management system 830 has validated that the account is in good status and is qualified for “approval”, a PIN request is generated by the system and sent to WCM 810 via a real-time interface along with information relating to the transaction and certain account information. (If the account is not in good status or does not qualify for an “approval”, a denial message would be sent through the network(s) to the origination point.) The PIN request message sent to WCM 810 should include fields such as the name of the organization that originated the authorization request, location ID from where the request originated (e.g. a store address), date/time of authorization request, transaction amount being authorized (or purpose of transaction if a non-financial transaction), transaction ID, last four digits of account number, credential type (e.g. Visa Credit Card), issuer name, and the E.164 mobile phone number retrieved from the credential holder's account (in Application Unique String format as

Claim Element	Exemplary Citations to US20060165060A1 (“Dua ’060”)
	defined earlier). There must be a valid E.164 mobile phone number in the account record in order to enable OTA PIN verification with a credential. Dua ’060 at claim 75 75. The system of claim 50 wherein said issued credential comprises a credential record including at least one account number associated with said issued credential. To the extent this limitation is not disclosed by Dua ’060, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Dua ’060, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.

DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 11,270,174

EXHIBIT G4: US5943624A ("Fox '624")

As demonstrated in the claim charts below, the claims of U.S. Patent No. 11,270,174 ("the '174 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Fox '624 and (b) under 35 U.S.C. § 103(a) as obvious over Fox '624 standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, Applicant's Admitted Prior Art, and/or the additional prior art references discussed in Exhibit G and Exhibits G1–G5, 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 '174 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 '174 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's application of the claims at issue in this case, and these charts should not be interpreted as an admission or concession by Defendants that any particular construction or application of any claim limitation by Plaintiff is correct or proper. Additionally, these charts provide representative examples of portions of the charted references that disclose the indicated limitations of the claims; additional portions of these references other than the representative examples provided herein may also disclose the indicated limitation(s) and Defendants contend that the asserted claims are invalid in light of the charted reference(s) as a whole in its or their entirety. Where a particular figure is cited, the citation should be understood to encompass the caption and description of the figure as well as any text relating to or describing the figure. Conversely, where particular text referring to a figure is cited, the citation should be understood to include the figure as well.

Claim Element	Exemplary Citations to US5943624A ("Fox '624")
1[pre]. A mobile phone comprising:	By providing this disclosure, Defendants do not take a position on whether the preamble is a claim limitation. Fox '624 discloses or renders obvious "[a] mobile phone." For example: Fox '624 at Abstract A cellular telephone (10) incorporates the electronics for implementing both a cellular telephone function (46) and a smartcard function (45). This allows the electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone 10 also includes an RF interface (40) for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox '624 at Fig. 1

Claim Element

Exemplary Citations to US5943624A ("Fox '624")

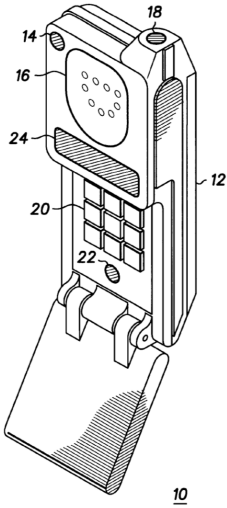


FIG. 1

Fox '624 at Fig. 2

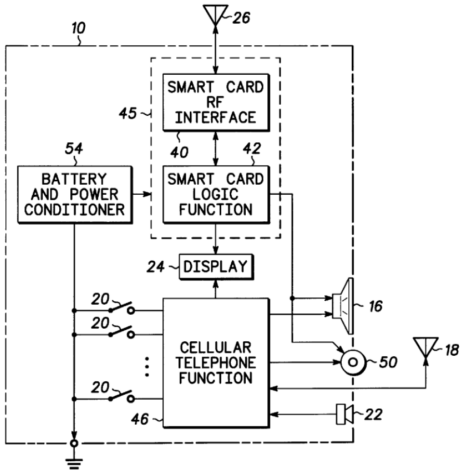


FIG. 2

Claim Element

Exemplary Citations to US5943624A ("Fox '624")

Fox '624 at Fig. 4

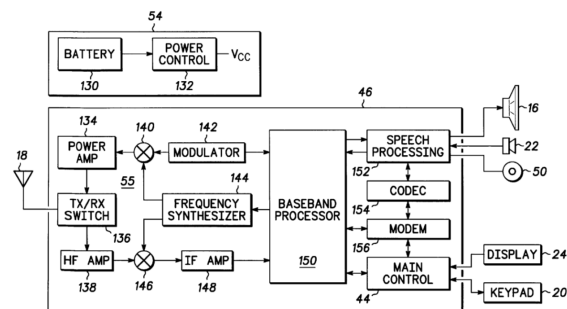


FIG. 4

Fox '624 at Fig. 5

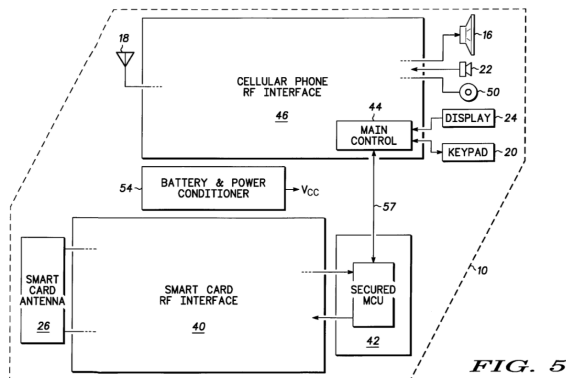


FIG. 5

Fox '624 at 1:5–8

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

Fox '624 at 1:60–61

FIG. 1 is a pictorial diagram illustrating a cellular telephone for incorporating a smartcard function therein;

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

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

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

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

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

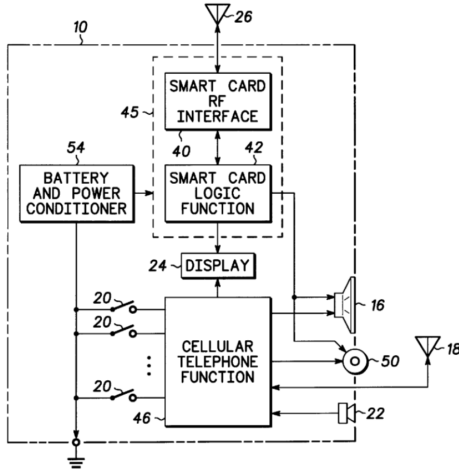
Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox ’624 at 7:1–6 ncorporating said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

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. Fox ’624 at 8:34–37 13. The cellular telephone of claim 10 wherein said smartcard circuitry, said RF interface, and said cellular telephone circuitry are fabricated on a single semiconductor chip as an integrated circuit. Fox ’624 at 8:38–41 14. The cellular telephone of claim 10 wherein said cellular telephone circuitry, said smartcard circuitry, and said RF interface are included within a housing of the cellular telephone. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] a memory to hold transaction data for use in a plurality of transactions;	Fox ’624 discloses or renders obvious “a memory to hold transaction data for use in a plurality of transactions.” For example: Fox ’624 at Fig. 3 45 FIG. 3 Fox ’624 at 1:5–8 This invention relates to smartcard electronic devices and, more particularly, to the incorporation of smartcard devices in a cellular telephone for enhanced verification, security and accessibility to data stored on the smartcard.

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Fox ’624 at 1:9–30 Smartcards are fast becoming the common media to transfer information of many types relative to banking, transportation, subscriber, health, identification, etc. Typically, smartcards are housed within a plastic card, taking the form and size, for example, of a plastic credit card. Such smartcards include a microcomputer having some form of memory for storing and processing data. When a transaction within the capability of the smartcard is to be performed, the smartcard interacts with an external system which may be, for example, an automated teller machine, a merchant's point of sale system, etc. In performing such a transaction, typically the smartcard is inserted into a card reader associated with the external system through which electrical contact is made between the card reader and the smartcard. However, such systems requiring the smartcard to come into contact with the external system suffer from the disadvantages that the smartcard must be physically inserted into the external reader, the contacts between the smartcard and the external reader must be aligned for proper signal transfer, and the contacts may become worn or dirty thereby causing unreliability through signal degradation or signal interruption. Fox ’624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox ’624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM) 45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data

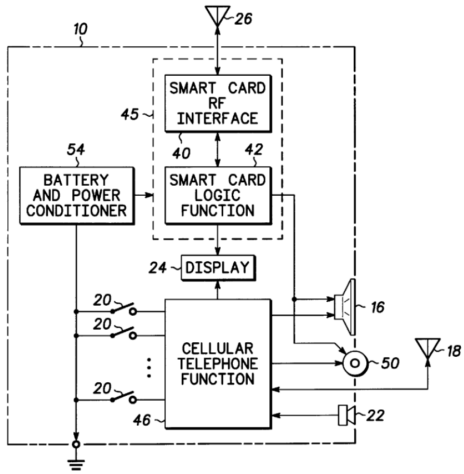
Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox ’624 at 4:43–56 Referring to FIG. 5, a detailed block diagram illustrating the electronic circuitry of cellular telephone circuitry 46 of FIG. 4 and smartcard circuitry 42 of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. It is understood that components shown in FIG. 5 that are identical to components shown in FIGS. 3 and 4 are identified by the same reference numbers. Signal line 57, which couples main control 44 of cellular telephone circuitry 46 to smartcard circuitry 42, provides a means for MPU 41 to communicate with main control (MPU) 44 for performing both cellular telephone and smartcard functions. Alternately, the functions of main control 44 and MPU 41 of smartcard logic function 42 may be combined into one single MPU. Fox ’624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox ’624 at 5:27–34 Smartcard data may also be accessed and displayed on display 24 through the use of selector buttons 20. For example, the balance of a smartcard may be displayed on display 24. Additionally, a menu system enabling the display of different data types, for example, medical information or multiple account balances or transaction lists, could also be provided on display 24 and of which could be accessed via selector buttons 20. Fox ’624 at 5:35–46 Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox ’624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox ’624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account. Fox ’624 at 7:1–6 ncorporating said integrated circuit into the housing of the cellular telephone so that said integrated circuit is coupled to the display and to the user accessible selector buttons to provide an interface between the user and both said smartcard circuitry and said cellular telephone circuitry; Fox ’624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox ’624 at 8:16–19 wherein said smartcard circuitry includes means for utilizing said cellular telephone circuitry to update information associated with said smartcard functions that is stored in said cellular telephone; Fox ’624 at 8:20–27

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1b] a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;	Fox ’624 discloses or renders obvious “a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions.” For example: Fox ’624 at Fig. 2  FIG. 2 Fox ’624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox ’624 at 2:53–59 Cellular telephone 10 of FIG. 2 includes smartcard radio-frequency (RF) interface 40 coupled to antenna 26 for transmission and reception of RF data. The transmission/reception of RF data is utilized for performing and executing various smartcard functions while not suffering from the problems described earlier with respect to smartcard contact interfaces. Fox ’624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM) 45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox ’624 at 3:49–59 Smartcard antenna 26 may take the form, for example, of capacitor 103 and a wire such as inductor 101. These two components form a tuned circuit that is resonant at the desired frequency of information and/or power transmission into the smartcard. The resonance is modified by the capacitor 104 and FET switch 105 under control of the logic function 42 via the answer back circuit 118 and transmitter driver 114, when information is transmitted out of the smartcard. The answer back circuit 118 receives the digital message from 42, formats and encodes it for RF transmission. Fox ’624 at 4:9–13

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Cellular telephone circuitry 46 includes RF interface comprising a transmit/receive switch 136 to direct energy in RF interface 55 for receipt of calls via the antenna 18, or to direct energy out of RF interface 55 when transmitting from the phone. Fox ’624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox ’624 at 5:27–34 Smartcard data may also be accessed and displayed on display 24 through the use of selector buttons 20. For example, the balance of a smartcard may be displayed on display 24. Additionally, a menu system enabling the display of different data types, for example, medical information or multiple account balances or transaction lists, could also provided on display 24 and of which could be accessed via selector buttons 20. Fox ’624 at 6:41–44 4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox ’624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
[1c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;	Fox ’624 discloses or renders obvious “a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network.” For example: Fox ’624 at Abstract A cellular telephone (10) incorporates the electronics for implementing both a cellular telephone function (46) and a smartcard function (45). This allows the electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone 10 also includes an RF interface (40) for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox ’624 at Fig. 2  FIG. 2 Fox ’624 at Fig. 5

Claim Element

Exemplary Citations to US5943624A ("Fox '624")

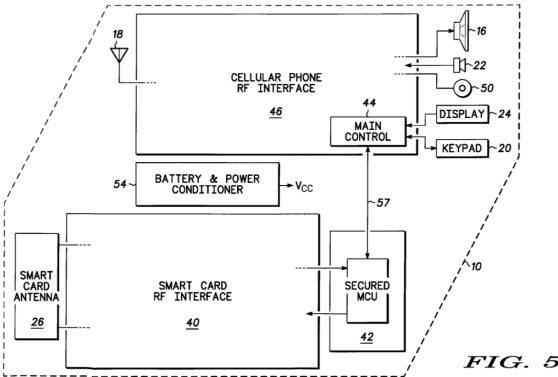


FIG. 5

Fox '624 at 1:62–64

FIG. 2 is a detailed block diagram illustrating the electronics for incorporating both a smartcard function and a cellular telephone function;

Fox '624 at 2:3–7

FIG. 5 is a detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 4 and the smartcard circuitry of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions.

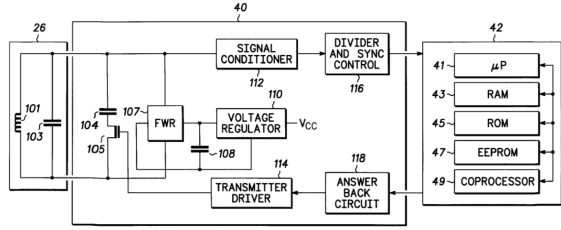
Fox '624 at 2:10–29

Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system.

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Fox ’624 at 2:30–37 Cellular telephone 10 includes casing 12 for housing the electronics for implementing both a smartcard function and a cellular telephone function as will be described and shown in more detail with respect to FIG. 2. Cellular telephone 10 includes on-off switch 14, speaker 16 and cellular telephone antenna 18. Additionally, cellular telephone 10 includes selector buttons 20, voice input/microphone 22 and display 24. Fox ’624 at 2:43–52 Referring to FIG. 2, a detailed block diagram illustrating the electronics associated with cellular telephone 10. As mentioned earlier, cellular telephone 10 includes the electronic circuitry for performing both a cellular telephone function and a contactless smartcard function whereby the human interface that selects the cellular telephone and the smartcard functions is accessed through the selector buttons 20 that are on the exterior of the cellular telephone housing case 12, as shown in FIG. 1 and represented electronically as switches in FIG. 2. Fox ’624 at 2:64–3:2 Cellular telephone 10 also includes cellular telephone function circuitry 46 (or simply cellular telephone circuitry) for performing the necessary functions of operating a cellular telephone. Telephone circuitry 46 may take the form of any electronics for performing a cellular telephone function, whereby one embodiment is shown in detail in FIG. 4. Fox ’624 at 3:27–34 The present invention provides a cellular telephone that incorporates the electronic circuitry for implementing both a cellular telephone function and a smartcard function functions via smartcard circuitry 42 and cellular telephone circuitry 46, respectively. This allows the smartcard electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. Fox ’624 at 5:35–46 Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox ’624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox ’624 at 6:4–5 cellular telephone circuitry, including a main controller, for performing cellular telephone functions; Fox ’624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account. Fox ’624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox ’624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox ’624 at 7:36–41

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	cellular telephone circuitry for performing cellular telephone functions, said cellular telephone functions including establishing a communications connection between the cellular telephone and a remote communications entity via an external cellular communications system; Fox ’624 at 8:16–19 wherein said smartcard circuitry includes means for utilizing said cellular telephone circuitry to update information associated with said smartcard functions that is stored in said cellular telephone; Fox ’624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1d] a driver to excite the current carrying conductor; and	Fox ’624 discloses or renders obvious “a driver to excite the current carrying conductor.” For example: Fox ’624 at Fig. 2

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Fox ’624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM) 45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox ’624 at 3:49–59 Smartcard antenna 26 may take the form, for example, of capacitor 103 and a wire such as inductor 101. These two components form a tuned circuit that is resonant at the desired frequency of information and/or power transmission into the smartcard. The resonance is modified by the capacitor 104 and FET switch 105 under control of the logic function 42 via the answer back circuit 118 and transmitter driver 114, when information is transmitted out of the smartcard. The answer back circuit 118 receives the digital message from 42, formats and encodes it for RF transmission. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1e] a processor coupled to control the driver.	Fox ’624 discloses or renders obvious “a processor coupled to control the driver.” For example: Fox ’624 at Fig. 3  45 FIG. 3

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Fox ’624 at 3:49–59 Smartcard antenna 26 may take the form, for example, of capacitor 103 and a wire such as inductor 101. These two components form a tuned circuit that is resonant at the desired frequency of information and/or power transmission into the smartcard. The resonance is modified by the capacitor 104 and FET switch 105 under control of the logic function 42 via the answer back circuit 118 and transmitter driver 114, when information is transmitted out of the smartcard. The answer back circuit 118 receives the digital message from 42, formats and encodes it for RF transmission. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
2. The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	Fox ’624 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.” For example: Fox ’624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox ’624 at 5:13–25 When a user desires to initiate a smartcard function with a corresponding RF reader, the user may, for example, cause cellular telephone 10 to come into the RF power range associated with RF interface 40 so that communication between the reader and cellular telephone 10 may be facilitated. At that point, some initial handshaking may be performed and the reader may then prompt the user to enter a PIN, via selector buttons 20, to ensure that the proper person is in possession of cellular telephone 10. From there, a specific transaction within the capability of smartcard logic function 42 may be executed, for example, a point-of-sale transaction, via a merchant's reader, or the transfer of funds, via an automated teller machine (ATM). Fox ’624 at 6:41–44

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	4. The cellular telephone according to claim 1 wherein said RF interface utilizes a cellular telephone antenna for transmitting and receiving information associated with said smartcard functions. Fox ’624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
3. The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	Fox ’624 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.” For example: Fox ’624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
4. The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Fox ’624 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.” For example: Fox ’624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26

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

Claim Element

Exemplary Citations to US5943624A ("Fox '624")

Fox '624 at Fig. 2

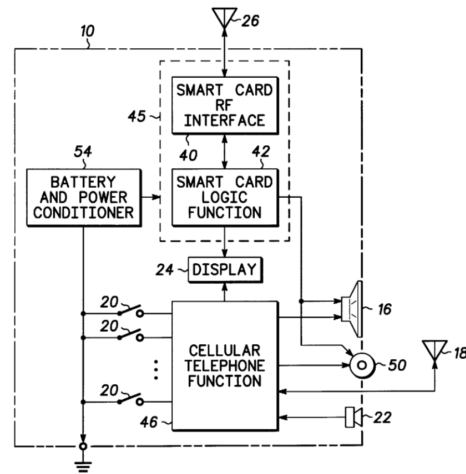


FIG. 2

Fox '624 at Fig. 3

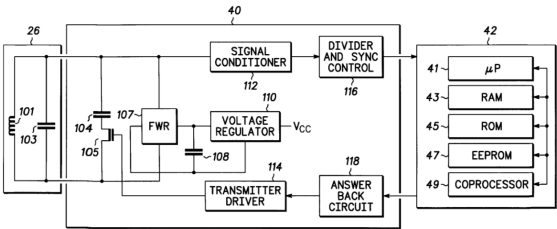


FIG. 3

Fox '624 at 2:53–59

Cellular telephone 10 of FIG. 2 includes smartcard radio-frequency (RF) interface 40 coupled to antenna 26 for transmission and reception of RF data. The transmission/reception of RF data is utilized for performing and executing various smartcard functions while not suffering from the problems described earlier with respect to smartcard contact interfaces.

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Fox ’624 at 3:35–48 Referring now to FIG. 3, a more detailed block diagram is shown illustrating the electronic circuitry of antenna 26, smartcard RF interface 40 and smartcard circuitry 42. Smartcard circuitry 42 includes microprocessor unit (MPU) 41, random access memory (RAM) 43, read-only memory (ROM) 45 and electrically erasable read-only memory (EEPROM) 47, and coprocessor 200 for accomplishing various smartcard functions wherein MPU 41 executes instruction stored on ROM 45 and temporarily stores data on RAM 43 and wherein EEPROM 47 is a non-volatile memory which may be used for storing data identifying the uniqueness of smartcard 45. And wherein coprocessor 49 executes security algorithms used to verify the identity of the smartcard and the smartcard infrastructure. Fox ’624 at 3:49–59 Smartcard antenna 26 may take the form, for example, of capacitor 103 and a wire such as inductor 101. These two components form a tuned circuit that is resonant at the desired frequency of information and/or power transmission into the smartcard. The resonance is modified by the capacitor 104 and FET switch 105 under control of the logic function 42 via the answer back circuit 118 and transmitter driver 114, when information is transmitted out of the smartcard. The answer back circuit 118 receives the digital message from 42, formats and encodes it for RF transmission. <i>See also</i> [1d]. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
7. The mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.	Fox ’624 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.” For example: Fox ’624 at Abstract A cellular telephone (10) incorporates the electronics for implementing both a cellular telephone function (46) and a smartcard function (45). This allows the electronics to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone 10 also includes an RF interface (40) for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function,

Claim Element

Exemplary Citations to US5943624A ("Fox '624")

information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure.

Fox '624 at Fig. 2

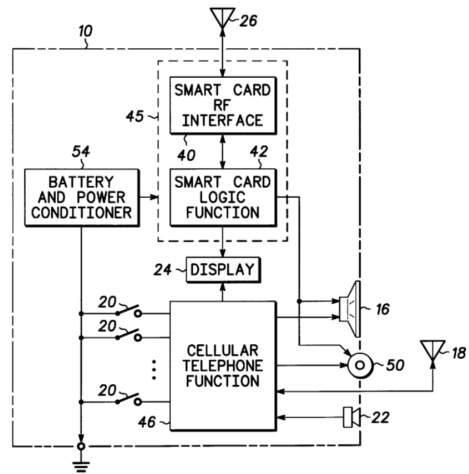


FIG. 2

Fox '624 at Fig. 5

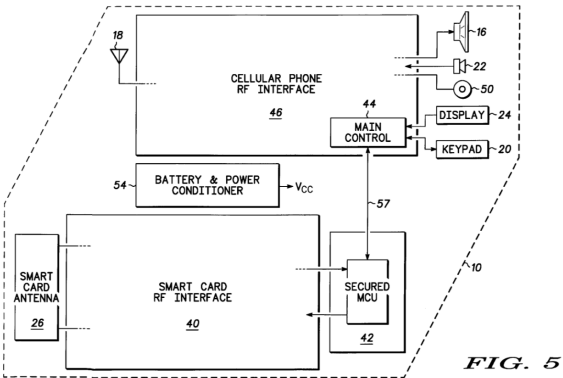


FIG. 5

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Fox ’624 at 1:62–64 FIG. 2 is a detailed block diagram illustrating the electronics for incorporating both a smartcard function and a cellular telephone function; Fox ’624 at 2:3–7 FIG. 5 is a detailed block diagram illustrating the electronics of the cellular telephone circuitry of FIG. 4 and the smartcard circuitry of FIG. 3 combined to form a cellular telephone for implementing both cellular telephone and smartcard functions. Fox ’624 at 2:10–29 Referring to FIG. 1, a pictorial diagram is shown illustrating the conceptual idea of incorporating a smartcard and its associated functions within cellular telephone 10. Cellular telephone 10 includes cellular telephone circuitry and smartcard circuitry (shown in block form in FIG. 2 and in detailed block form in FIGS. 3 and 4) for performing both a cellular telephone function and a smartcard function. The circuitry for accomplishing the smartcard function includes an RF interface and smartcard logic function circuitry. The RF interface provides a contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system. This integration of a contactless smartcard into a cellular telephone function provides ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system. Fox ’624 at 2:30–37 Cellular telephone 10 includes casing 12 for housing the electronics for implementing both a smartcard function and a cellular telephone function as will be described and shown in more detail with respect to FIG. 2. Cellular telephone 10 includes on-off switch 14, speaker 16 and cellular telephone antenna 18. Additionally, cellular telephone 10 includes selector buttons 20, voice input/microphone 22 and display 24. Fox ’624 at 3:27–34 The present invention provides a cellular telephone that incorporates the electronic circuitry for implementing both a cellular telephone function and a smartcard function functions via smartcard circuitry 42 and cellular telephone circuitry 46, respectively. This allows the smartcard electronics to be

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. Fox ’624 at 5:35–46 Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox ’624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox ’624 at 6:4–5 cellular telephone circuitry, including a main controller, for performing cellular telephone functions; Fox ’624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account. Fox ’624 at 6:58–67 obtaining an integrated circuit having cellular telephone circuitry and smartcard circuitry disposed on a single semiconductor chip, said cellular telephone circuitry for communicating with a selected external communications entity via an external cellular telephone system and said smartcard circuitry for use in

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	performing smartcard functions by communicating with an external smartcard reader via a direct external radio frequency (RF) channel between the cellular telephone and the external smartcard reader; and Fox ’624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and Fox ’624 at 7:36–41 cellular telephone circuitry for performing cellular telephone functions, said cellular telephone functions including establishing a communications connection between the cellular telephone and a remote communications entity via an external cellular communications system; Fox ’624 at 8:16–19 wherein said smartcard circuitry includes means for utilizing said cellular telephone circuitry to update information associated with said smartcard functions that is stored in said cellular telephone; Fox ’624 at 8:20–27 wherein said smartcard functions include financial transaction functions, said means for utilizing using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said means for utilizing updating a memory location associated with said account using said financial information. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
8. The mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.	Fox ’624 discloses or renders obvious “[t]he mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.” For example: Fox ’624 at 5:35–46

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
	Moreover, since cellular telephone 10 includes both smartcard and cellular telephone functions, information stored within the smartcard of telephone 10 has the ability to be updated or modified by utilizing the incorporated cellular telephone function. For example, cellular telephone function 46 may access, via the cellular telephone infrastructure, a banking institution while main control 44 communicates with MPU 41 for allowing electronic cash to be downloaded onto the smartcard. In this manner, the smartcard within cellular telephone 10 may be updated via wireless communications by making use of the internal cellular telephone function. Fox ’624 at 5:48–60 By now it should be apparent that a novel cellular telephone has been provided that incorporates the electronics for implementing both a cellular telephone function and a smartcard function. This allows the smartcard electronic circuitry to be protected from damage by the housing associated with the cellular telephone and also decreases the likelihood that the smartcard will be lost or stolen. The cellular telephone also includes an RF interface for wireless communication between the smartcard and an external reader. Further, by making use of the cellular telephone function, information associated with the smartcard function may be updated or modified via existing cellular telephone infrastructure. Fox ’624 at 6:23–30 erein said smartcard functions include financial transaction functions, wherein said smartcard controller is capable of using said cellular telephone circuitry to contact a banking institution via an external cellular telephone system to obtain financial information relating to a particular account, said smartcard controller using said financial information to update a memory location associated with said account. Fox ’624 at 7:7–14 wherein said smartcard circuitry is electrically coupled to said cellular telephone circuitry on said single semiconductor chip, said smartcard circuitry including means for utilizing said cellular telephone circuitry to contact a remote external entity via the external cellular telephone system for updating information associated with said smartcard functions that is stored in said cellular telephone; and To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.

Claim Element	Exemplary Citations to US5943624A (“Fox ’624”)
9. The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.	Fox ’624 discloses or renders obvious “[t]he mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.” For example: Fox ’624 at 5:1–12 Generally, the smartcard function within cellular telephone 10 is interrogated or updated by a smartcard infrastructure using an RF field that is received by the integral smartcard antenna 26 whereby antenna 26 may be the same or separate from antenna 18 associated with the cellular telephone function. Likewise, data from the smartcard is also transferred to the infrastructure using the same antenna. For example, a smartcard infrastructure may be an external system such as an RF card reader associated with a banking institution for performing ATM transactions, or a point-of-sale (POS) system associated with a merchant for performing a sales transaction. Fox ’624 at 5:27–34 Smartcard data may also be accessed and displayed on display 24 through the use of selector buttons 20. For example, the balance of a smartcard may be displayed on display 24. Additionally, a menu system enabling the display of different data types, for example, medical information or multiple account balances or transaction lists, could also provided on display 24 and of which could be accessed via selector buttons 20. To the extent this limitation is not disclosed by Fox ’624, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Fox ’624, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.

DEFENDANTS' INVALIDITY CONTENTIONS FOR U.S. PAT. 11,270,174

EXHIBIT G5: US20030075610A1 ("Ong '610")

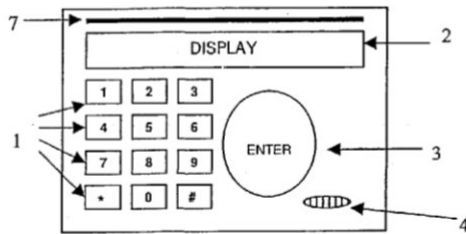
As demonstrated in the claim charts below, the claims of U.S. Patent No. 11,270,174 ("the '174 patent") are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Ong '610 and (b) under 35 U.S.C. § 103(a) as obvious over Ong '610 standing alone and as set forth herein, and/or combined 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 G and Exhibits G1–G5, 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 '174 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.

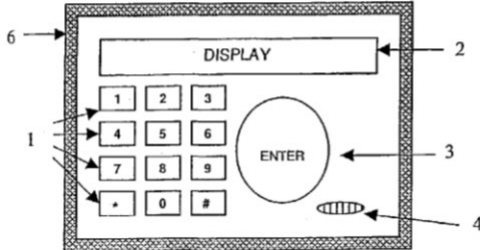
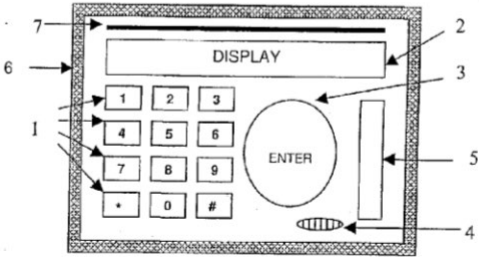
Defendants have conducted the invalidity analysis herein based at least in part and in some instance entirely upon Plaintiff's apparent application of the claims of the '174 patent. By charting the prior art against the claims and limitations herein, Defendants are not admitting or agreeing to Plaintiff's 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.

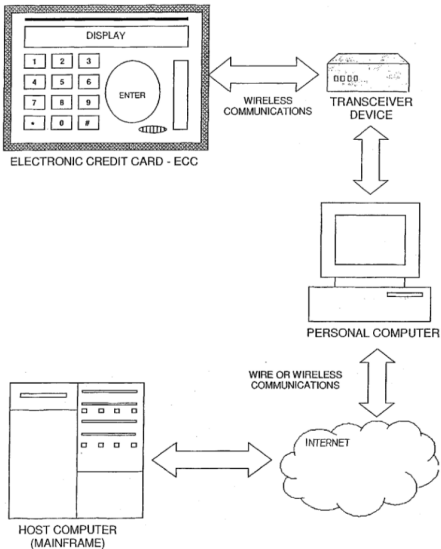
Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	To the extent this limitation is not disclosed by Ong ’610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong ’610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1a] a memory to hold transaction data for use in a plurality of transactions;	Ong ’610 discloses or renders obvious “a memory to hold transaction data for use in a plurality of 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 [0014] a storage means for storing the user's account details for use in an electronic funds transfer transaction; and Ong ’610 at [0019] Preferably the storage means is arranged to store a financial limit for transactions that the electronic credit card may be used for. Preferably the financial limit is provided to the transaction station by the communication means. Alternatively the electronic credit card including a processor means for keeping track of the use of the electronic credit card and will not generate or provide the authorisation code if the financial limit is exceeded. Alternatively the financial limit may be retrieved via the transaction station from a financial institution. Ong ’610 at [0019]–[0020] Preferably the storage means is arranged to store more than one set of account details. Ong ’610 at [0021]

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	Preferably the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong ’610 at [0026] Preferably the storage means stores transaction details and a processor means is provided to calculate the funds available. Ong ’610 at [0041] Referring to FIG. 1, there is shown an electronic credit card including a user verification means; a means for generating a unique code (not shown); a storage means for storing the user's account details (not shown); and a communication means. In this embodiment the user verification means includes a keypad for entry of a personal identification number (PIN) and the communication means includes a infra red communication device 5, a magnetic induction telecommunication device 6, radio frequency telecommunication device in the form of an antenna 7. The electronic credit card also includes a display 2, an enter/confirmation button and an audio transducer 4 for providing an audible sound. Ong ’610 at [0063] The electronic credit card can store more than one credit card/debit card accounts. These can be cards distributed from different financial institutions, organisations or companies. The electronic credit card can retain amounts of transactions conducted by the user, with information regarding his or her financial balance in relation to the account limit. This may be available for one or more credit card accounts. Ong ’610 at claim 1 a storage means for storing the user's account details for use in an electronic funds transfer transaction; and Ong ’610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. Ong ’610 at claim 21 . An electronic credit card in accordance with claim 6, wherein the storage means stores transaction details and a processor means is provided to calculate the funds available from the financial limit.

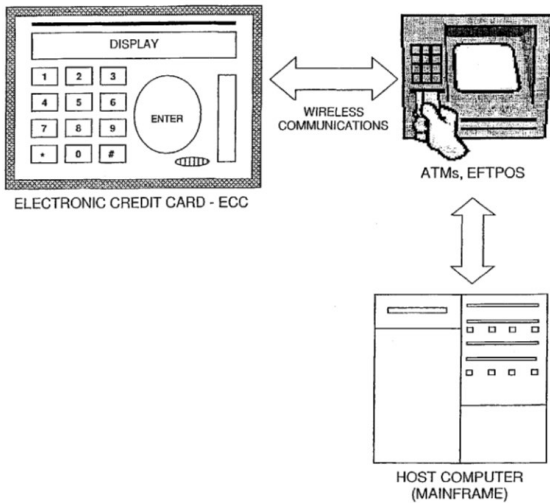
Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	To the extent this limitation is not disclosed by Ong ’610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong ’610, those elements, as known to them or as disclosed by other prior art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

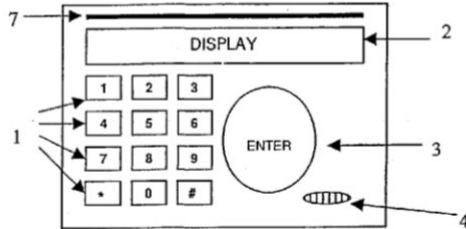
Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	Figure 6: A drawing of ECC physical form covering SAC with PIN control using magnetic induction telecommunication device. Drawing is not to scale.  Ong ’610 at Figure 10 Figure 10: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong ’610 at [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]

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	The electronic code also includes a processor means for receiving input from the keypad 1 and the button 3. The processor means is also arranged to control output of the display 2 and output of the audio transducer 4. The processor means is further arranged to control communication via the communication means 5, 6, 7. Ong ’610 at [0042]–[0043] The keypad in combination with firmware control of the processor forms the user verification means. The processor under the control of firmware forms a means for generating the unique authorisation code. The infra red communication device, magnetic communication device, or radio frequency communication device under the control of firmware control of the processor forms the communication means. The firmware may be stored in the storage means and may be reprogrammed. Ong ’610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong ’610 at [0050] FIG. 6 shows a version of the electronic credit card with a keypad forming part of the user verification means and magnetic induction communication device 6 forming part of the communication means. Ong ’610 at [0053] FIG. 10 shows a version of the electronic credit card with a keypad 1 forming part of the user verification means, a combination of infra red transmitter receiver 5, radio frequency antenna 7 and induction 6 forming part of the communication means. Ong ’610 at [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.

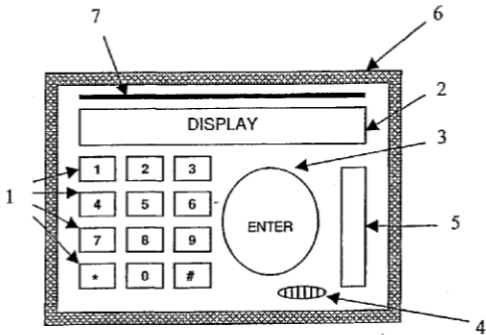
Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	Ong ’610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the 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. To the extent this limitation is not disclosed by Ong ’610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong ’610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading.
[1c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;	Ong ’610 discloses or renders obvious “a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network.” For example: Ong ’610 at Figure 2 Figure 2: A drawing of ECC communications link to PC and Mainframe Computer. Drawing is not to scale.  <pre> graph TD ECC[ELECTRONIC CREDIT CARD - ECC] <--> WIRELESS COMMUNICATIONS TD[TRANSCEIVER DEVICE] TD <--> PC[PERSONAL COMPUTER] PC <--> WIRE OR WIRELESS COMMUNICATIONS I((INTERNET)) I <--> HC[HOST COMPUTER MAINFRAME] </pre>

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 [0025] Preferably the communication means includes a telephone network interface. Ong ’610 at [0030] FIG. 2 is a schematic representation of communication between an electronic credit card of FIG. 1 with a personal computer and thus and in turn via computer network with a host computer; 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.
[1d] a driver to excite the current carrying conductor; and	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.
[1e] a processor coupled to control the driver.	Ong ’610 discloses or renders obvious “a processor coupled to control the driver.” For example: 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. 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 represents a point-of-sale transaction.	Ong ’610 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.” For example: Ong ’610 at Figure 3 Figure 3: A drawing of ECC communications link to Teller Machines, ATMs, EFTPOS and Host Computer. Drawing is not to scale.  The diagram illustrates the communication architecture of the ECC system. On the left is the 'ELECTRONIC CREDIT CARD - ECC', which features a 'DISPLAY' at the top, a numeric keypad with digits 1-9, 0, and *, an 'ENTER' button, and a small antenna at the bottom. A double-headed arrow labeled 'WIRELESS COMMUNICATIONS' connects the ECC to a central unit labeled 'ATMs, EFTPOS'. This unit includes a keypad and a screen, with a hand icon indicating user interaction. Below this unit is a 'HOST COMPUTER (MAINFRAME)', represented by a large rectangular box with multiple internal compartments. A vertical double-headed arrow connects the 'ATMs, EFTPOS' unit to the 'HOST COMPUTER (MAINFRAME)'. Ong ’610 at Figure 5.

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong ’610 at [0047] Referring to FIG. 3, the electronic credit card communicates by it's communication means with an automatic teller machine (ATM) or an electronic funds transfer point of sale (EFTPOS) machine, which in turn communicates via standard methods to a host computer to perform electronic funds transfer, cash withdrawal or other transaction. Ong ’610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong ’610 at claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong ’610 at claim 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.

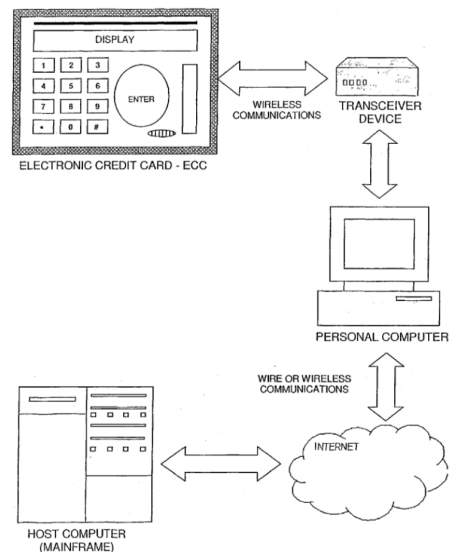
Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	<i>See also</i> claim 1 above.
3. The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	Ong ’610 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.” For example: 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 claim 1 a communication means for communicating with a transaction station to provide the transaction station with account details of the user and the authorisation code to facilitate an electronic fund transfer transaction. Ong ’610 at claim 11 An electronic credit card in accordance with claim 1, wherein the storage means is arranged to store electronic cash and the communication means is arranged to facilitate the use of the electronic cash stored in the storage means if the user identification is verified. To the extent this limitation is not disclosed by Ong ’610, it would have been obvious to one of ordinary skill in the art to combine, with the teachings of Ong ’610, those elements, as known to them or as disclosed by other prior art identified in the cover pleading. <i>See also</i> claim 1 above.
4. The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Ong ’610 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.” 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

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	latest financial information including balances on its display unit. Keypads (1) enable PIN (personal identification number) entries so that an ECC is operational. Information Display Unit (2) including an LCD (liquid crystal display) screen or other display screens provides visual information. ENTER key (3) confirms a transaction. It is also used to activate an ECC when a PIN is keyed. Audio Transducer (4) confirms entries made on keypads (1). Audio Transducer is also used to activate a financial transaction via a telephone. Data transmission/reception is via Infra red (5), Magnetic (6) and Radio Frequency (7) devices. Ong ’610 at Figure 1 Figure 1: A drawing of ECC physical form covering SAC with PIN control using a combination of infra-red, radio frequency and magnetic induction telecommunication devices. Drawing is not to scale.  Ong ’610 at Figure 2

Claim Element

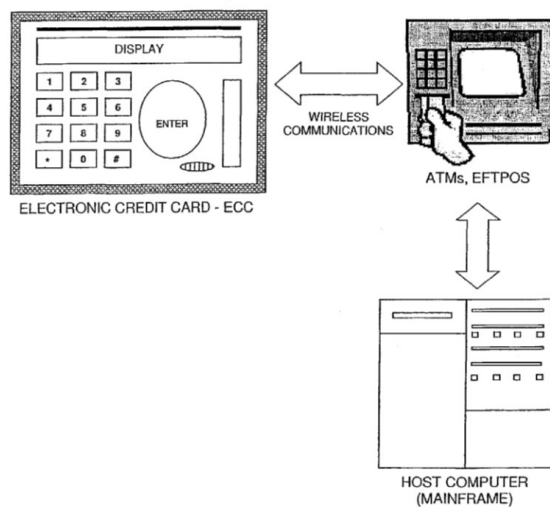
Exemplary Citations to US20030075610A1 (“Ong ’610”)

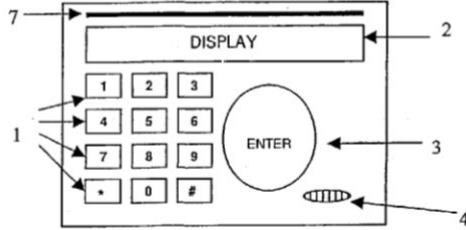
Figure 2: A drawing of ECC communications link to PC and Mainframe Computer.
Drawing is not to scale.



Ong ’610 at Figure 3

Figure 3: A drawing of ECC communications link to Teller Machines, ATMs, EFTPOS and Host Computer. Drawing is not to scale.

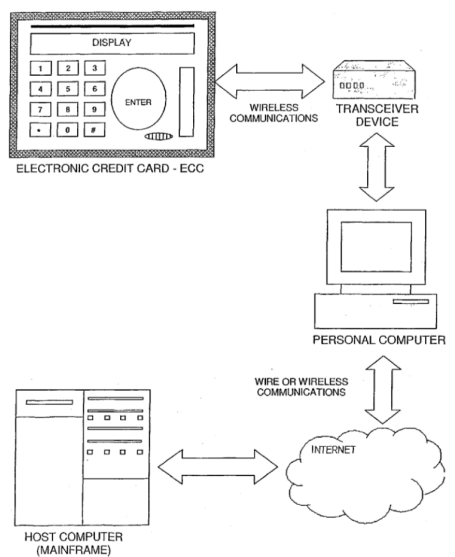


Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	Ong ’610 at Figure 5. Figure 5: A drawing of ECC physical form covering SAC with PIN control using radio frequency telecommunication device. Drawing is not to scale  Ong ’610 at [0001] The present invention relates to an electronic credit 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;

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	Ong ’610 at [0033] FIG. 5 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong ’610 at [0034] FIG. 6 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong ’610 at [0035] FIG. 7 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong ’610 at [0036] FIG. 8 is a further alternative embodiment of an electronic credit card in accordance with the present invention; Ong ’610 at [0037] 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

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	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 [0047] Referring to FIG. 3, the electronic credit card communicates by it's communication means with an automatic teller machine (ATM) or an electronic funds transfer point of sale (EFTPOS) machine, which in turn communicates via standard methods to a host computer to perform electronic funds transfer, cash withdrawal or other transaction. Ong ’610 at [0048] FIG. 4 shows a typical physical form of an electronic credit card with a keypad as the user verification means, and infra red receiver as part of the communication means. Ong ’610 at [0049] FIG. 5 shows a version of the electronic credit cards with a keypad forming part of the user verification means and radio frequency antenna forming part of the communication means. Ong ’610 at [0050] FIG. 6 shows a version of the electronic credit card with a keypad forming part of the user verification means and magnetic induction communication device 6 forming part of the communication means. Ong ’610 at [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

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone. Ong ’610 at claim 1 An electronic credit card comprising at least: Ong ’610 at claim 1 a 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. <i>See also</i> claim 1 above.
6. The mobile phone of claim 1 wherein the driver comprises a current driver.	<i>See also</i> 1[d] 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. <i>See also</i> claim 1 above.
7. The mobile phone of claim 1 wherein the network is one of a	Ong ’610 discloses or renders obvious “[t]he mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.” For example:

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
cellular network or a wireless local area network.	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 [0025] Preferably the communication means includes a telephone network interface. Ong ’610 at [0030] FIG. 2 is a schematic representation of communication between an electronic credit card of FIG. 1 with a personal computer and thus and in turn via computer network with a host computer; 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. <i>See also</i> claim 1 above.
8. The mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more	Ong ’610 discloses or renders obvious “[t]he mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.” For example: Ong ’610 at [0019]

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
parts of the transaction data is downloaded periodically.	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 [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 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]–[0059] The electronic credit card financial limit can be verified by the transaction station with a link to a remote site system. This will prevent the electronic credit card from generating further transactions once the financial limit is reached. The funds limiting function is optional and may be activated by either the financial institution issuing the electronic credit card or by the holder to cross-check and either alert him or her of his or her account balance. The electronic credit card may transact electronic cash which can be used as a currency exchange device. A traveller going abroad can choose to have a set amount for a specific currency of a particular country that he or she is visiting. The electronic credit card may be incorporated into another electronic device or piece of equipment, for example it may have been incorporated in a mobile phone. Ong ’610 at claim 5 5. An electronic credit card in accordance with claim 1, wherein the unique authorisation code is generated in synchronisation with the transaction station.

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. <i>See also</i> claim 1 above.
9. The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.	Ong ’610 discloses or renders obvious “[t]he mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of 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 [0058]

Claim Element	Exemplary Citations to US20030075610A1 (“Ong ’610”)
	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 [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. 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. <i>See also</i> claim 1 above.