UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD., and

SAMSUNG ELECTRONICS AMERICA, INC.,

Petitioners,

v.

ICASHE, INC.,

Patent Owner.

Case IPR2025-00645

Patent No. 11,270,174

DECLARATION OF HENRY N. DREIFUS IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,270,174

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. QUALIFICATIONS 5

III. LEGAL UNDERSTANDING 9

IV. BACKGROUND OF THE TECHNOLOGY 16

V. THE '174 PATENT 18

A. '174 Patent Overview 18

B. The Prosecution History 21

VI. LEVEL OF ORDINARY SKILL IN THE ART 32

VII. CLAIM CONSTRUCTION 34

VIII. GROUNDS OF UNPATENTABILITY 34

IX. SPECIFIC GROUNDS FOR CHALLENGE 36

A. GROUND 1: Doughty in view of Abe (Claims 1-9) 36

1. Overview of Doughty (Ex. 1005, U.S. Patent App. Pub. 2004/0133787) 36

2. Overview of Abe (Ex. 1011, U.S. Patent App. Pub. US2005/0086171) 39

3. Motivation to Apply Abe's Teachings to Doughty 40

4. Invalidity of Claims 1-9 Over Doughty in view of Abe 44

B. Ground 2: Doughty in view of Abe and Fox (Claims 1-9) 96

C. Grounds 3-4: Doughty in view of Abe and Dua and Doughty in view of Abe, Fox, and Dua (Claim 7) 100

D. Grounds 5-6: Doughty in view of Abe and Flitcroft and Doughty in view of Abe, Fox, and Flitcroft (Claim 8) 102

E. Grounds 7-8: Doughty in view of Abe and Bursch and Doughty in view of Abe, Fox, and Bursch (Claim 9) 105

X. SECONDARY CONSIDERATIONS 107

XI. CONCLUSION 108

I. INTRODUCTION

1. My name is Henry N. Dreifus and I am currently the Managing Director of Dreifus Associates, Ltd., Inc. I have been retained on behalf of Samsung Electronics Co. Ltd. and Samsung Electronics America Inc. ("Samsung"), to provide my opinions on certain issues related to U.S. Patent No. 11,270,174 ("the '174 patent") in connection with the above-captioned *inter partes* review ("IPR") proceeding. In particular, I have been asked to provide my insights, analysis, and opinions regarding whether claims 1-9 of the '174 patent ("Challenged Claims") are obvious over the prior art references identified below.

2. I understand that the '174 patent is titled "Mobile Phone with Magnetic Card Emulation," names as inventors Siva G. Narendra, Thomas N. Spitzer, and Prabhakar Tadepalli, and according to USPTO records is currently assigned to iCashe, Inc. I have considered the '174 patent. I understand that the '174 patent has been provided as Ex. 1001.

3. I understand that the file history of the '174 patent has been provided as Ex. 1002. I have considered this file history, and I will refer to it as "the '174 File History."

4. I understand that the '174 patent is a continuation of U.S. Patent Application No. 17/021,347 ("the '347 Application"), which is a continuation of U.S. Patent Application No. 16/218,733, which is a continuation of U.S. Patent

Application No. 14/948,325, which is a continuation of U.S. Patent Application No. 14/747,770, which is a continuation of U.S. Patent Application No. 14/680,684, which is a continuation of U.S. Patent Application No. 13/592,323, which is a continuation of U.S. Patent Application No. 13/304,663, which is a continuation of U.S. Patent Application No. 13/114,434, which is a continuation of U.S. Patent Application No. 12/941,410, which is a continuation of U.S. Patent Application No. 12/539,369, which is a continuation of U.S. Patent Application No. 11/063,291 ("the '291 Application").

5. I understand that the '174 patent claims a priority date of February 22, 2005, the filing date of the '291 Application. I have been asked to assume the Challenged Claims are entitled to this priority date. I have not been asked to opine on whether the Challenged Claims of the '174 patent are entitled to this priority date, and do not provide any opinion on that subject.

6. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (see Section II). I am qualified to opine concerning what a person of ordinary skill in the art would have known and understood during that time. Before February 22, 2005, my level of skill in the art was at least that of a person of ordinary skill. I am qualified to opine concerning what a person of ordinary skill in the art would have known and understood at the time of the '174 patent's purported invention. My analysis and

conclusions herein are from the perspective of a person of ordinary skill in the art as of February 22, 2005.

7. As part of my independent analysis for this declaration, I have considered the following: the background knowledge/technologies that were commonly known to persons of ordinary skill in this art during the time before the earliest claimed priority date for the '174 patent; my own knowledge and experiences gained from my work experience in the field of the '174 patent and related disciplines; and my experience in working with others involved in this field and related disciplines.

8. I have considered the following non-exhaustive list of references in preparing my declaration. I have been instructed to assume that each of these references qualifies as prior art.

- **U.S. Patent App. Pub. No. 2004/0133787 ("Doughty")** to Ralph O. Doughty and Patrick Antaki ("Doughty"), titled "System, Method and Apparatus For Enabling Transactions Using A Biometrically Enabled Programmable Magnetic Stripe," filed on October 7, 2003 and published on July 8, 2004. I understand that a copy of this reference has been designated as Exhibit 1005. Throughout my declaration, references to Doughty are to Exhibit 1005.
- **U.S. Patent App. Pub. No. 2005/0086171 ("Abe")** to Makoto Abe, Shuichi Sekiya, and Yuji Fukuzawa ("Abe"), titled "Information Processing System, Information Communication Terminal and Method, Information Processing device and method, recording medium, and program," filed on July 15, 2003 and published on April 21, 2005. I understand that a copy of this reference has been designated as Exhibit 1011. Throughout my declaration, references to Abe are to Exhibit 1011.

- **U.S. Patent No. 5,943,624 ("Fox")** to Thomas Michael Fox, Gerald Vincent Piosenka, and Kenneth Henry Schmidt ("Fox"), titled "Contactless Smartcard for Use in Cellular Telephone," filed on July 15, 1996 and issued on August 24, 1999. I understand that a copy of this reference has been designated as Exhibit 1009. Throughout my declaration, references to Fox are to Exhibit 1009.

- **U.S. Patent App. Pub. No. 2006/0165060 ("Dua")** to Robin Dua ("Dua"), titled "Method and Apparatus for Managing Credentials Through a Wireless Network," filed on January 21, 2005 and published on July 27, 2006. I understand that a copy of this reference has been designated as Exhibit 1012. Throughout my declaration, references to Dua are to Exhibit 1012.

- **U.S. Patent No. 6,636,833 ("Flitcroft")** to Daniel I. Flitcroft and Graham O'Donnell ("Flitcroft"), titled "Credit Card System and Method," filed on January 22, 1999 and issued on October 21, 2003. I understand that a copy of this reference has been designated as Exhibit 1013. Throughout my declaration, references to Flitcroft are to Exhibit 1013.

- **U.S. Patent No. 7,917,444 ("Bursch")** to Todd Bursch ("Bursch"), titled "Secure Single-use Transaction Numbers," filed on October 29, 2002 and published on March 29, 2011. I understand that a copy of this reference has been designated as Exhibit 1010. Throughout my declaration, references to Bursch are to Exhibit 1010.

9. I understand that there is a pending district court litigation between Petitioners and iCashe, Inc. ("Samsung Litigation") involving the '174 patent.

10. I am being compensated by Samsung at my standard hourly consulting rate of $500 for my time on this matter. My compensation is not dependent on the outcome of this proceeding or any other proceeding between the parties.

11. In forming my opinions, I have relied on the documents cited in this declaration and the documents identified in the attached Appendix B. These documents comprise patents, file histories, printed publications, and other related

documents. As I discuss below, each document is a type that experts in my field would have reasonably relied upon when forming their opinions. Further, experts in my field would have had access to each document either through the applicable patent offices and/or well-known libraries, conferences, or publications in the field. My opinions are also based upon my personal and professional experience.

II. QUALIFICATIONS

12. I am qualified by education and experience to testify as an expert in the field of electronic devices used for transactions including mobile payments including magnetic stripe emulation and RF (Radio-Frequency) for mobile payment applications. The following overview of my background pertains to my qualifications for providing expert testimony in this matter.

13. I am the Founder and Managing Director of Dreifus Associates, Limited (DAL), an Identity technology and Personnel Assurance solutions development and integration organization established in 1991.

14. I have more than 35 years of experience in advanced card solutions including extensive project work on strategic engagements developing systems applying multiple types of card technologies ranging from magnetic, optical and intelligent (smart card) for financial, security, consumer marketing, and information applications.

15. I received a Bachelor of Science in Computer Science and Engineering

from the Moore School of Engineering at the University of Pennsylvania in 1982, where I was a member of the Engineering Student Council and Chairman of the Association of Computing Machinery (ACM) Chapter. I also obtained a Master of Business Administration degree from Washington University of St. Louis in 1988, where I was a member of the Beta Gamma Sigma Honor Society.

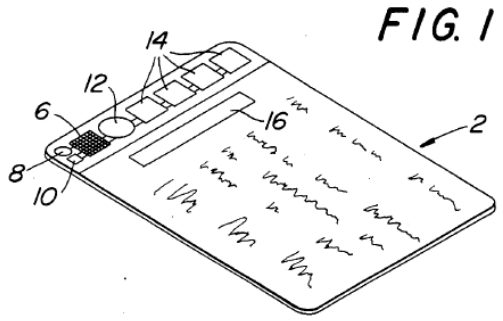
16. I have served as a recognized worldwide advisor in the card technology industry with a vision for the application of enabling technologies to solve business problems.

17. I was also a founding director of the Smart Card Industry Association and served as a delegate to the International Standards Organization (ISO) and the American National Standards Institute (ANSI) developing worldwide standards for smart (integrated circuit) cards.

18. My project assignments in smart card-based solutions include providing consulting and advisory work to various participants of the financial transaction and identification solutions supply chain ranging from the card manufacturers, system component manufacturers to system operators. This has included work for American Express, MasterCard International, Rand McNally Corporation, Visa, Arthur Blank & Company, United States Department of Defense, AT&T, and others.

19. I am the sole inventor of U.S. Patent No. 4,575,621 (the ’621 patent),

which issued on March 11, 1986. This patent is directed to a contactless portable electronic transaction card 2, for which I designed and wrote the initial device operating system, an example of which is provided in the figure below:



20. During my decades of industry experience, I have been involved in the development of many large-scale card programs including financial transaction and payment platforms, identification (ID) card projects, and I am well-versed in the types of cards, card personalization, and security features that are included in such cards. I have served as a senior project advisor and consultant in the development of need assessments and specifications for large-scale national card programs. Examples of large-scale card programs include:

- Supporting the framework and design for card platform products to incorporate (smart card) integrated circuit card-based solutions including the American Express Blue Card and American Express's participation in the development of the ICAO contactless "ePassport" machine readable travel documents (MRTD) initiatives;

- The United States Department of Defense Common Access Card for Active Military and Civilian Employees and Geneva Conventions ID Card (which now serves as a basis for all Federal ID Cards (both contact and contactless) issued to Federal Employees across the US Government), including supporting the US Department of Defense representation to the GlobalPlatform;
- The National ID Card program for the Country of Jamaica;
- The National ID Card program for the Organization of Eastern Caribbean States (OECS) member countries; and
- The National ID Card program for the Sultanate of Oman.

21. My responsibilities in connection with these large-scale card programs included developing card specifications, drafting the technical portions of the request for proposals, proposal evaluations, technical acceptance (conformance) review, acceptance testing, and implementation as well as supporting roll outs of finished cards and systems.

22. This work included the planning, design and development of solutions for producing and issuing various types of cards and portable secure data carrier technologies incorporating integrated circuits, such as secure element chips.

23. One such project in the mid-1990's supported Rand McNally Corporation's DocuSystems Division for the feasibility, evaluation, and

development of an integrated circuit (smart) card high speed manufacturing platform. This work included the design and development aspects of an integrated circuit card manufacturing line that would include the assembling and subsequent programming/personalization of cards.

24. I also co-authored the book Smart Cards: A Guide to Building and Managing Smart Card Applications, published by John Wiley & Sons.

25. A detailed record of my professional qualifications, including a list of publications, awards, and professional activities, is set forth in my curriculum vitae attached to this report as Appendix A.

26. Based on my experience and education, I believe that I am qualified to opine as to the knowledge and level of skill of one of ordinary skill in the art at the time of the alleged invention of the ’174 patent (which I further describe below) and what such a person would have understood of the state of the art during that time. Based on my above-described experience in the field of electronic devices used for transactions including, e.g., mobile payment using magnetic stripe emulation and RF, and the acceptance of my publications in my field, I believe that I am qualified to be an expert with respect to the above-described area of the ’174 patent.

III. LEGAL UNDERSTANDING

A. My Understanding of Claim Construction

27. I am not an attorney and offer no legal opinions, but in the course of

my work, I have had experience studying and analyzing patents and patent claims from the perspective of a person skilled in the art.

28. I have been informed that patent claims are construed from the viewpoint of a person of ordinary skill in the art of the patent at the time of the alleged invention. I have been informed that patent claims generally should be interpreted consistent with their plain and ordinary meaning as understood by a person of ordinary skill in the art in the relevant time period (*i.e.*, at the time of the purported invention, or the so called "effective filing date" of the patent application), after reviewing the patent claim language, the specification, and the prosecution history (*i.e.*, the intrinsic record).

29. I have further been informed that a person of ordinary skill in the art must read the claim terms in the context of the claim itself, as well as in the context of the entire patent specification. I understand that in the specification and prosecution history, the patentee may specifically define a claim term in a way that differs from the plain and ordinary meaning. I understand that the prosecution history of the patent is a record of the proceedings before the U.S. Patent and Trademark Office and may contain explicit representations or definitions made during prosecution that affect the scope of the patent claims. I understand that an applicant may, during the course of prosecuting the patent application, limit the scope of the claims to overcome prior art or to overcome an examiner's rejection, by

clearly and unambiguously arguing to overcome or distinguish a prior art reference, or clearly and unambiguously disavowing claim coverage.

30. In interpreting the meaning of the claim language, I understand that a person of ordinary skill in the art may also consider "extrinsic" evidence, including expert testimony, inventor testimony, dictionaries, technical treatises, other patents, and scholarly publications. I understand this evidence is considered to ensure that a claim is construed in a way that is consistent with the understanding of those of ordinary skill in the art at the time of the claimed invention. For example, this can be useful for a technical term whose meaning may differ from its ordinary English meaning. I understand that extrinsic evidence may not be relied on if it contradicts or varies the meaning of claim language provided by the intrinsic evidence, particularly if the applicant has explicitly defined a term in the intrinsic record.

B. My Understanding of Anticipation

31. I understand that a patent claim is invalid as "anticipated" if all the limitations of the claim are present, either expressly or inherently, in a single prior art publication or patent.

32. I also understand that a prior art reference can disclose a claimed feature because the feature is expressly described or because the feature is inherent in the disclosure. I understand that something is inherent in a prior art reference if the missing descriptive matter must necessarily be present, not merely probably or

possibly present, and it would be so recognized by a person of ordinary skill in the art as of the priority date of the patent. I understand that it is acceptable to examine evidence outside of the prior art reference (i.e., extrinsic evidence) in determining whether a feature, while not expressly discussed in the reference, is necessarily present in it.

33. I have further been informed that where a reference discloses multiple embodiments, the reference should not be limited to a preferred embodiment. Instead, each disclosed embodiment may anticipate.

34. Moreover, I have been informed that as part of an anticipation analysis, it is proper to take into account not only specific teachings of the reference, but also the inferences that one skilled in the art would reasonably be expected to draw therefrom. A reference can anticipate a claim even if it does not expressly spell out all the limitations arranged or combined as in the claim, if a person of skill in the art, reading the reference, would at once envisage the claimed arrangement or combination.

C. My Understanding of Obviousness

35. I understand that a claim may be invalid if the subject matter described by the claim as a whole would have been obvious to a hypothetical person of ordinary skill in the art in view of a prior art reference or in view of a combination of references at the time the claimed invention was made. Therefore, I understand

that obviousness is determined from the perspective of a hypothetical person of ordinary skill in the art and that the asserted claims of the patent should be read from the point of view of such a person at the time the claimed invention was made. I further understand that a hypothetical person of ordinary skill in the art is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent in suit.

36. I have been informed that there are two criteria for determining whether prior art is analogous and thus can be considered prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the patentee's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the patentee is involved. I have also been informed that the field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field. I have also been informed that a reference is reasonably pertinent if, even though it may be in a different field from that of the patentee's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to a patentee's attention in considering their problem.

37. I have also been advised that an analysis of whether a claimed invention would have been obvious should be considered in light of the scope and content of

the prior art, the differences (if any) between the prior art and the claimed invention, and the level of ordinary skill in the pertinent art involved. I understand as well that a prior art reference should be viewed as a whole.

38. I have also been advised that in considering whether a claimed invention would have been obvious over a combination of prior art references, I may assess whether there are apparent reasons to combine known elements in the prior art in the manner claimed in view of interrelated teachings of multiple prior art references, the effects of demands known to the design community or present in the marketplace, and/or the background knowledge possessed by a person of ordinary skill in the art. I understand that other principles may be relied on in evaluating whether a claimed invention would have been obvious, and that these principles include the following:

- A combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results;
- When a device or technology is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or in a different one, so that if a person of ordinary skill can implement a predictable variation, the variation is likely obvious;
- If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond their skill;
- An explicit or implicit teaching, suggestion, or motivation to combine two prior art references to form the claimed combination may demonstrate obviousness, but proof of obviousness does not depend on or require showing a teaching, suggestion, or motivation to combine;

- Market demand, rather than scientific literature, can drive design trends and may show obviousness;
- In determining whether the subject matter of a patent claim would have been obvious, neither the particular motivation nor the avowed purpose of the named inventor controls whether the claim is obvious;
- One of the ways in which a patent's subject can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims;
- Any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed;
- "Common sense" teaches that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle;
- A person of ordinary skill in the art is also a person of ordinary creativity, and is not an automaton;
- A patent claim can be proved obvious by showing that the claimed combination of elements was "obvious to try," particularly when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions such that a person of ordinary skill in the art would have had good reason to pursue the known options within his or her technical grasp; and
- One should be cautious of using hindsight in evaluating whether a claimed invention would have been obvious.

39. I further understand that, in making a determination as to whether the claimed invention would have been obvious to a person of ordinary skill, the Board may consider certain objective factors if they are present, such as: commercial success of products practicing the claimed invention; long-felt but unsolved need; teaching away; unexpected results; copying; and praise by others in the field. These

factors are generally referred to as "secondary considerations" or "objective indicia" of nonobviousness. I understand, however, that for such objective evidence to be relevant to the obviousness of a claim, there must be a causal relationship (called a "nexus") between the claim and the evidence, and that this nexus must be based on a novel element of the claim rather than something in the prior art. I also understand that even when they are present, secondary considerations may be unable to overcome primary evidence of obviousness (such as motivation to combine with predictable results) that is sufficiently strong.

IV. BACKGROUND OF THE TECHNOLOGY

40. The '174 patent is generally directed to a mobile phone that mimics a swipe of a magnetic card (e.g., credit card) by producing a time-varying magnetic field that represents transaction data (e.g., credit card data). '174 patent, 2:58-64, 3:42-48, 4:28-38, 5:38-53, 14:19-24, claims 1-2; Ex.1002 ('174FH), 1517-19. But these concepts were already known in the art as the USPTO already recognized during prosecution of the '174 patent. During its prosecution, the Examiner rejected the claims over Doughty-CON (Ex.1004), which is a continuation of and has

substantially the same disclosures as Doughty (Ex.1005).[1] The claims were allowed only after the Applicant amended the independent claims to recite "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." Ex.1002, 1517-19, 1539, 1544-45.

41. But the concept of a network interface to connect to a network to download transaction data was known. Abe discloses a system "to enable safer electronic commercial transactions," operable for a "mobile telephone" to communicate with another device via a "network." Abe, [0005], [0091], [0092], [0179], [0203], [0484]. Abe teaches that a "card identification number 351" is assigned to a "non-contact card" included in the mobile telephone , and is "provided via the network 10 by the authentication server 41" to enhance security. Abe, [0178]-[0179], [0308]. In my opinion, a person of ordinary skill in the art would have been motivated to apply Abe's teachings to Doughty to advantageously allow the device to download data used to perform electronic transactions as disclosed in Doughty.

42. As I discuss below, the claims of the '174 patent are obvious over the

[1] As I discuss below in Section V.B, the differences between Doughty and Doughty-CON are immaterial to the Examiner's analysis during prosecution of the '347 Application

prior art. Further, there were no technological barriers to combining these teachings from the prior art and a person of ordinary skill in the art would have been motivated to combine these teachings and would have understood that the combination would have yielded predictable results.

V. THE '174 PATENT

A. '174 Patent Overview

43. The '174 patent generally relates to an "intelligent electronic device" (e.g., "mobile phone") that internally communicates with an "electronic transaction card." '174 patent, Abstract, 2:58-3:10. The "electronic transaction card" "may be programmed to operate as a credit card" such that it "emit[s] one or more time-varying magnetic fields to emulate the swiping of a credit card." '174 patent, 5:38-44, 4:30-32, 11:47-59. "Electronic transaction card 104 may then be used with a magnetic stripe or smartcard based merchant point-of-sale terminal to effect a transaction." '174 patent, 4:32-35. According to the '174 patent, "the term 'transaction' refers to any beneficial use of an electronic transaction card." '174 patent, 4:16-17.

44. As shown in Figure 22, the electronic transaction card includes **processing element 2020** coupled to "**magnetic/smartcard circuitry 2030**," which "may include **circuits to produce time-varying magnetic fields** or **signals compatible with a smart card reader**." '174 patent, 11:67-12:2, 12:41-64, Figs.

20, 22. The electronic transaction device also includes "**volatile memory 2220**" storing "financial transaction data 2222." '174 patent, 12:47-52, Fig. 22. The "**magnetic/smartcard circuitry 2030**" is **coupled to** the "**volatile memory 2220**" via the "**processing element 2020**" as shown in Fig. 22. Additionally, "magnetic field producing circuits 312 may include voltage drivers, [and] current drivers." '174 patent, 6:64-67. "Intelligent electronic device 202 may include a mechanism to allow intelligent electronic device 202 to communicate with a wired or wireless network." '174 patent, 5:8-10. For example, this mechanism "may include circuitry to communicate with a cellular phone network." '174 patent, 5:11-12. The intelligent electronic device may also have "wired or wireless connectivity to a network other than a cellular network." '174 patent, 5:22-23.

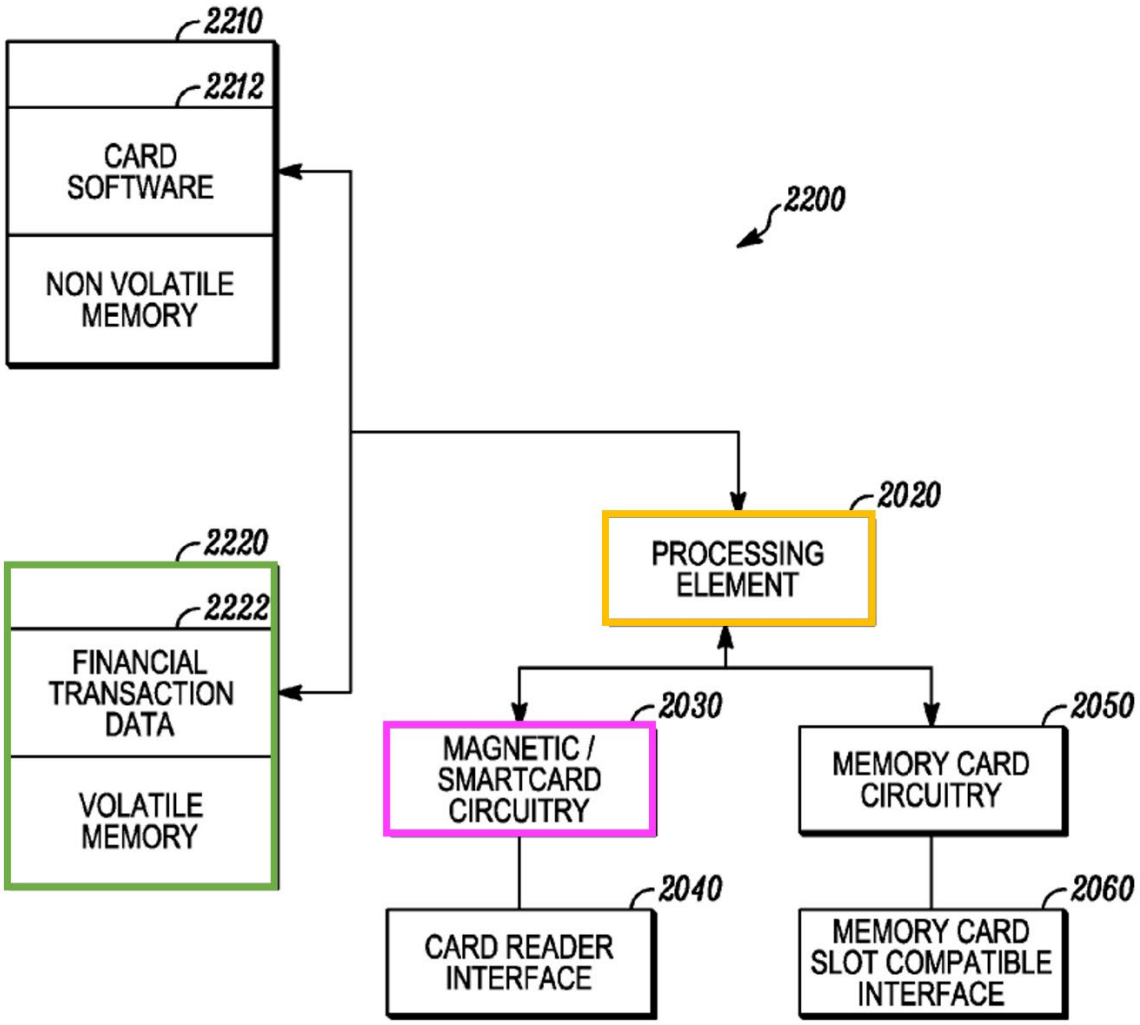


FIG. 22

The '174 patent discloses in another embodiment that a "processing device" "may read instructions from volatile memory 310 and/or nonvolatile memory 306 and perform actions in response thereto" and "execute program instructions that influence communications between" the device and "a magnetic card reader." '174 patent, 7:20-26.

B. The Prosecution History

45. In formulating my opinions, I also considered the contents of the prosecution history of the ’174 patent. *See* Ex. 1002.

46. The ’174 patent issued from U.S. Pat. App. 17/021,347 (“the ’347 Application”), filed September 15, 2020. During prosecution of the ’174 patent, the Examiner rejected claims 1-18 under Section 102 as being anticipated by Doughty-CON (U.S. Patent App. Pub. 2011/0240748). Ex. 1002, 1454.

47. While there are some minor differences in disclosure between Doughty-CON and Doughty, any substantive differences are not relevant to the material the Examiner identified as meeting limitations of the claims of the ’347 Application. Ex. 1008.

48. The following chart summarizes the citations to Doughty-CON the Examiner found taught the ’174 pending Claims:

’174 Patent (Pre-Amendment)	**Doughty-CON (Disclosure Relied Upon By Examiner)[2]**
[1.pre] A mobile phone comprising:	**Doughty-CON** [0046]
[1.a] a memory to hold transaction data for repeated use in a plurality of transactions;	**Doughty-CON** Fig. 3, 312 (“Memory”); [0009]

[2] The same paragraphs numbers and figure numbers in Doughty have identical or substantively identical disclosures as the paragraphs and figures in Doughty-CON cited by the Examiner as identified in this chart.

[1.b] current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;	**Doughty-CON** Fig. 3, 308 ("Magnetic Field Generator"); [0051]
[1.d] a driver to excite the current carrying conductor;	**Doughty-CON** Fig. 5B, 554 ("Control Circuit"); [0051]
[1.e] a processor coupled to control the driver.	**Doughty-CON** Fig. 3, 314 ("Device Processor or Controller"); [0051]
[2] The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	**Doughty-CON** [0008], [0095]-[0097]
[3] The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	**Doughty-CON** [0008], [0038]
[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	**Doughty-CON** [0008], [0038]
[5] The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.	**Doughty-CON** [0051]
[6] The mobile phone of claim 1 wherein the driver comprises a current driver.	**Doughty-CON** [0051]

Ex.1002, 1454-1457.

49. In response, Applicant amended the independent claims to include the limitation "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." Ex. 1002, 1517-19. Applicant also removed "repeated" from

"a memory to hold transaction data for repeated use in a plurality of transactions" in the independent claims. Ex. 1002, 1517-20. The claims were subsequently allowed on November 10, 2021. Ex. 1002, 1539, 1544-45.

50. I have also reviewed the language in the material from Doughty-CON cited by the Examiner during prosecution of the '374 Application, and compared it to language from Doughty. Based on my review, the language in Doughty is either identical to the language in Doughty-CON, or there are differences that are immaterial to the limitations for which the citations were used. Below, I walk though paragraphs cited, and compare the language in Doughty and Doughty-CON.

51. The difference in language of [0008] in Doughty and Doughty-CON is immaterial:

U.S. Patent App. Pub. 2004/0133787 ("Doughty")	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
[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	**[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*~~ **in the event of loss or** fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and

commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.	flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.

52. The only difference is the removal of "due to loss of the device of" and insertion of "in the event of loss or" in its place. But the Examiner did not rely on "due to loss of the device of" in the rejection. Ex. 1002, 1454-57.

53. The difference in language of [0009] in Doughty and Doughty-CON is immaterial:

U.S. Patent App. Pub. 2004/0133787 ("Doughty")	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
[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	**[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.	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*~~ **if** 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.

54. The only differences are the removal of "spatially" and the replacement of "of" with "if." But the Examiner did not rely on "spatially" in the rejection and the change from "of" to "if" was likewise irrelevant. Ex. 1002, 1454-56.

55. The difference in language of [0038] in Doughty and Doughty-CON is immaterial:

U.S. Patent App. Pub. 2004/0133787 ("Doughty")	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
[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.	**[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*~~ **in the event of loss 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.

56. The only difference is the removal of "due to loss of the device or" and insertion of "in the event of loss or" in its place. But the Examiner did not rely on "due to loss of the device or" in the rejection. Ex. 1002, 1455-57.

57. The difference in language of [0046] in Doughty and Doughty-CON is immaterial:

U.S. Patent App. Pub. 2004/0133787 ("Doughty")	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
[0046] The components of the device 302 are typically disposed within or	**[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.	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*~~ **with** 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*~~ **belonging**, such as a watch, *a* jewelry, a key ring, a tag and eye glasses, etc.

58. The only differences are the replacements of "will" with "with" and "device/belonging" with "belonging." But the Examiner did not rely on "device/belonging" in the rejection and the change from "will" to "with" is likewise irrelevant. Ex. 1002, 1457.

59. The difference in language of [0051] in Doughty and Doughty-CON is immaterial:

U.S. Patent App. Pub. 2004/0133787 ("Doughty")	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
[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	**[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.	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.

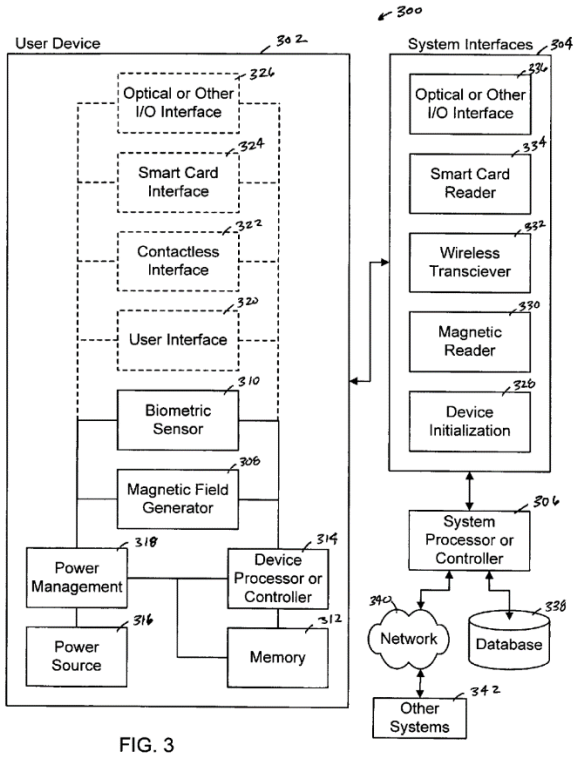
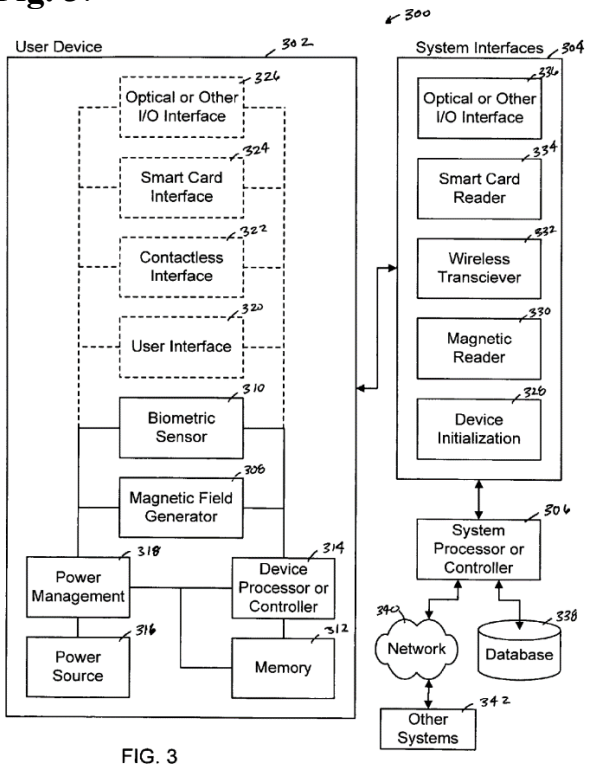
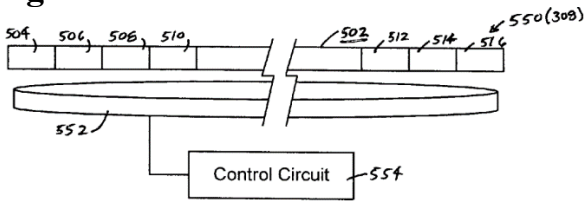
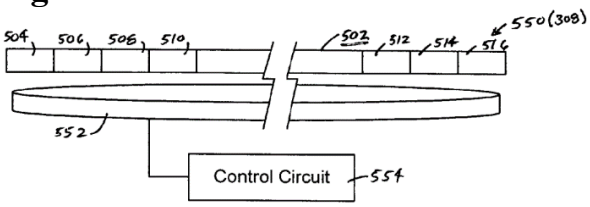
60. The only difference is the removal of "spatially distributed," but the Examiner did not rely on "spatially distributed" in the rejection. Ex. 1002, 1454-57.

61. There is no difference in the language of paragraphs [0095]-[0097]:

U.S. Patent App. Pub. 2004/0133787 ("Doughty")	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
[0095] Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment includes making retail purchases in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions.	**[0095]** Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment includes making retail purchases in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions.
[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	**[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.	availability for, and legitimacy of, the check presented for payment.
[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.	**[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.

62. Furthermore, there are no differences in Figs. 3 and 5B:

U.S. Patent App. Pub. 2004/0133787 ("Doughty")	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
Fig. 3:  FIG. 3	**Fig. 3**:  FIG. 3
Fig. 5B:  FIG. 5B	**Fig. 5B**:  FIG. 5B

VI. LEVEL OF ORDINARY SKILL IN THE ART

63. In rendering the opinions set forth in this declaration, I was asked to consider the patent claims and the prior art through the eyes of a person of ordinary skill in the art at the time of the alleged invention. I understand that the factors considered in determining the ordinary level of skill in a field of art include the level

of education and experience of persons working in the field; the types of problems encountered in the field, the teachings of the prior art, and the sophistication of the technology at the time of the alleged invention. I understand that a person of ordinary skill in the art is not a specific real individual, but rather is a hypothetical individual having the qualities reflected by the factors above. I understand that a person of ordinary skill in the art would also have knowledge from the teachings of the prior art, including the art cited below.

64. I have been asked to assume that the Challenged Claims are entitled to the benefit of the February 22, 2005 filing date of the '291 Application filing date.

65. Upon consideration of these factors, and based on my knowledge and experience in the field and my review of the '174 patent and file history, I believe that a person having ordinary skill in the art in this matter would have had at least a Bachelor's degree in electrical engineering, computer engineering, computer science, or the equivalent thereof, and approximately two years of professional experience in the field of electronic devices used for transactions. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

66. Based on my experiences, I have at least the skills of a person having ordinary skill in the art as well as a good understanding of the capabilities of a person having ordinary skill in the art at the time of the '347 Application's filing. To be

clear, all of my opinions in this declaration are from the perspective of one of ordinary skill in the art as I have defined it here during the relevant timeframe.

VII. CLAIM CONSTRUCTION

67. I have been instructed that the Challenged Claims of the ’174 patent are to be given their ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the alleged invention in light of the specification and the prosecution history pertaining to the patent. I have followed these principles in my analysis set forth in this document.

68. I understand that presently the parties have not proposed constructions for the ’174 patent in the Samsung Litigation.

VIII. GROUNDS OF UNPATENTABILITY

69. As I explain above in Section IV, the concept of using a mobile phone to perform transactions by producing a time-varying magnetic field that mimics the swipe of a magnetic card was well-known in the art.

70. In this section, I will explain why the teachings or combinations of teachings from the following references render obvious each of the Challenged Claims:

Name	Exhibit	Publication	Filed	Published/ Issued
Doughty	1005	US2004/0133787	10/7/2003	7/8/2004
Abe	1011	US2005/0086171	7/15/2003	4/21/2005

Fox	1009	US5,943,624	7/15/1996	8/24/1999
Dua	1012	US2006/0165060	1/21/2005	7/27/2006
Flitcroft	1013	US6,636,833	1/22/1999	10/21/2003
Bursch	1010	US7,917,444	10/29/2002	3/29/2011

I have been instructed to assume that each of these references qualifies as prior art.

71. As I explain below, the Challenged Claims are invalid based upon the following prior art grounds:

- **Ground 1**: Challenged Claims 1-9 of the '174 patent are rendered obvious by **Doughty** in view of **Abe**.
- **Ground 2**: Challenged Claims 1-9 of the '174 patent are rendered obvious by **Doughty** in view of **Abe** and **Fox**.
- **Ground 3**: Challenged Claim 7 of the '174 patent is rendered obvious by **Doughty** in view of **Abe** and **Dua**.
- **Ground 4**: Challenged Claim 7 of the '174 patent is rendered obvious by **Doughty** in view of **Abe**, **Fox**, and **Dua**.
- **Ground 5**: Challenged Claim 8 of the '174 patent is rendered obvious by **Doughty** in view of **Abe** and **Flitcroft**.
- **Ground 6**: Challenged Claim 8 of the '174 patent is rendered obvious by **Doughty** in view of **Abe**, **Fox**, and **Flitcroft**.
- **Ground 7:** Challenged Claim 9 of the '174 patent is rendered obvious by **Doughty** in view of **Abe** and **Bursch**.
- **Ground 8:** Challenged Claim 9 of the '174 patent is rendered obvious by **Doughty** in view of **Abe, Fox,** and **Bursch**.

72. It is my opinion that Challenged Claims of the '174 patent are unpatentable as I explain below. I note that in this discussion, I may focus on the particular language in the specific claims, but it should be understood that my

analysis applies to the corresponding elements of all Challenged Claims containing identical or substantially identical language.

IX. SPECIFIC GROUNDS FOR CHALLENGE

73. As I explain above in Section IV, although the '174 patent purports to have invented the concept of using a mobile phone to perform transactions by producing a time-varying magnetic field that mimics the swipe of a magnetic card, such devices were well-known in the art. As I describe below, the cited prior art provides these teachings.

74. In this section, I explain why claims 1-9 of the '174 patent are rendered obvious by the teachings of Doughty and Abe, either alone or in combination with Fox, Dua, Flitcroft and/or Bursch. I note that, in this discussion, I may focus on the particular language in specific claims, but it should be understood that my analysis applies to the corresponding limitations of all claims containing identical or substantially identical language.

A. GROUND 1: Doughty in view of Abe (Claims 1-9)

1. Overview of Doughty (Ex. 1005, U.S. Patent App. Pub. 2004/0133787)

75. Doughty discloses a system in which a user device 302 includes components that can be mounted onto a substrate that is incorporated into a mobile device such as a "telecommunications device." [0046]. User device 302 includes "**magnetic field generator 308**," which can "create a time-varying magnetic signal

for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader." [0010]. "Magnetic field generator 308" may have the form of a "programmable magnetic stripe 550" consisting of a "control circuit 554" and "a single inductive coil 552" such that the inductive coil 552 is "pulsed with varying currents and current directions" so as to emulate a time-varying magnetic field. [0051], Fig. 5B. A "**device processor or controller 314**" is coupled to magnetic field generator 308. [0040]. User device 302 also includes a "**memory 312**" for holding transaction data such as "binary data to enable a transaction." [0040], [0041].

76. User device 302 "can be used to enable any type of transaction" such as "an access transaction," "a financial transaction," or "a commercial transaction," including a transaction with a "point-of-sale device." Doughty, [0054], [0098]. The disclosed "commercial transactions" may include credit card transactions. Doughty [0038].

77. Figure 3 illustrates an exemplary embodiment of the user device 302 as used together with system interfaces 304. Figure 5B illustrates the magnetic field generator, element 308 in Figure 3.

"circuitry to produce a time-varying magnetic field"

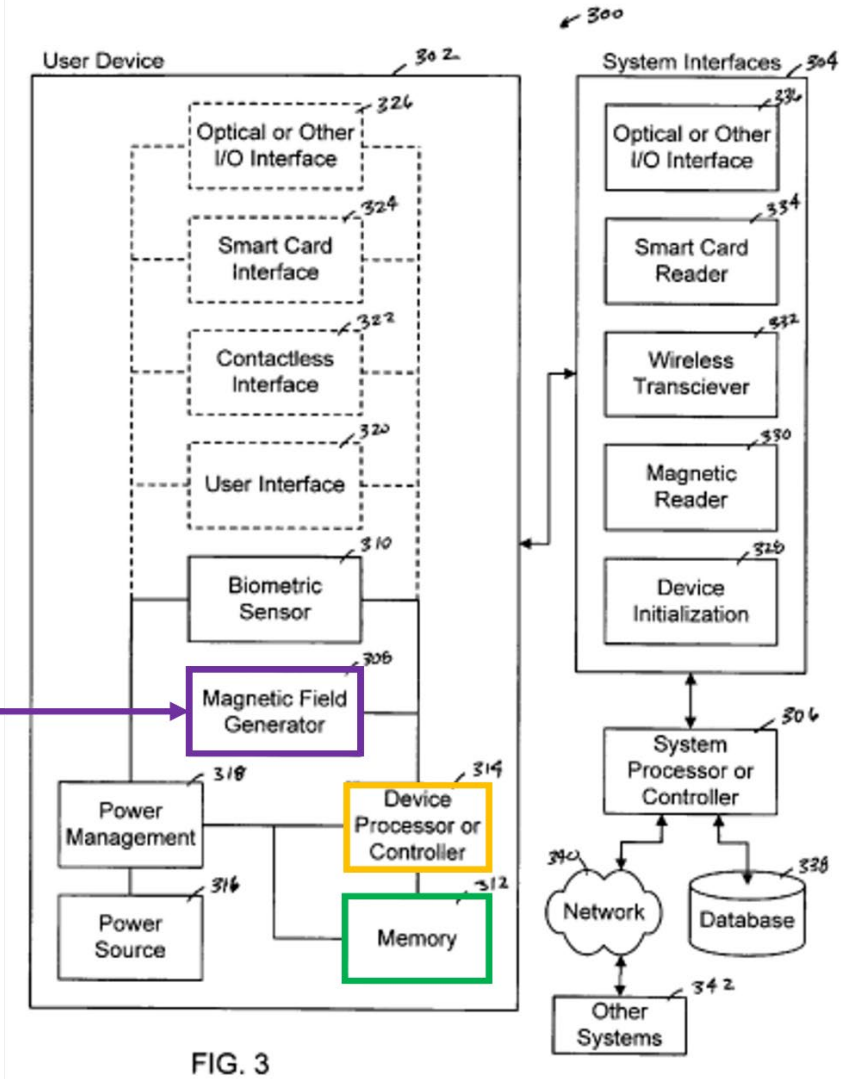
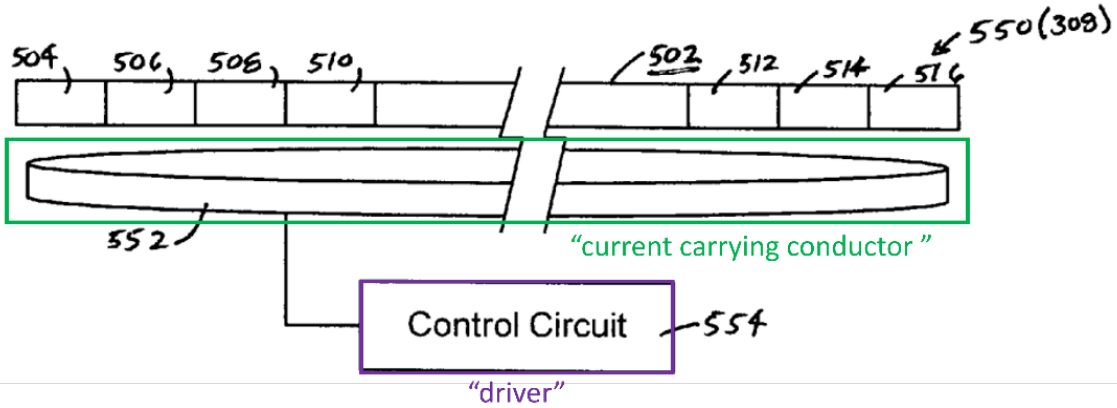


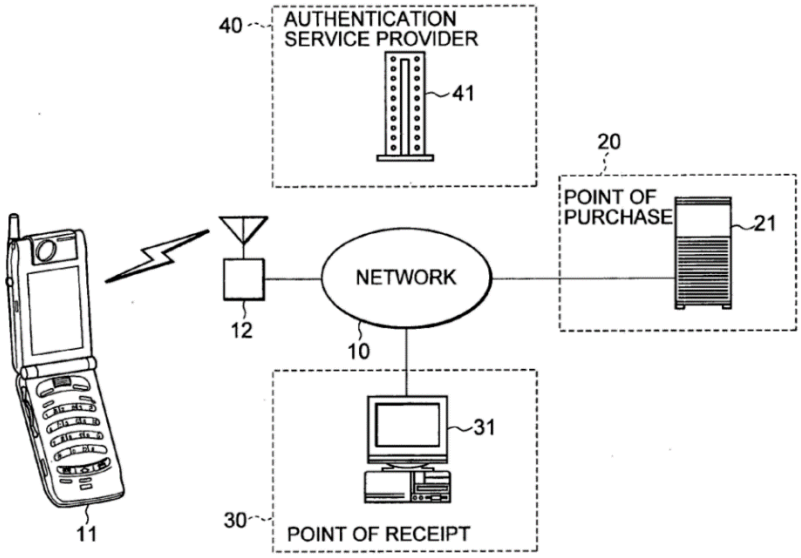
FIG. 3



2. Overview of Abe (Ex. 1011, U.S. Patent App. Pub. US2005/0086171)

78. Abe discloses a system "to enable safer electronic commercial transactions to be carried out in a straightforward manner." [0005]. Abe discloses a "mobile telephone 11" that communicates with another device via a "network 10." [0091], [0092], [0179], [0203], [0484]. The mobile telephone receives transaction data from an "authentication server 41" via the network to authenticate a transaction. [0179], [0186], [0187], [0189], [0190], [0329]. For example, "temporary commercial transaction information rewriting key 362" and "card identification number 351" are provided to the mobile phone by the authentication server, which then uses this information to perform a transaction. [0179], [0187], [0197], [0220], [0258], [0266], [0314], [0454]. "The card identification number 351…is a number for identifying the non-contact IC card 146" within the mobile telephone, and is provided "when the user of the mobile telephone 11 is registered as a purchaser of merchandise." [0178]-[0179]. The temporary commercial transaction information rewriting key is "a kind of one-time password" to perform a transaction that is deleted after use. [0187]. The authentication server "can supply temporary commercial transaction information rewriting keys 362 to the mobile telephone 11 any number of times." [0187].

FIG. 1



3. Motivation to Apply Abe's Teachings to Doughty

79. Abe and Doughty are analogous art, in the same field as the '174 patent, which includes electronic devices for performing transactions, and are reasonably pertinent to purported problems addressed by the named inventors of the '174 patent involving the use of electronic devices to securely perform transactions. '174 patent, 1:48-67, 5:29-37, 6:9-18, 12:41-64; Doughty [0002], [0003], [0004], [0007], [0008], [0038], [0040], [0041], [0046]; Abe Abstract, [0001], [0002], [0003], [0004], [0005], [0006], [0179], [0183], [0509], [0510], [0511], [0512], [0513].

80. In my opinion, a person of ordinary skill in the art would have been motivated to apply Abe's teachings of a mobile phone to Doughty's telecommunications device. To the extent that it is argued that "telecommunications

device" in Doughty refers to the more general class of devices communicating over a distance, instead of to a mobile phone specifically, a person of ordinary skill in the art would have been motivated to look to a reference like Abe, which teaches examples of such telecommunications devices in which to implement functionality to perform commercial transactions, including a mobile telephone. Doughty, [0038], [0040]; Abe, [0091], [0092], [0179], [0203], [0484]. For example, a person of ordinary skill in the art would have understood that integration of smartcard functionality into a mobile phone provides numerous advantages, including ease of use, enhanced security from theft or loss, and the ability to use the phone's display and input functionality to view and update/change information stored within the smartcard. Fox, 2:21-29 (incorporation of smartcard circuitry into a phone allows "ease of use of the smartcard"). Moreover, a person of ordinary skill in the art would have understood that implementing the functionality in a mobile phone would advantageously allow a user to perform commercial transactions with a device that a user would already be carrying around with them, including to locations where transactions would take place. Fox, 2:21-29 (incorporation of smartcard circuitry into a phone allows "ease of use of the smartcard"). A person of ordinary skill in the art would have found it straightforward and advantageous to apply Abe's teachings to Doughty given Doughty's teaching that its system could be implemented in a variety of mobile devices, including a "telecommunications device." Doughty,

[0046].

81. In my opinion, a person of ordinary skill in the art would have also been motivated to apply Abe's teachings of downloading transaction data from an authentication server over a network to Doughty's telecommunications device to advantageously improve the security of its financial transactions, as desired by Doughty. For example, Doughty identifies the problem that "[t]he security of current magnetic stripe cards is suspect due to the ease of card theft and 'skimming' of card data for creating and using fake cards." Doughty, [0003]. Doughty further explains that "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, [0008]. Though Doughty discloses biometric authentication for authenticating the *user* performing a transaction (e.g., Doughty [0009]), it does not address how to protect against other security vulnerabilities contemplated by Abe, such as authenticating the *device* used to perform the transaction, and preventing the tampering of sensitive information used in the transaction. Abe [0179]. For example, Abe discloses that the authenticating server 41 supplies the mobile telephone used in the transaction with a "card identification number 351" over the network 10 to ensure that the device performing the transaction is pre-approved by the authentication server. Abe, [0179], [0308]. For example, if two devices have the same card identification, it can be

determined that purchasing information of a mobile phone "has been illegally duplicated." Abe, [0308].

82. Additionally, a person of ordinary skill in the art would have been motivated to apply Abe's teachings of downloading temporary rewriting keys to Doughty's telecommunications device to advantageously limit unauthorized tampering or use of sensitive information. For example, Abe discloses that "in order to prevent illegal duplication and falsification, it is not possible to make, edit or delete the temporary commercial transaction information without using the temporary commercial transaction information rewriting key 362." Abe [0186].

83. In my opinion, a person of ordinary skill in the art would have found it straightforward to apply Abe's teachings of downloading transaction data from an authentication server over a network to Doughty's telecommunications device. For example, Doughty already teaches the use of binary data with various types of transaction data. Doughty, [0041]. A person of ordinary skill in the art would have found it straightforward to download some of that data from a network as taught by Abe. Moreover, a person of ordinary skill in the art would have found it straightforward to include temporary transaction data and a card identification number as taught by Abe in the binary transaction data stored by Doughty, as the temporary transaction data and a card identification number would similarly be binary data in a form to be stored in memory.

84. Accordingly, a person of ordinary skill in the art would have had a reasonable expectation of success applying Abe's teachings to Doughty's telecommunications device, and a person of ordinary skill in the art would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

4. Invalidity of Claims 1-9 Over Doughty in view of Abe

85. As I discuss below, Claims 1-9 are disclosed or rendered obvious by Doughty in view of Abe. In addition to my discussion in Sections IX.A.1-3, the following discussion identifies example disclosures followed by bulleted excerpts from Doughty and of Abe that each disclose or render obvious Claims 1-9.

a. Element [1.pre]

86. **Element [1.pre] recites "A mobile phone comprising."** This element is met by Doughty and Abe.

87. **To the extent that the preamble is limiting, Doughty discloses a mobile phone** (*e.g.*, "personal communication device, such as…telecommunications device"). *E.g.*, Doughty:

- **Fig. 3:**

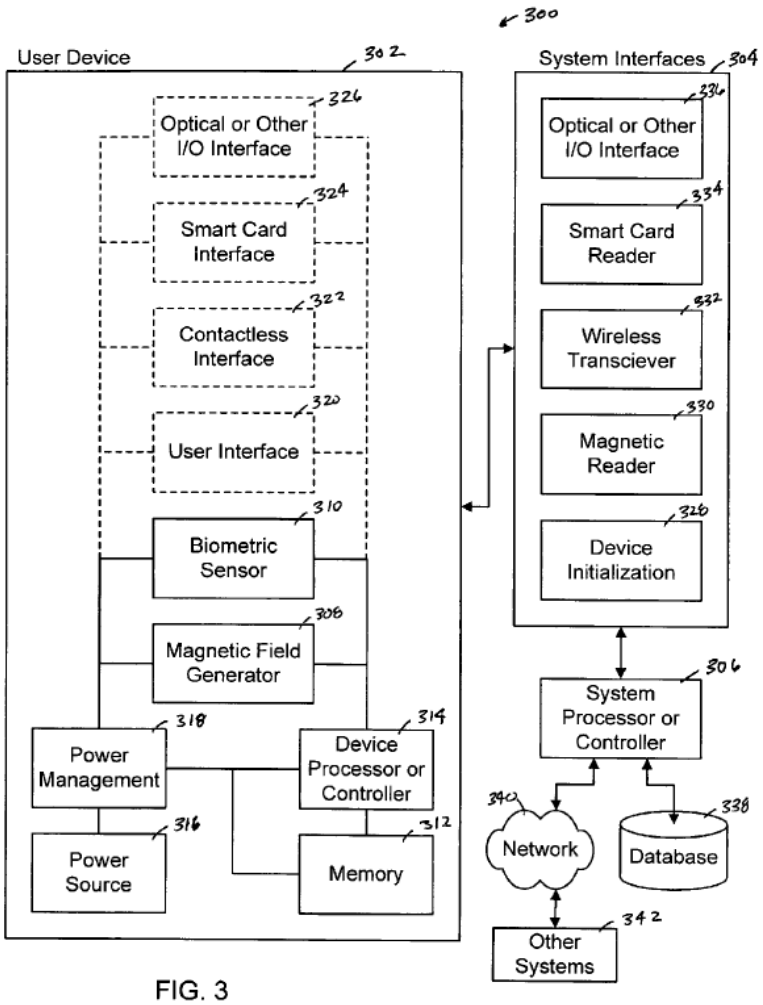


FIG. 3

- **[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."

- **[0046]:** "The components of ***the device 302 are typically disposed within or mounted on a 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***.… 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."

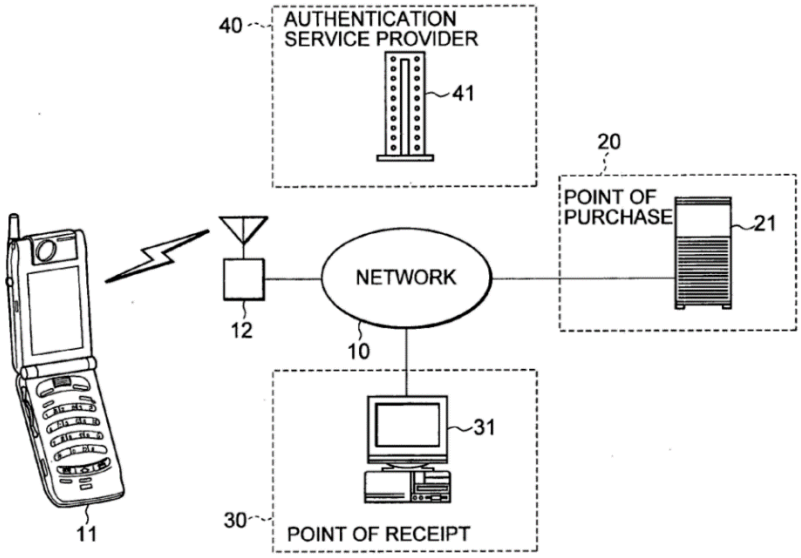
88. Doughty discloses a "personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager…." [0046]. The personal communication device includes a "user device 302" that is "disposed within or mounted on a substrate" that is "integrated into [the] personal communication device." [0040], [0046], Fig. 3. In my opinion, a person of ordinary skill in the art would have understood that a telecommunications device used as a "personal communication device" is a mobile phone.[3] Indeed, a PDA and a pager are other mobile devices. A mobile phone is used for telecommunications, and it is also personal to a user for communications.

89. **To the extent further disclosure is required, Abe discloses a mobile phone** (*e.g.*, "cellular mobile telephone 11"). *E.g.*, Abe:

- **Fig. 1:**

[3] For example, U.S. Patent No. 6,400,965 (issued June 4, 2002) discloses a "mobile telecommunication device 100" is a "cellular telephone handset." Ex. 1029, 1:14-16, Fig. 1. Moreover, U.S. Patent App. Pub. 2006/0017626 (filed July 12, 2004) discloses a "telecommunication device such as a mobile phone." Ex. 1028, Abstract.

FIG. 1



- **[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."

- **[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)."

90. Abe discloses using a "cellular mobile telephone 11" to house hardware

used to perform commercial transactions. Abe, [0092]-[0093], Fig. 1.

91. As I discussed in Section IX.A.3 above, it would have been obvious to apply Abe's teachings of a mobile phone to Doughty's telecommunications device.

b. Element [1.a]

92. **Element [1.a] recites "a memory to hold transaction data for use in a plurality of transactions."** This element is met by Doughty.

93. **Doughty discloses a memory** (*e.g.*, "memory 312") **to hold transaction data** (*e.g.*, "binary data to enable a transaction") **for use in a plurality of transactions** (*e.g.*, "transactions"). *E.g.*, Doughty:

- **Fig. 3:**

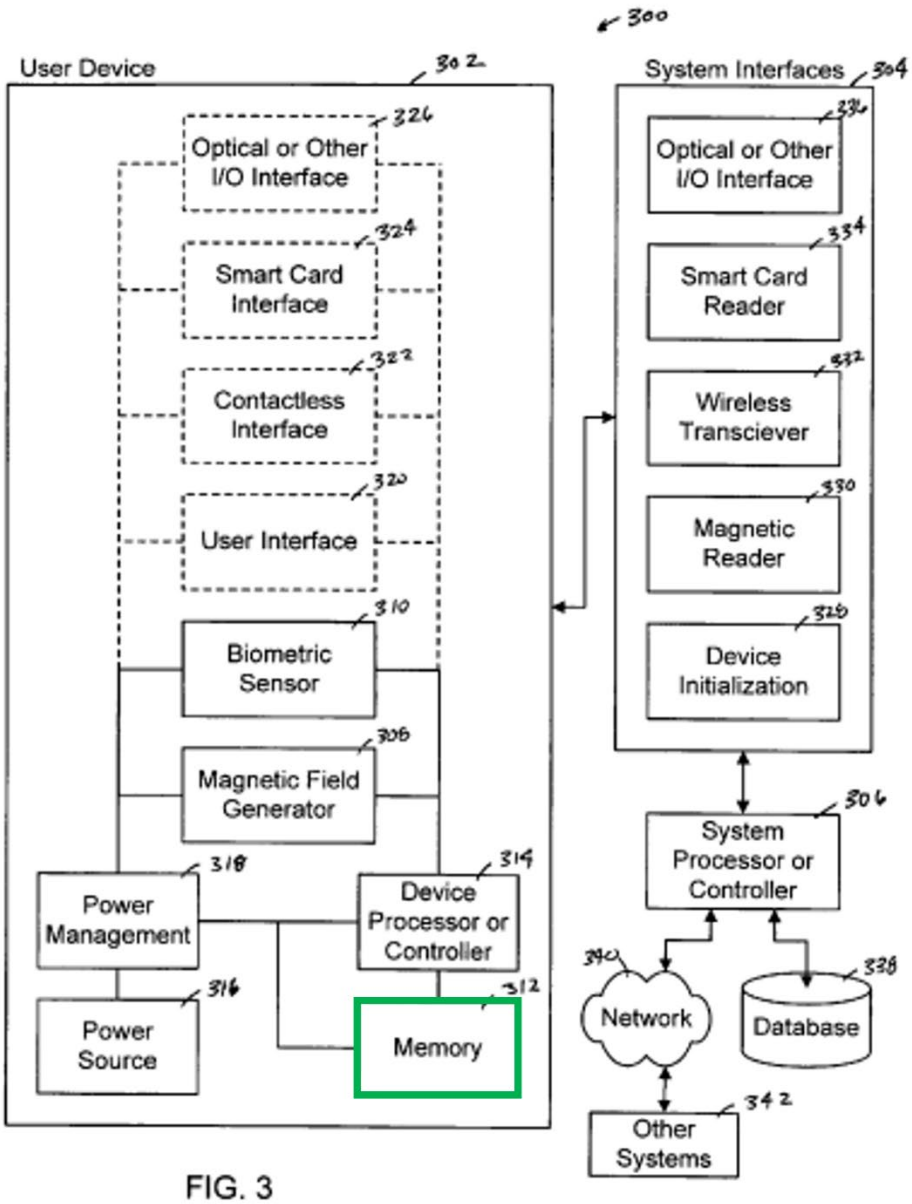
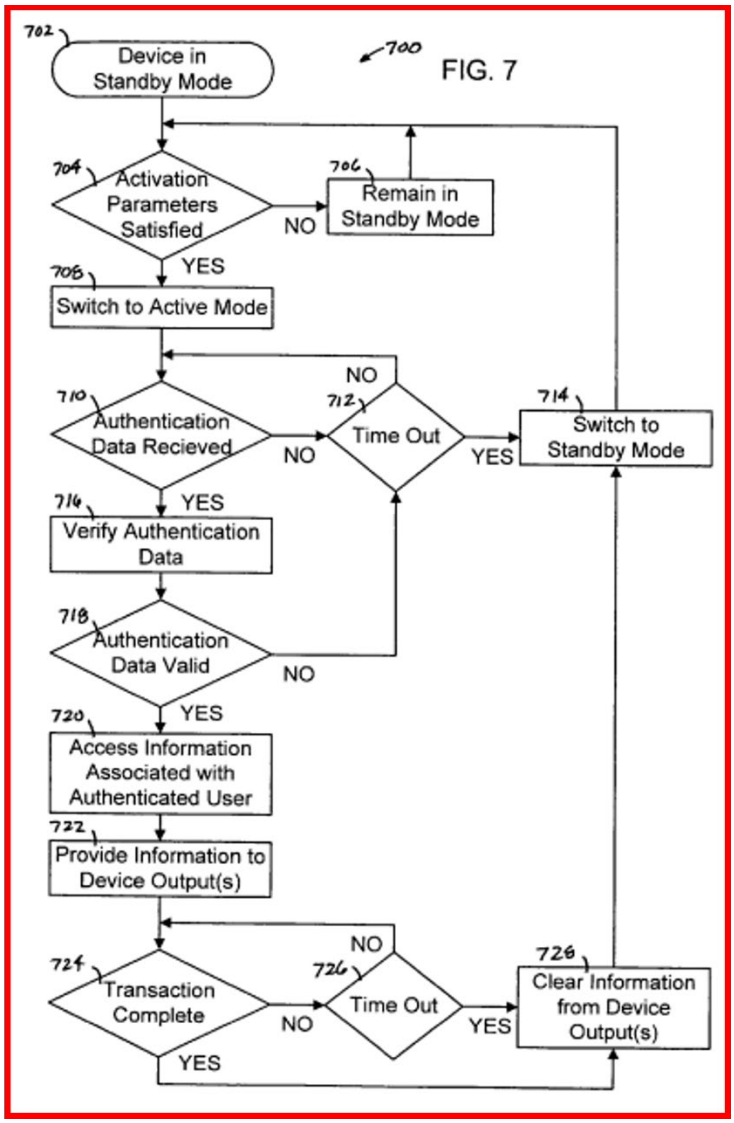

300
User Device
302
Optical or Other I/O Interface
326
Smart Card Interface
324
Contactless Interface
322
User Interface
320
Biometric Sensor
310
Magnetic Field Generator
308
Power Management
318
Power Source
316
Device Processor or Controller
314
Memory
312
System Interfaces
304
Optical or Other I/O Interface
336
Smart Card Reader
334
Wireless Transciever
332
Magnetic Reader
330
Device Initialization
328
System Processor or Controller
306
Network
340
Database
338
Other Systems
342

FIG. 3

- **Fig. 7:**

"transactions"



- **[0009]:** "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***."

- **[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."

- **[0041]:** "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***.…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."

- **[0055]:** "***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.***"

94. Doughty further discloses that the user device 302 includes "a memory 312" that stores data "for later transmission by the magnetic field generator 308." [0040], [0041], Fig. 3. The time varying magnetic field transmitted by the magnetic field generator 308 includes "binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc." [0040], [0041]. For example, the data stored in memory 312 can be read from a magnetic stripe of another device so that device 302 can replace the other device. [0040]. As such, a person of ordinary skill in the art would have understood, or at minimum found it obvious, that the binary data to enable a transaction is stored in memory 312 to advantageously allow user device 302 to be used for transactions at a later time,

after receiving the transaction data. In fact, that is the purpose of memory in a device. For example, U.S. Patent App. Pub. 2006/0168418 (filed January 1, 2005) discloses a mobile phone configured with different types of "memory to store data." Ex. 1043, [0003].

95. Doughty further discloses that the transaction data stored in memory is used for a plurality of transactions. [0041] (explaining that information from the magnetic stripe is "stored in memory 312 for later transmission by the magnetic field generator 308"). For example, the "binary data" in the magnetic signal includes persistent data that would not change from one transaction to the next, such as the "user name," "user number" and "device expiration date." [0041]. Doughty discloses that, in an embodiment, this same information is imprinted on a physical card. For example, in Figure 4A "card number 406," (corresponding to "user number") "expiration date 408" (corresponding to "device expiration date") and "the cardholder's name 410" (corresponding to "user name") are imprinted on the card.

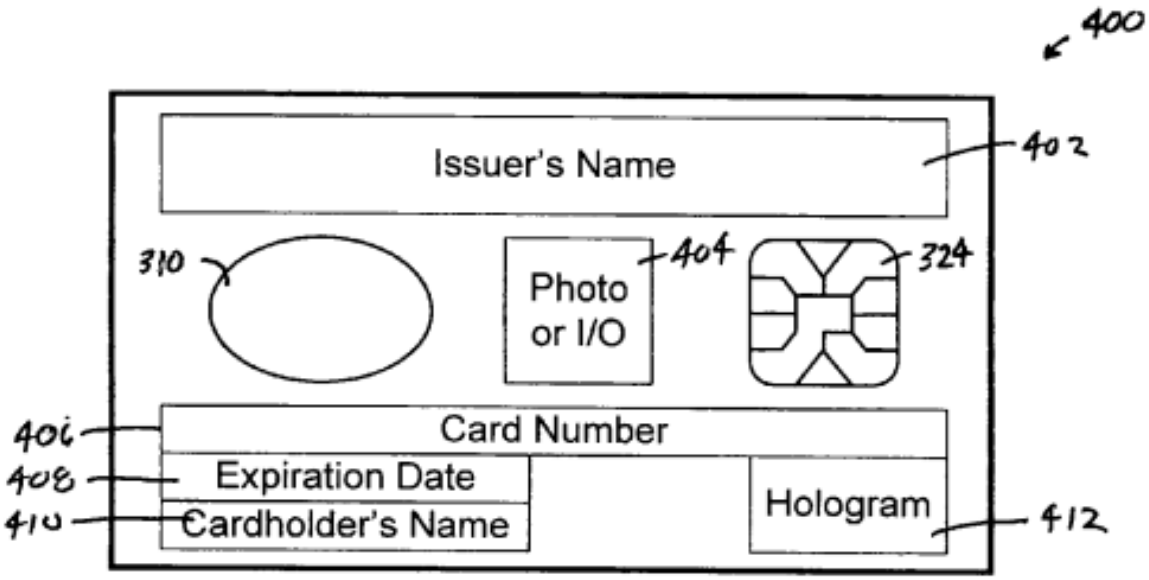


FIG. 4A

Because the information is imprinted on the card, it is not something that changes over time, and therefore the "user number," "device expiration date" and "user name" are persistent across multiple transactions. In other words, the binary data containing this information is used across multiple transactions.

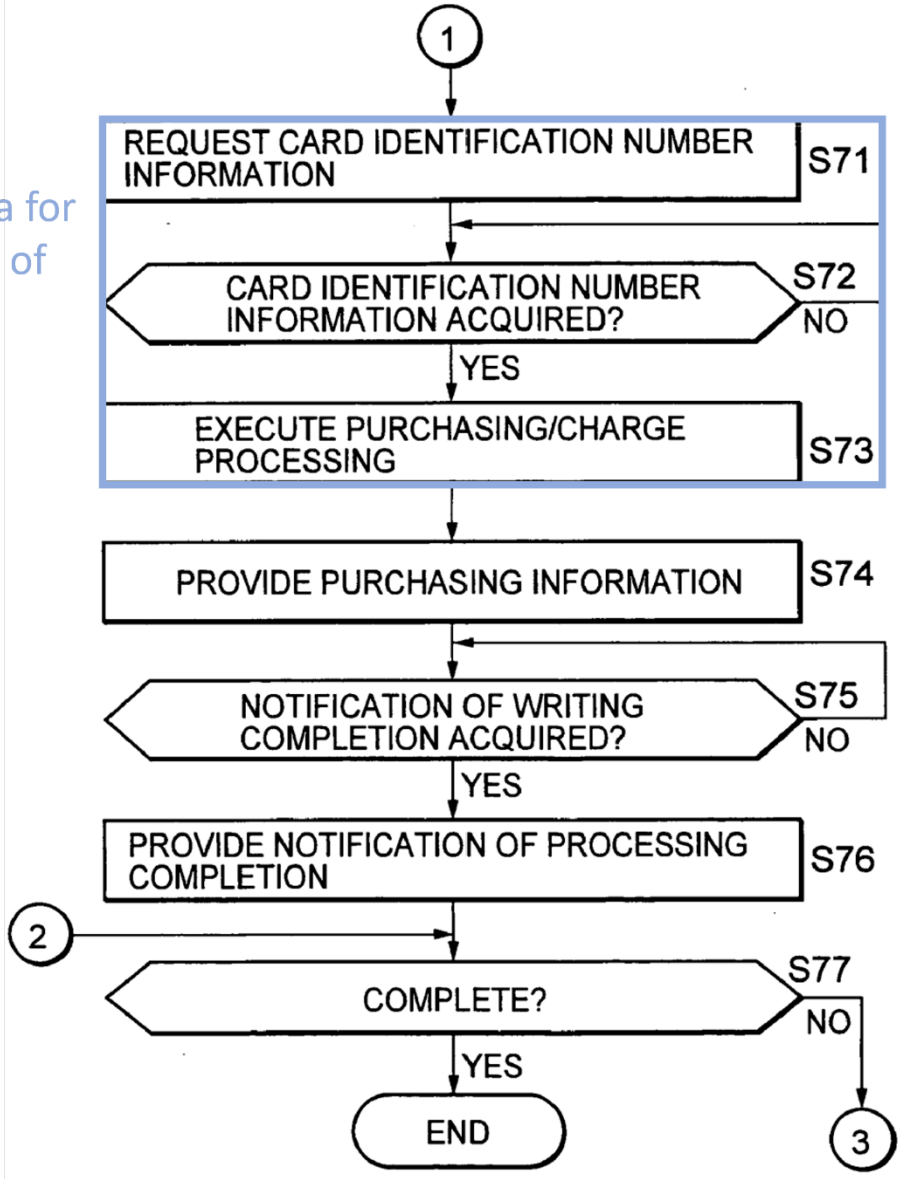
96. Moreover, Doughty discloses device 302 (using the user name, user number and device expiration date) is used across multiple transactions. For example, Figure 3 represents a system for "enabling transactions" and Figure 7 shows a flowchart for transactions in which after step 724 ("transaction complete") the device returns to standby mode for initiating a new transaction. [0040], [0055], Fig. 7.

97. For these reasons, in my opinion, a person of ordinary skill in the art would have understood, or at minimum found it obvious, that the memory is used to hold transaction data (such as "binary data to enable a transaction, such as a user name, user number, device expiration date") corresponding to a plurality of transactions in order to enable transactions using the data.

98. **To the extent further disclosure is required that the transaction data is used in a plurality of transactions, Abe discloses transaction data** (*e.g.*, "card identification number 351") **for use in a plurality of transactions** (*e.g.*, each "commercial transaction")**.** *E.g.*, Abe:

- **Fig. 17:**

FIG. 17



"transaction data for use in a plurality of transactions"

- **[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."
- **[0197]:** "*The point-of-purchase server 21* that has acquired the user trustworthiness 352 and confirmed that the user of the mobile telephone 11 is trustworthy then *makes a request to the mobile telephone 11 for the card identification number 351 allotted to the non-contact IC card 146* (arrow 376). The mobile telephone 11 then provides the card identification number 351 in response to this request."
- **[0198]:** "The point-of-purchase server 21 that has acquired the card identification number 351 then carries out processing relating to purchasing and charging, and sells the merchandise. The point-of-purchase server 21 then generates purchasing information 353 constituting information relating to the current commercial transaction and provides this to the mobile telephone 11 together with the purchasing information rewriting key 361 (arrow 378)."
- **[0245]:** "To conform with this request, ***in step S26*** of FIG. 14, the main control unit 131 of ***the mobile telephone 11 supplies card identification number information to the point-of-purchase server 21***."
- **[0246]:** "***In step S72, the CPU 201 controls the communication unit 224 so as to determine whether or not card identification number information provided by the mobile telephone 11 has been acquired***, and waits until it is determined that acquisition has taken place."

99. Abe discloses that a "card identification number 351" is obtained as part of a user registration process to identify the "non-contact IC card." [0179]. The card identification number 351 is provided to a "point-of-purchase server 31" during each "commercial transaction." [0197]-[0198], [0245]-[0246]. In this regard, when the point-of-sale server has "acquired the user trustworthiness 352 and confirmed

that the user of the mobile telephone 11 is trustworthy," the server "makes a request to the mobile telephone 11 for the card identification number 351." [0198]. Once mobile telephone 11 provides card identification number 351, the point-of-sale server "carries out processing relating to purchasing and charging, and sells the merchandise." [0198]

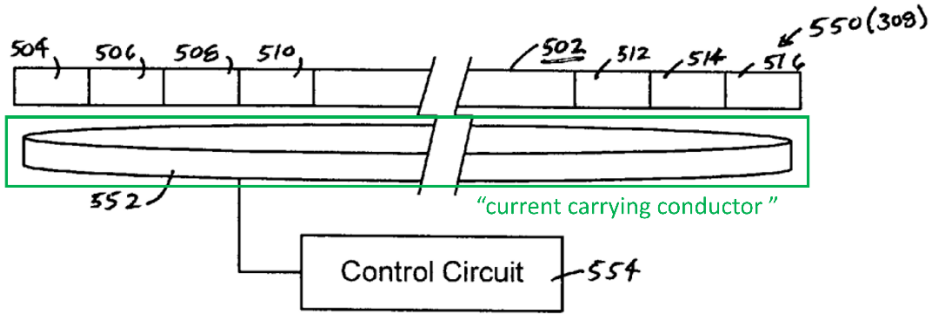
100. As I discussed in Section IX.A.3 above, it would have been obvious to apply Abe's teachings of downloading transaction data including a card identification number to Doughty's telecommunications device.

c. Element [1.b]

101. **Element [1.b] recites "a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions."** This element is met by Doughty.

102. **Doughty discloses a current carrying conductor** (*e.g.*, "inductive coil 552" of "programmable magnetic stripe 500") **capable of producing a time-varying magnetic field** (*e.g.*, "creat[ing] a time-varying magnetic signal") **that represents the transaction data** (*e.g.*, represents "binary data to enable a transaction") **in the plurality of transactions** (*e.g.*, "transactions"). *E.g.*, Doughty:

- **Fig. 5B:**



- **[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."

- **[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."***

103. See my discussion of element [1.a] above (Sections IX.A.4.b).

104. Doughty further discloses that "magnetic field generator 308" comprises "programmable magnetic stripe 550" including "inductive coil 552." [0051], Fig. 5B. Each time the device is used, "magnetic field generator 308" creates a time-varying magnetic field that "includes binary data to enable a transaction." [0041]. As I discussed above for element [1.a], the binary data for enabling transactions would be used for each of a plurality of transactions. *See* [1.a] (Section IX.A.4.b). Inductive coil 552 is a current carrying conductor that is "electrically connected" to the control circuit and is pulsed with "varying currents and current directions" to emulate a time-varying magnetic field. [0051].

d. Element [1.c]

105. **Element [1.c] recites "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."** This element is met by Doughty and Abe.

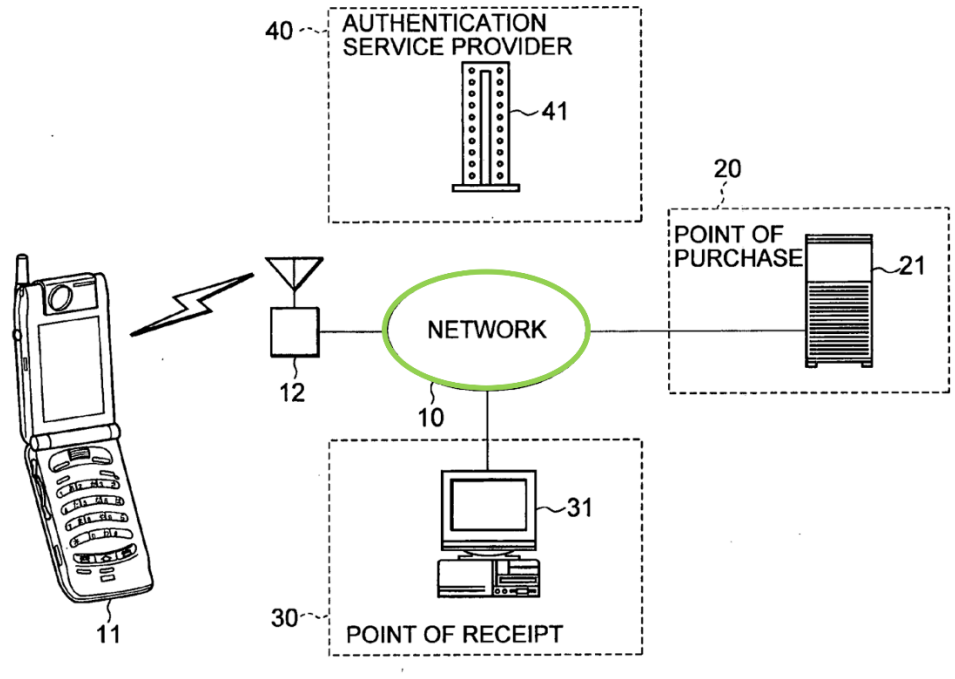
106. **Doughty discloses the mobile phone** (e.g., "telecommunications device"; *see* [1.pre] (Section IX.A.4.a)) **and the transaction data** (*e.g.,* "binary data to enable a transaction"; *see* [1.a] (Section IX.A.4.b)).

107. See my discussion of elements [1.pre] and [1.a] above (Sections IX.A.4.a-b).

108. **Abe discloses a network interface** (*e.g.*, antenna illustrated in Figure 1) **for connecting the mobile phone** (*e.g.*, "mobile telephone 11") **to a network** (*e.g.*, "network 10") **wherein one or more parts** (*e.g.*, "temporary commercial transaction information rewriting key 362" and/or "card identification number 351") **of transaction data** (*e.g.*, transaction data received from "authentication server 41") **are downloadable to the mobile phone via the network** (*e.g.*, "supplied"/ "provided" by the "authentication server 41" to the "mobile telephone 11" via "network 10"). *E.g.*, Abe:

- **Fig. 1:**

FIG. 1



- **[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)."

- **[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."

- **[0185]:** "The point-of-receipt server 31 shown in FIG. 11C stores the purchasing information rewriting key 361 described above and ***a temporary commercial transaction information rewriting key 362 constituting key information required in making, editing and deleting of temporary commercial transaction information*** described in the following in the storage unit 273."

- **[0186]:** "The temporary commercial transaction information rewriting keys 362 are distributed in advance by the authentication service provider 40 and is key information for making, editing and deleting etc. temporary commercial transaction information described in the following. ***Therefore, in order to prevent illegal duplication and falsification, it is not possible to make, edit or delete the temporary commercial transaction information without using the temporary commercial transaction information rewriting key 362.***"

- **[0187]:** "***The temporary commercial transaction information rewriting key 362 is key information for making, editing and deleting etc. temporary commercial transaction information. The temporary commercial transaction information rewriting key 362 is a kind of one-time password and is supplied to the mobile telephone 11 etc.*** while the point-of-receipt server 31 authentication server 41 generating the temporary commercial transaction information rewriting key 362 update the temporary commercial transaction information. When the temporary commercial transaction information is updated using the temporary commercial transaction information rewriting key 362 provided, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362 used. ***The point of receipt server 31 and the authentication server 41 generating the temporary commercial transaction information rewriting key 362 can supply temporary commercial transaction information rewriting keys 362 to the mobile telephone 11 any number of times."***

- **[0189]:** "***The user trustworthiness rewriting key 363 is key information for updating the user trustworthiness 352 stored in the non-contact IC card 146 of the mobile telephone 11.*** Therefore, in order to prevent illegal duplication and falsification, it is not possible to make, edit or delete the user trustworthiness 352 without using the user trustworthiness rewriting key 363."

- **[0190]:** "The user trustworthiness rewriting key 363 is key information for making, editing and deleting etc. user trustworthiness. ***The user trustworthiness rewriting key 363 is a kind of one-time password, and is supplied to the mobile telephone 11 etc. while the authentication server 41 generating the user trustworthiness rewriting key 363 is instructing updating of the user reliability.*** When user trustworthiness is updated using the user trustworthiness rewriting key 363 provided, the mobile telephone 11 deletes the user trustworthiness rewriting key 363 used. The authentication server 41 generating the user trustworthiness rewriting key 363 can supply the user trustworthiness rewriting key 363 to the mobile telephone 11 etc. any number of times."

- **[0328]:** "The main control unit 131 updated with user trustworthiness 352 stored in the non-contact IC card 146 ***then advances processing to step S181 of FIG. 26***, deletes the user trustworthiness rewriting key 363, and provides notification of completion of writing to the authentication server 41. This processing corresponds to the arrow 437 of FIG. 24."

- **[0329]:** "As described in the following, ***the authentication server 41 that has acquired the notification of completion of writing provides a temporary commercial transaction information rewriting key 362 to the mobile telephone 11***, and instructs the deletion of the temporary commercial transaction information 391 stored in the non-contact IC card 146."

- **[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.***"

109. See my discussion of element [1.a] above (Sections IX.A.4.b).

110. Abe further discloses that a "mobile telephone 11" communicates with "authentication server 41 via the network 10." [0484], Fig. 1. For example, the mobile phone 11 includes an antenna (illustrated in Figure 1) that wirelessly connects with base station 12 in network 10, thereby providing an interface to network 10. [0092].

111. Abe further discloses that mobile telephone 11 receives various transaction information from authentication server 41, including "card identification number 351" and various "rewriting key[s]" that "prevent illegal duplication and falsification." [0179], [0186]-[0187], [0189]-[0190], [0329], [0093], Fig. 24-26. For example, Abe discloses card identification number 351 is "provided via the network 10 by the authentication sever 41" to "mobile telephone 11." [0179]. In addition, Abe discloses that its mobile telephone 11 is "provided" or "supplied a temporary commercial transaction information rewriting key 362" by the "authentication server 41" to authenticate a transaction performed by the mobile telephone 11. [0187]-[0188], [0329], Fig. 24-26. The information is provided by "authentication server 41" to "mobile telephone 11" through "network 10." [0179], [0187].

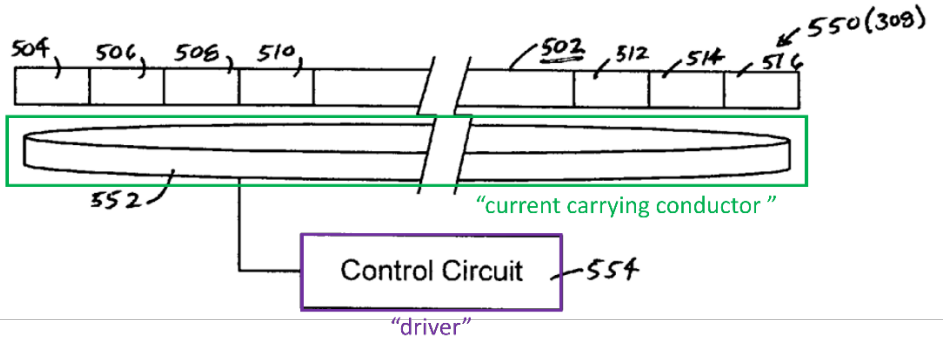
112. As I discussed in Section IX.A.3 above, a person of ordinary skill in the art would have been motivated to apply Abe's teachings of downloading transaction data from an authentication server over a network to Doughty's telecommunications device such that the downloaded transaction data is stored in the memory.

e. Element [1.d]

113. **Element [1.d] recites "a driver to excite the current carrying conductor."** This element is met by Doughty.

114. **Doughty discloses a driver** (*e.g.*, "control circuit 554") **to excite the current carrying conductor** (*e.g.*, "inductive coil 552"). *E.g.*, Doughty:

- **Fig. 5B:**



- **[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."

115. See my discussion of element [1.b] above (Sections IX.A.4.c).

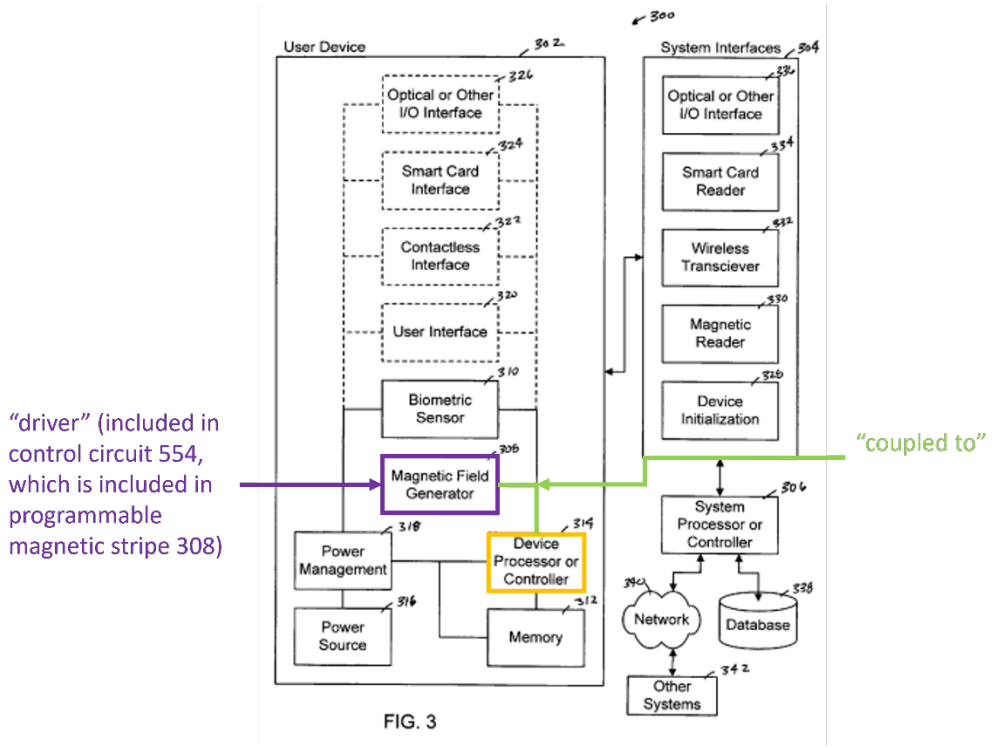
116. Doughty discloses that "inductive coil 552 is electrically connected to the control circuit 554," and that "[b]y establishing the configuration in this manner, the inductive coil 442 can be pulsed with varying currents and current directions" so as to emulate a time-varying magnetic field. [0051], Fig. 5B. In order to effect the pulsing of the inductive coil with varying currents and current directions, a person of ordinary skill in the art would have understood, or at minimum found it obvious, that the control circuit 554 is or at least includes a driver to excite the inductive coil. For example, U.S. Patent 6,670,796 (issued December 30, 2003) explains that driver circuits are used to drive current "through the inductive load" to "induce[] a larger [] current to flow through the inductive load." Ex.1036, 1:10-25, 44-46. A driver that induces such current flow by adjusting the inductive load provides the "varying currents and current directions" Doughty describes as being established through the connection of the control circuit 554 to the inductive coil 552, to the extent such detailed description is not explicitly provided by Doughty itself.

f. Element [1.e]

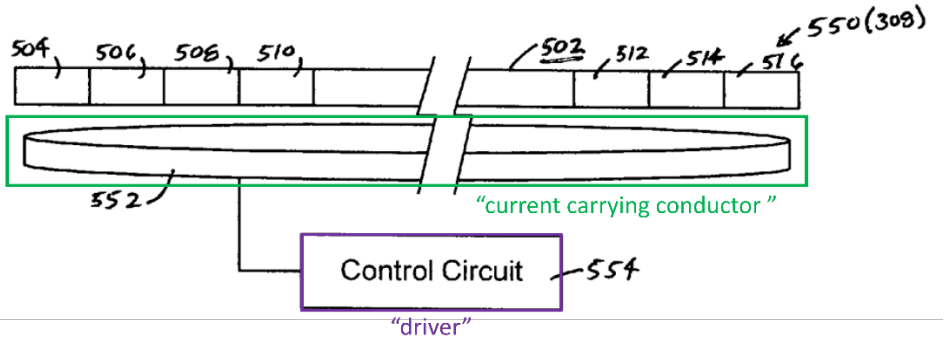
117. **Element [1.e] recites "a processor coupled to control the driver."** This element is met by Doughty.

118. **Doughty discloses a processor coupled to control the driver** (*e.g.*, "device processor or controller 314" "manage[s]" "control circuit 554"). *E.g.*, Doughty:

- **Fig. 3:**



- **Fig. 5B:**



- **[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."

- **[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).***"

119. See my discussion of element [1.d] above (Section IX.A.4.c).

120. Doughty further discloses that "device processor 314" is coupled to the driver ("control circuit 554," *see* [1d]) because the "control circuit 554" "may be integrated into the device processor 314," but need not be integrated. [0051]. In my opinion, a person of ordinary skill in the art would have understood, or at minimum found obvious, that control circuit 554 is coupled to the device processor 314 when

not integrated into the device processor 314. The purpose for integrating these components would be to reduce the area and minimize the number of connection points between two components. For example, when the components are separate, a signal line must be established across the board, with a connection at each of the control circuit 554 and device processor 314 to allow signals to be communicated between. On the other hand, when the components are integrated, there is no need to maintain connections between chips. Moreover, a functionally equivalent structure to having the control circuit 554 integrated into processor 314 would be to couple control circuit 554 and processor 314 so that they communicate with each other. The processor/controller includes "logic" that "manages" the "programmable magnetic stripes 550 (308 FIG. 3)," which "includes…a control circuit 554" ([0039], [0051]). Because the control circuit 554 drives the coils (as I explain in [1.d] in Section IX.A.4.e above), the processor 314 would manage the control circuit 554 in order to manage the overall operation of "programmable magnetic stripes 550 (308 FIG. 3)." Thus, a person of ordinary skill in the art would have understood, or at minimum found it obvious, that device processor 314 is coupled to the driver to control the driver of control circuit 554.

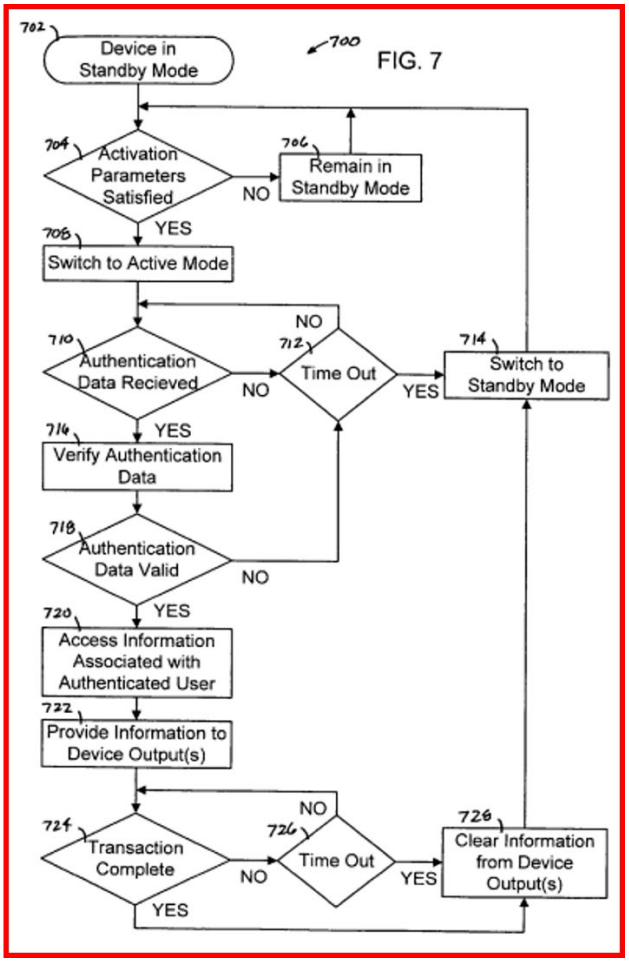
g. Claim 2

121. **Claim 2 recites "The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction."** This element is met by Doughty.

122. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Doughty discloses that the time-varying magnetic field** (*e.g.*, "time-varying magnetic signal") **represents a point-of-sale transaction** (*e.g.*, used for "any type of transaction" including "a financial transaction" or "a commercial transaction" with a "point of sale device"). *E.g.*, Doughty:

- **Fig. 7:**

"point-of-sale transaction"



- **Fig. 19:**

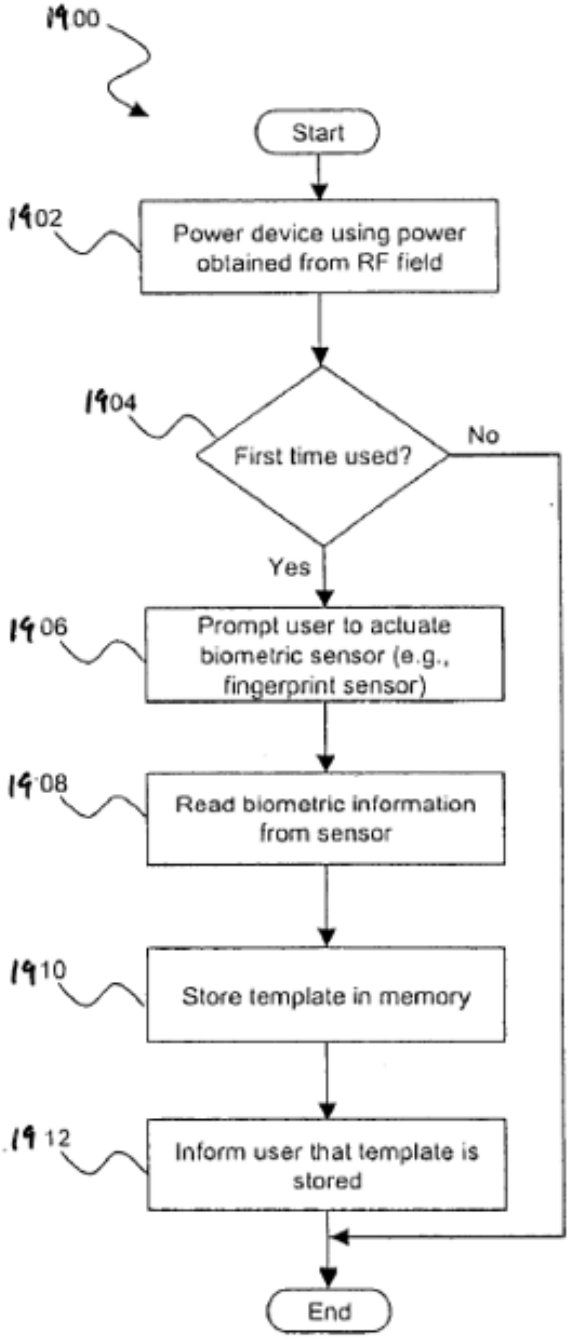
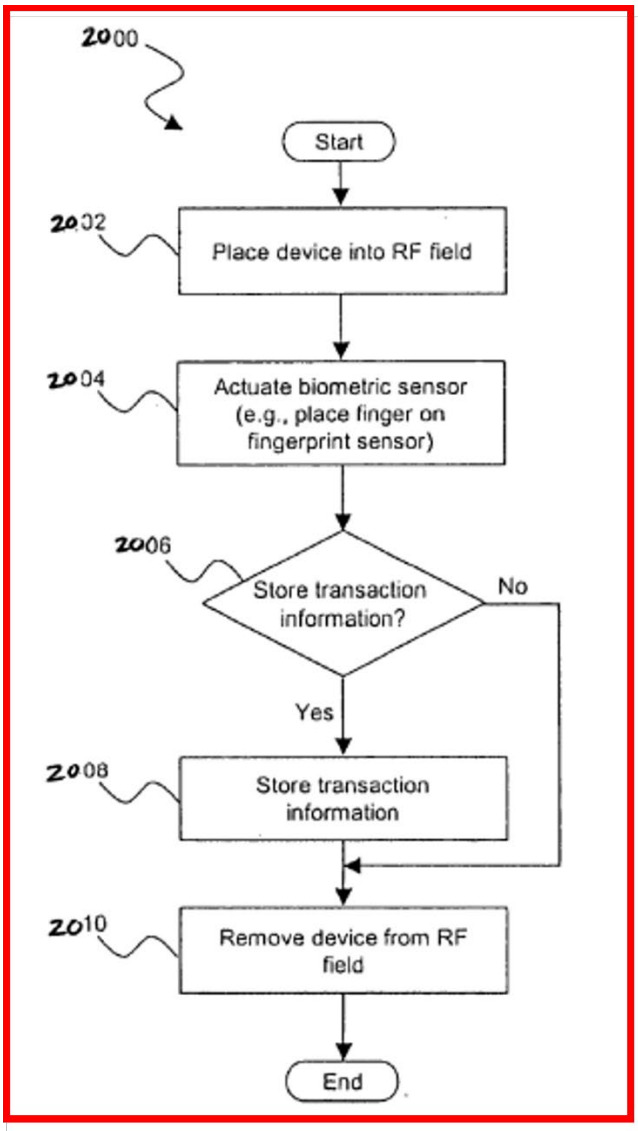


Fig. 19

- **Fig. 20:**



"point-of-sale transactions"

Fig. 20

- **[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."

- **[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."

- **[0041]:** "The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal…***the magnetic signal includes binary data to enable a transaction***, such as a ***user name, user number, device expiration date***, transaction approval/denial, etc."

- **[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."

- **[0095]:** "Referring now to FIGS. 19 and 20, in another embodiment, ***methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment***. The financial transaction environment includes making ***retail purchases*** in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions."

- **[0098]:** "Referring specifically to FIG. 19, before ***the device 800 is usable in financial transactions***, it should be initialized by the buyer/owner with the registration of a selected fingerprint pattern into secured memory of the device 800. To register a selected fingerprint, ***the device owner holds the device 800 in the RF field generated by a point of sale ("POS") device, which may be a kiosk, personal computer, cash register, or similar device.*** The RF energy from the POS device provides for the power of the device 800 and display activation in step 1902…."

- **[0099]:** "Referring specifically to FIG. 20, ***to authorize a payment transaction*** where invoice information is displayed by the POS device, ***the user of the device 800 holds the device 800 within a RF field generated by a RF reader connected to the POS device*** in step 2002. For example, the user may hold the device 810 at an approximate six inch distance from the RF reader. In step 2004, the user actuates the biometric sensor 802 (e.g., touches the fingerprint sensor with his/her finger or thumb) to effect a comparative match with his/her previously registered fingerprint securely stored in the memory of the card. A successful match effects an encrypted approval and transfer of cardholder account data to the seller's administrative account receivables processing system."

- **[0101]:** "While the preceding description shows and describes one or more embodiments, it will be understood by those skilled in the art that various changes in form and entail may be made therein without departing from the spirit and scope of the present disclosure…. Therefore, the claims should be interpreted in a broad manner, consistent with the present disclosure."

- ***See also*** **[0096]-[0097].**

123. See my discussion of element [1.b] above (Sections IX.A.4.c).

124. Doughty discloses the user device transmits a "time-varying magnetic signal" that carries "binary data to enable a transaction." [0041]. Doughty further discloses that "the device can be used to enable any type of transaction." [0054]. Doughty further discloses that "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," and specifically "a secure and flexible system for security and/or commercial transactions using credit…cards." [0038]. As such, a person of ordinary skill in the art would have understood, or at minimum found obvious, that the time-varying magnetic signal represents a point-of-sale transaction. For example, magnetic stripe readers are point-of-sale terminals used for credit cards. In this regard, U.S. Patent App. Pub. 2003/0004811 (filed March 11, 2002 and published January 2, 2003) discloses credit card transaction at "a department store or a shopping center" involves a "POS terminal" to "read[] card information for a credit card received by a shop employee." Ex. 1044, [0004]. Moreover, a person of skill in the art would have understood that using Doughty's time-varying magnetic field to perform credit card (and thus point-of-sale) transactions would reduce the number of cards a user carries around and increase security. For example, Fox explains that the integration of smartcard functionality into a mobile telephone would provide ease of use of a smartcard as well as enhanced security. Fox, 2:21-29.

125. In addition, Doughty further discloses that Figures 19 and 20 provide "methods 1900 and 2000" for "using the present disclosure in a financial transaction environment." [0095]. In describing this method, Doughty discusses specifically "device 800" as an exemplary device that can be used for the method, but a person of ordinary skill in the art would have understood that device 302 is also part of the

"present disclosure," and methods 1900 and 2000 are thus equally applicable to device 302. [0054], [0095]-[0097], [0101]. Doughty discloses that, in method 1900, "retail purchases" are made by "hold[ing] the device 800 in the RF field generated by point-of-sale ('POS') device, which may be a kiosk, personal computer, cash register, or similar device" in order "[t]o register a selected fingerprint." [0098], Fig. 19. Additionally, Doughty discloses that "device 800" is used to "authorize a payment transaction" by "hold[ing] the device 800 within a RF field generated by a RF reader connected to the POS device." [0099], Fig. 20.

126. In my opinion, to the extent it is argued that Doughty discloses method 1900 as a separate embodiment, not applicable to device 302, a person of ordinary skill in the art would have found it obvious to use Doughty's user device to perform point-of-sale transactions by communicating with a point-of-sale device to perform financial transactions using the time-varying magnetic signal. For example, a person of ordinary skill in the art would have understood that the use of device 302 for point-of-sale transactions would advantageously allow a user to conveniently purchase goods without the need to separately carry cards (e.g., credit cards) to perform those transactions. For example, by enabling the use of device 302 in a telecommunications device for point-of-sale transactions, this avoids "theft or loss" of individual cards that would otherwise need to be carried around. Fox, 2:21-29. In my opinion, a person of ordinary skill in the art would have had a reasonable

expectation of success in using the device in this manner and known such an application (yielding the claimed limitations) would predictably work and provide the expected functionality.

h. Claim 3

127. **Claim 3 recites "The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction."** This element is met by Doughty.

128. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Doughty discloses that the time-varying magnetic field** (*e.g.*, "time-varying magnetic signal") **represents an access transaction** (*e.g.*, represents an "access transaction"). *E.g.*, Doughty:

- **[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."

- **[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."

- **[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). I*n 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."

- **[0054]:** "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."

129. See my discussion of element [1.b] above (Sections IX.A.4.c).

130. Doughty further discloses the user device transmits a "time-varying magnetic signal" that carries "binary data to enable a transaction." [0041]. Doughty further discloses that "the device can be used to enable any type of transaction, such as an access transaction." [0054].

i. Claim 4

131. **Claim 4 recites "The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction."** This element is met by Doughty.

132. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Doughty discloses that the time-varying magnetic field** (*e.g.*, "time-varying magnetic signal") **represents a credit card transaction** (*e.g.*, "commercial transactions using…credit…cards"). *E.g.*, Doughty:

- **[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."

- **[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***."

- **[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). I***n 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."

- **[0054]:** "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."

- **[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.***"

133. See my discussion of element [1.b] above (Sections IX.A.4.c).

134. Doughty further discloses the user device transmits a "time-varying magnetic signal" that carries "binary data to enable a transaction." [0041]. Doughty further discloses that "the device can be used to enable any type of transaction." [0054]. Moreover, Doughty discloses that each of its interfaces—including magnetic field generator 308, which produces the time-varying magnetic field—is able to be used to perform such transactions. [0055]. Doughty further discloses that "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," and specifically "a secure and flexible system for security and/or commercial transactions using credit…cards." [0038]. Consistent with this, Doughty further discloses that the "magnetic field generator 308" is in the form of a "magnetic stripe" that transmits "a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader." [0010], [0040], [0041], [0051], Fig. 3. A credit card has a magnetic stripe. *See, e.g.*, U.S. Patent No. 5,466,919 (issued November 14, 1995) (Ex. 1032), 2:16-17, 31-32 ("On the back side of the [credit] card…there are usually located a magnetic strip[e]…containing magnetically encoded account identification."). As such, a person of ordinary skill in the art would have understood, or at minimum found obvious, that the time-varying magnetic signal represents a credit card transaction to advantageously avoid the need for a user to

carry additional cards. For example, credit cards are a commonly accepted form of payment, and by storing and communicating credit card data with a mobile device incorporating user device 302, a user can easily make purchases with credit without the need to pull out their credit card for each transaction. For example, U.S. Patent No. 4,877,947 (issued on October 31, 1989) discloses that "[t]he type of card most commonly used [for commercial transactions] is the credit card." Ex. 1030, 1:14-16. A person of ordinary skill in the art would have understood that the use of device 302 for credit card transactions would advantageously allow a user to conveniently purchase goods without the need to separately carry credit cards to perform those transactions. For example, this avoids "theft or loss" of individual cards that would otherwise need to be carried around. Fox, 2:21-29.

j. Claim 5

135. **Claim 5 recites "The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card."** This element is met by Doughty.

136. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Doughty discloses the time-varying magnetic field** (*e.g.*, "time-varying magnetic signal") **emulates a swipe of a magnetic card** (*e.g.*, "emulating data obtained from swiping a magnetic stripe card"). *E.g.*, Doughty:

- **Fig. 3:**

"the time-varying magnetic field"

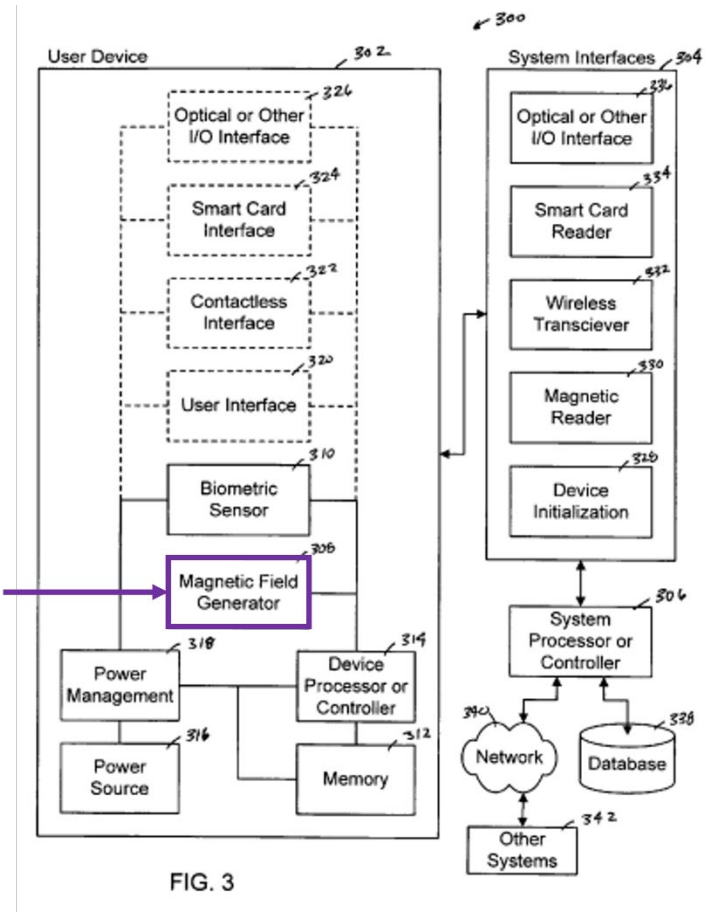


FIG. 3

- **[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…and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory.... 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."

- **[0040]:** "***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 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."

- **[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***."

- **[0051]:** "The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554….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***…. 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."

137. See my discussion of element [1.b] above (Section IX.A.4.c).

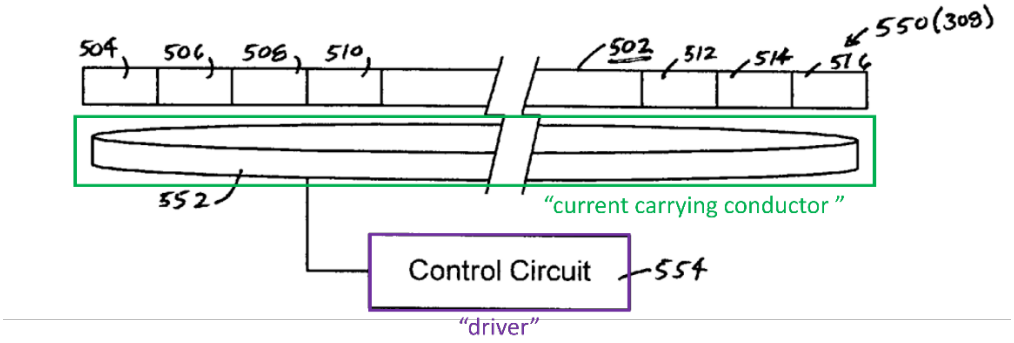
138. Doughty further discloses that the "magnetic field generator 308" is in the form of a "magnetic stripe" that transmits "a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader." [0010], [0040], [0041], [0051], Fig. 3.

k. Claim 6

139. **Claim 6 recites "The mobile phone of claim 1 wherein the driver comprises a current driver."** This element is met by Doughty.

140. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Doughty discloses that the driver comprises a current driver** (*e.g.*, driver that "pulses" the inductive coil with "varying currents and current directions"). *E.g.*, Doughty:

- **Fig. 5B:**



- **[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."

141. See my discussion of element [1.d] above (Section IX.A.4.e).

142. As I discussed above for element [1.d], Doughty discloses or renders obvious a driver (*e.g.*, "control circuit 554") to excite the current carrying conductor (e.g., "inductive coil 552"). *See* [1.d] (Section IX.A.4.e). Moreover, Doughty discloses that "inductive coil 552" is "pulsed with varying currents and current directions" so as to emulate a time-varying magnetic field. [0051], Fig. 5B. Because the current is driven through the antenna, the driver disclosed or rendered obvious as I discuss for element [1.d] is a current driver.

l. Claim 7

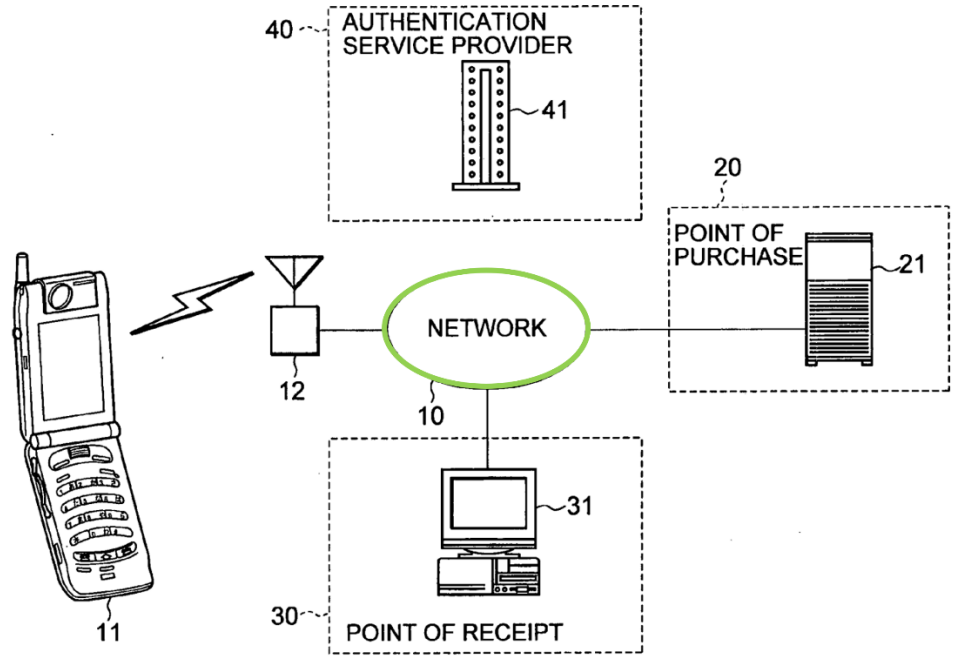
143. **Claim 7 recites "The mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network."** This element is met by Abe.

144. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Abe discloses the network** (*e.g.*, "network 10") **is a cellular network** (*e.g.*,

cellular network with "base station 12" over which "mobile telephone 11" communicates). *E.g.*, Abe:

- **Fig. 1:**

FIG. 1



- **[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***…."

145. See my discussion of element [1.c] above (Sections IX.A.4.d).

146. As I discussed in [1.c] (Section IX.A.4.d) above, Abe discloses that a "mobile telephone 11" communicates with "authentication server 41 via the network 10." [0484], Fig. 1. Moreover, Abe discloses that mobile telephone 11 communicates with the network 10 via a base station 12. [0092]. A base station is a

network component commonly used in cellular networks for use by a mobile phone to communicate data. For example, U.S. Patent App. Pub. 2006/0017626 (filed July 12, 2004) discloses that "wireless networks are increasingly being used for data communication . . . so that mobile-phone users can access Internet-based resources" and that mobile phones "communicat[e] with base stations." Ex. 1028, [0005], [0008]. As such, a person of ordinary skill in the art would have understood, or at minimum found it obvious, that the mobile telephone 11 is communicating with the authentication service provider 41 over a cellular network or a wireless local area network.

147. As I discussed in Section IX.A.3 above, a person of ordinary skill in the art would have been motivated to apply Abe's teachings of downloading transaction data to Doughty's telecommunications device.

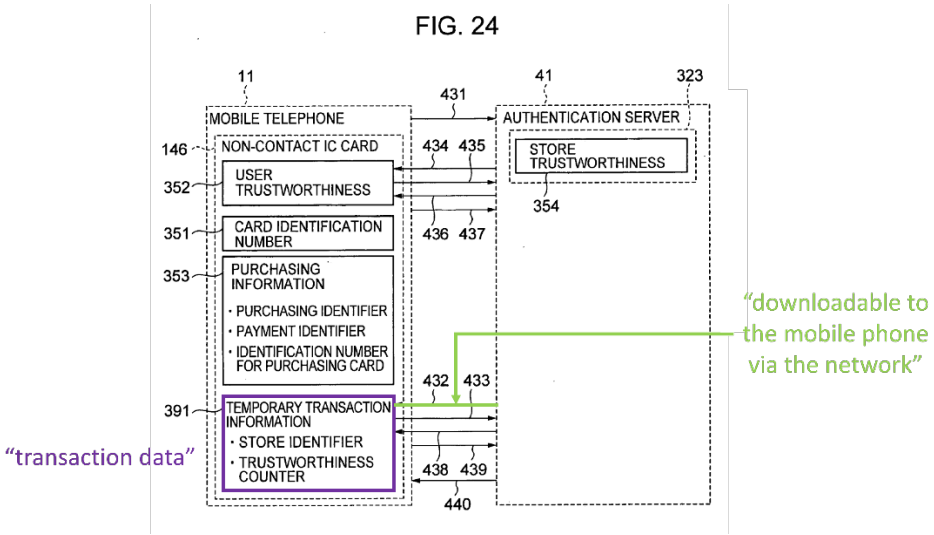
m. Claim 8

148. **Claim 8 recites "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."** This element is met by Abe.

149. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Abe discloses that downloaded transaction data** (*e.g.*, "temporary commercial transaction information rewriting key 362") **is valid for a limited number of**

transactions (*e.g.*, "one-time") **and the one or more parts** (*e.g.*, "temporary commercial transaction information rewriting key 362") **of the transaction data** (*e.g.*, transaction data received from "authentication server 41") **is downloaded periodically** (*e.g.*, supplied to the mobile telephone for each transaction). *E.g.*, Abe:

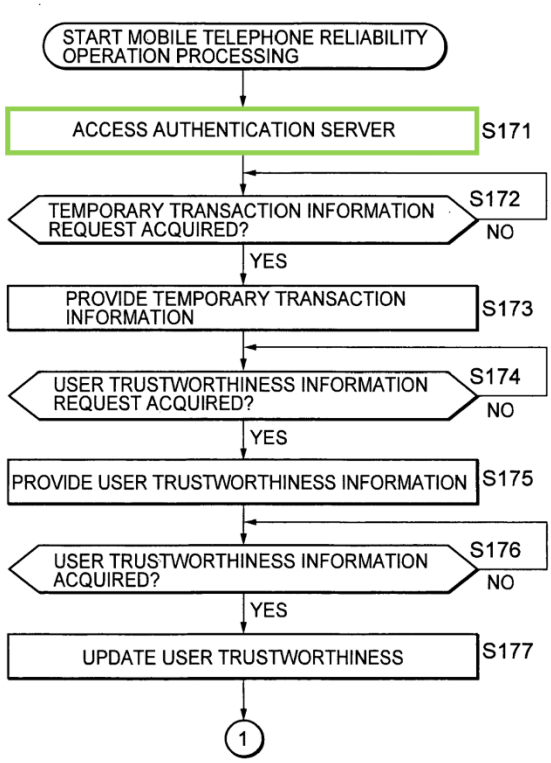
- **Fig. 24:**



- **Fig. 25:**

"transaction data are downloadable to the mobile phone via the network"

FIG. 25



- **[0187]:** "***The temporary commercial transaction information rewriting key 362 is key information for making, editing and deleting etc. temporary commercial transaction information. The temporary commercial transaction information rewriting key 362 is a kind of one-time password and is supplied to the mobile telephone 11 etc.*** while the point-of-receipt server 31 authentication server 41 generating the temporary commercial transaction information rewriting key 362 update the temporary commercial transaction information. When the temporary commercial transaction information is updated using the temporary commercial transaction information rewriting key 362 provided, the mobile telephone 11 deletes the temporary commercial transaction information rewriting key 362 used. The point of receipt server 31 and the authentication server 41 generating the temporary commercial transaction information rewriting key 362 can supply temporary commercial transaction information rewriting keys 362 to the mobile telephone 11 any number of times."

- **[0329]:** "As described in the following, ***the authentication server 41 that has acquired the notification of completion of writing provides a temporary commercial transaction information rewriting key 362 to the***

mobile telephone 11, and instructs the deletion of the temporary commercial transaction information 391 stored in the non-contact IC card 146."

- **[0330]:** "In step S182, the main control unit 131 ***determines whether or not an instruction to delete the temporary commercial transaction information has been acquired via the antenna 112, and waits until it is determined that acquisition has taken place.***"

- **[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.***"

150. See my discussion of elements [1.a] and [1.c] above (Section IX.A.4.b and d).

151. As I discussed for element [1.c] (Section IX.A.4.d) above, Abe discloses that its mobile telephone 11 downloads "temporary commercial transaction information rewriting key 362" from the "authentication server 41" to authenticate a transaction performed by the mobile telephone 11. *See* [1.c] (Section IX.A.4.d). Abe further discloses that "temporary commercial transaction rewriting key 362" is a "one-time password"[4] that is "supplied to the mobile telephone 11" during the course of a transaction and therefore is downloaded transaction data. Figs. 24-26,

[4] In my opinion, a value used for a single transaction meets the claim language requiring a "limited number of transactions." This is consistent with the '174 patent, which also discloses a single-use "single transaction account number" in which its card uses "a different number for each transaction." '174, 5:44-52.

[0187], [0329]. After temporary commercial transaction information is updated, the mobile phone deletes the temporary commercial transaction rewriting key 362. [0187], [0330]. The authentication server supplies new temporary commercial transaction rewriting keys "any number of times." [0187].

152. In my opinion, to the extent it is argued that "limited number of transactions" requires multiple transactions, it would have also been obvious to use a password for some other limited number of times (e.g., two) such that it advantageously does not need to be downloaded as often. For example, this would allow for transactions to occur even if a device did not have a network connection at the moment a transaction was being performed.

153. Because the temporary commercial transaction rewriting keys are downloaded "any number of times" for a given transaction ([0187]), such downloading would occur repeatedly, from time to time. As such, a person of ordinary skill in the art would have understood, or at minimum found it obvious, that temporary commercial transaction rewriting keys are downloaded periodically. For example, Merriam-Webster's Collegiate Dictionary (11th ed., 2003) (which I understand has been identified as Ex. 1042, and would have been accessible to a person of ordinary skill in the art, e.g., through a library or a bookstore), defines "periodically" as "from time to time." Ex. 1042, 921. This is consistent with iCashe's

infringement contentions, in which the downloading is allegedly performed from time to time.[5]

154. As I discussed in Section IX.A.3 above, a person of ordinary skill in the art would have been motivated to apply Abe's teachings of downloading temporary transaction information to Doughty's telecommunications device.

n. Claim 9

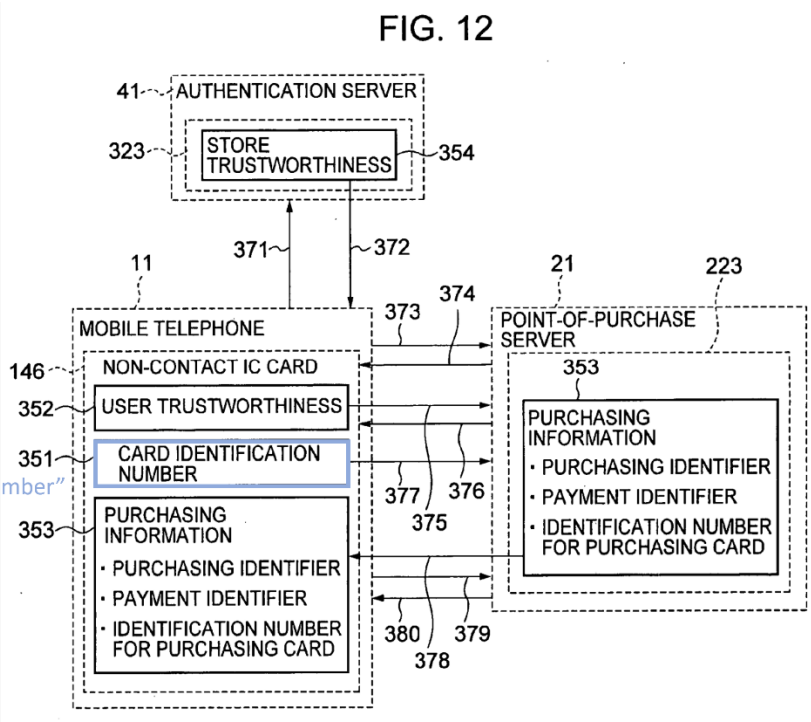
155. **Claim 9 recites "The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions."** This element is met by Abe.

156. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-f). **Abe discloses that the transaction data** (*e.g.*, transaction data received from "authentication server 41") **includes a transaction number used for each transaction of the plurality of transactions** (*e.g.*, "card identification number 351"). *E.g.*, Abe:

- **Fig. 12:**

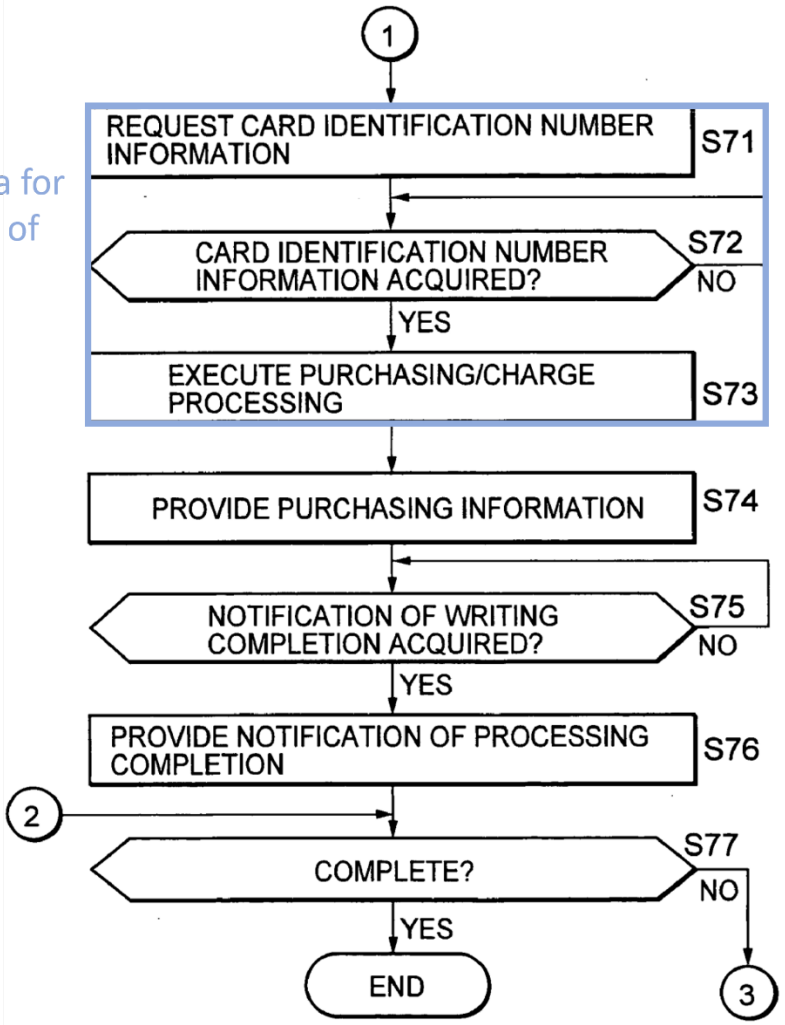
[5] Ex. 1014, Appx.H-1, 81-84.

FIG. 12


41
AUTHENTICATION SERVER
323
STORE TRUSTWORTHINESS
354
371
372
11
21
223
373
374
MOBILE TELEPHONE
POINT-OF-PURCHASE SERVER
146
NON-CONTACT IC CARD
353
352
USER TRUSTWORTHINESS
PURCHASING INFORMATION
• PURCHASING IDENTIFIER
• PAYMENT IDENTIFIER
• IDENTIFICATION NUMBER FOR PURCHASING CARD
351
CARD IDENTIFICATION NUMBER
"transaction number"
377
376
375
353
PURCHASING INFORMATION
• PURCHASING IDENTIFIER
• PAYMENT IDENTIFIER
• IDENTIFICATION NUMBER FOR PURCHASING CARD
380
379
378

- **Fig. 17:**

FIG. 17



"transaction data for use in a plurality of transactions"

- **[0197]:** "The point-of-purchase server 21 that has acquired the user trustworthiness 352 and confirmed that the user of the mobile telephone 11 is trustworthy then makes a request to the mobile telephone 11 for the card identification number 351 allotted to the non-contact IC card 146 (arrow 376). ***The mobile telephone 11 then provides the card identification number 351 in response to this request.***"

- **[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."

- **[0245]:** "To conform with this request, in step S26 of FIG. 14, the main control unit 131 of the mobile telephone 11 supplies card identification number information to the point-of-purchase server 21."

157. See my discussion of elements [1.a] and [1.c] above (Section IX.A.4.b and d).

158. Abe discloses that the "card identification number 351" included in the downloaded transaction data is provided to a point-of-purchase or point-of-receipt server during the course of a transaction. [0197], [221], [0245], Fig. 12, 17. The identification of a card number as a transaction number is consistent with iCashe's infringement contentions, in which the transaction number is allegedly "card information." Ex. 1014, Appx.H-1, 84-86. The card identification number 351 identifies the "non-contact IC card" that is performing the transaction. [0179]. Because the card identification number identifies the IC card, and is provided during each individual transaction, it is used for each of a plurality of transactions. [0179].

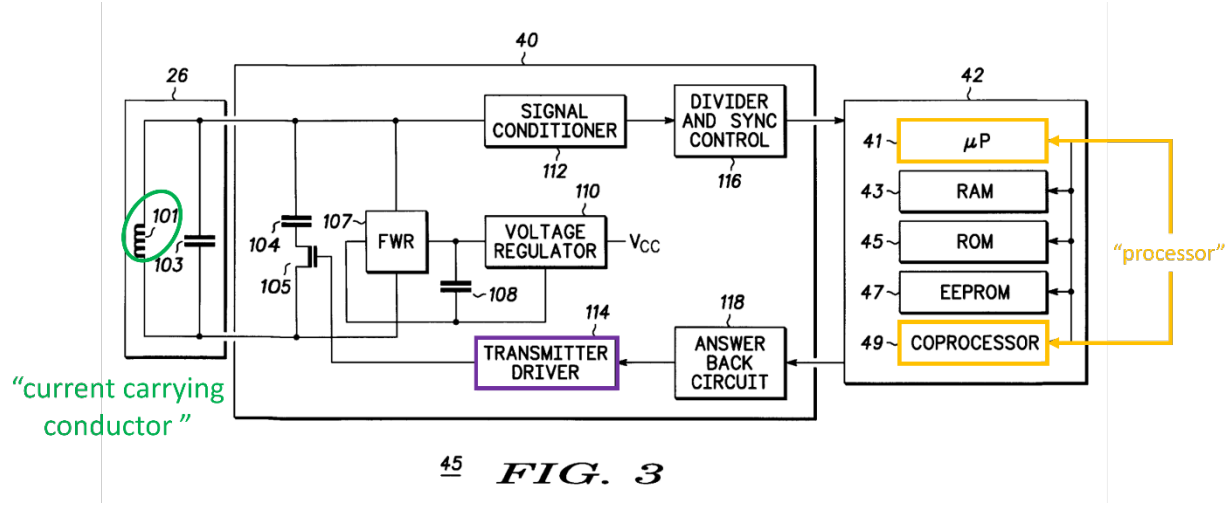
159. As I discussed in Section IX.A.3 above, a person of ordinary skill in the art would have been motivated to apply Abe's teachings of downloading transaction data to Doughty's telecommunications device.

B. Ground 2: Doughty in view of Abe and Fox (Claims 1-9)

160. To the extent it is argued that further disclosure is required of "a

(current) driver to excite the current carrying conductor," and "a processor coupled to control the driver" (elements [1.d] and [1.e], and claim 6 (Sections IX.A.4.e, f, and k)) Doughty in view of Fox renders obvious these limitations.

161. Fox discloses a "cellular telephone 10" that includes a "smartcard function" including an "RF interface" providing a "contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system." Fox, 2:10-29. The disclosed RF interface includes a "smartcard antenna 26" that "may take the form, for example, of capacitor 103 and a wire such as inductor 101." Fox, 3:49-59, Fig. 3. The current to the inductor is controlled by "transmitter driver 114" when "information is transmitted out of the smartcard." Fox, 3:49-59, Fig. 3. Smartcard logic function circuitry (including microprocessor 41 and coprocessor 49) are coupled to control the transmitter driver. Fox, 3:49-59, 4:43-56, Fig. 3.



45 FIG. 3

162. Fox discloses a current driver (*e.g.*, "transmitter driver 114") to excite the current carrying conductor (*e.g.*, "inductor 101"). *See, e.g.*, Fox, 3:49-59, Fig. 3.

For example, Fox discloses that smartcard antenna 26, which transmits a time-varying magnetic field ("transmission and reception of RF data"), includes inductor 101 and capacitor 103. Fox, 3:49-59. In order to transmit data from a smartcard, the "transmitter driver 114" adjusts the resonance frequency of capacitor 103 and inductor 101 by controlling capacitor 104 and FED switch 105. Fox at 3:49-59, Fig. 3.

163. Fox discloses a processor (e.g. "microprocessor 41" and/or "coprocessor 49") coupled to control the driver (e.g. coupled to "transmitter driver 114" as illustrated in Fig. 3 to perform "smartcard functions" via "transmitter driver 114"). *See, e.g.*, Fox, 3:49-59, Fig. 3. For example, Fox further discloses that smartcard logic function circuitry 42 (containing microprocessor 41 and coprocessor 49) controls "transmitter driver 114" to modify the resonance of inductor 101 and capacitor 103 via capacitor 104 and FED switch 105. Fox, 3:49-59. To perform this control, as illustrated in Fig. 3, microprocessor 41 and/or coprocessor 49 is coupled to transmitter driver 114 via answer back circuit 118.

164. Like Doughty and Abe, Fox is analogous art, in the same field as the '174 patent, which includes electronic devices for performing transactions, and are reasonably pertinent to alleged problems addressed by the named inventors of the '174 patent involving the use of electronic devices to securely perform transactions. Fox, 1:5-8, 2:10-29, 3:49-59, 4:43-56, Fig. 3.

165. In my opinion, a person of ordinary skill in the art would have been motivated to apply Fox's teachings of a transmitter driver that drives an inductor to Doughty's telecommunications device to excite Doughty's inductive coil 552 to produce a time-varying magnetic field as desired by Doughty. For example, while Doughty discloses that its inductive coil 552 is "pulsed with varying currents and current directions" to produce a time-varying magnetic field, it does not expressly provide details of how the coil is driven to do so, and a person of ordinary skill in the art would have looked to Fox for such implementation details. Doughty, [0051]. Fox teaches such details by disclosing a transmitter driver 114 to drive current to a smartcard antenna for emitting a magnetic field. Fox, 3:49-59, Fig. 3.

166. Further, in my opinion, a person of ordinary skill in the art would have been motivated to apply Fox's teachings of a processor to control a driver in implementing Doughty's telecommunication device (as modified by Abe's teachings) to control the production of a time-varying magnetic field. While Doughty teaches the generation of a time-varying magnetic field, Doughty does not explicitly identify what controls the disclosed varying current and current directions in inductor coil 552. Doughty, [0051]. A person of ordinary skill in the art would have looked to Fox's teachings of a processer, such as microprocessor 41 and/or coprocessor 49, to control transmitter driver 114 based on information that is to be transmitted by the antenna. Fox, 3:49-59, 4:43-56, Fig. 3.

167. A person of ordinary skill in the art would have found it straightforward and advantageous to apply Fox's teachings of a transmitter driver to drive current to an inductor and a processor to control the driver to Doughty's telecommunications device (as modified by Abe's teachings) to implement the functionality described in Doughty. In my opinion, a person of ordinary skill in the art would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

C. Grounds 3-4: Doughty in view of Abe and Dua and Doughty in view of Abe, Fox, and Dua (Claim 7)

168. In my opinion, to the extent it is argued that further disclosure is required that Abe's "network 10" is one of a cellular network or a wireless local area network, Dua discloses a network that is one of a cellular network (*e.g.*, "2.5G" or "3G") or a wireless local area network (*e.g.*, "Wi-Fi"). Dua, [0026], [0104].

169. Dua discloses a system for conducting "financial and other transactions requiring authorization" and discloses that "credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network." Dua, [0026]. Further, the system disclosed in Dua is "designed to interoperate with mobile 2.5G, 3G, and Wi-Fi networks among others." Dua, [0104]. Dua therefore discloses a system in which transaction data, such as transaction data is downloadable to a mobile phone via a cellular (2.5G or 3G) or wireless local area (Wi-Fi) network. Dua, [0026], [0104].

170. Like Doughty, Abe and Fox, Dua is analogous art, in the same field as the ’174 patent, which includes electronic devices for performing transactions, and is reasonably pertinent to alleged problems addressed by the named inventors of the ’174 patent involving the use of electronic devices to securely perform transactions using a network. Dua, [0026], [0104].

171. In my opinion, a person of ordinary skill in the art would have been motivated to apply Dua’s teachings of using a cellular or wireless local area network to the downloading of transaction data over a network as taught in Abe in implementing Doughty (as modified by Abe’s teachings and optionally modified by Fox’s teachings). For example, a person of ordinary skill in the art would have understood that cellular and wireless local area networks were common networks used for communication in order to advantageously improve the available usage of the telecommunications device. For example, U.S. Patent App. Pub. 2007/0236350 (filed January 23, 2004) discloses a “portable terminal such as a mobile phone” configured to communicate data over a “cellular network” or a “WLAN network” and perform a “payment procedure” with “point of sale equipment.” Ex. 1041, [0085], [0088], [0091], Fig. 2.

172. A person of ordinary skill in the art would have found it straightforward and advantageous to apply Dua’s teachings of a cellular or wireless area network to Abe’s disclosure of downloading transaction data over a network in implementing

Doughty (as modified by Abe's teachings and optionally modified by Fox's teachings). A person of ordinary skill in the art would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

D. Grounds 5-6: Doughty in view of Abe and Flitcroft and Doughty in view of Abe, Fox, and Flitcroft (Claim 8)

173. To the extent it is argued that further disclosure is required that downloaded transaction data is valid for a limited number of transactions and one or more parts of the transaction data is downloaded periodically, Flitcroft discloses downloaded transaction data (*e.g.*, "downloaded" "credit card numbers") is valid for a limited number of transactions (*e.g.*, "limited use") and the one or more parts of the transaction data is downloaded periodically (*e.g.*, supplied "monthly"). Flitcroft 5:5-19, 7:55-66, 10:36-51, 14:12-29.

174. Flitcroft discloses a credit card system in which "limited-use credit card numbers" are employed that can be deactivated upon a "limited-use event" such as when "the limited-use credit card is used to accrue charges which are greater than a prescribed monetary amount, which are greater than a prescribed frequency of use, and/or a combination of use frequency, individual transaction amount and total amount." Flitcroft, 5:5-19. For example, "the multiple use credit card number could be limited to, for example, five uses with a credit limit not exceeding $100 in each transaction and an aggregate credit limit not exceeding $400." Flitcroft, 7:55-66.

Additionally, the limited-use credit card can be "downloaded to a radio unit 140 (such as a portable telephone) via wireless communication." 10:48-51.

175. Flitcroft further discloses that a set of limited-use credit card numbers can be provided "in a monthly or other periodic account statement sent to the customer" and that these numbers "can be downloaded to a radio unit 140 (such as a portable telephone) via wireless communications." Flitcroft, 10:26-56.

176. Like Doughty, Abe and Fox, Flitcroft is analogous art, in the same field as the '174 patent, which includes electronic devices for performing transactions, and is reasonably pertinent to alleged problems addressed by the named inventors of the '174 patent involving the use of electronic devices to securely perform transactions using a network. Flitcroft 5:5-19; 10:26-56.

177. In my opinion, a person of ordinary skill in the art would have been motivated to apply Flitcroft's teachings of downloading limited-use credit card numbers periodically to Doughty's telecommunication device (as modified by Abe and optionally modified by Fox's teachings). A person of ordinary skill in the art would have understood that downloading limited-use credit card numbers periodically would advantageously improve the security of the telecommunications device by ensuring that the card number could not be used if it is obtained later, or that its use would be limited in time or by number of uses, thereby minimizing the

amount of money that is improperly transacted with the account number.[6] Flitcroft, 7:37-54. For example, Flitcroft discloses that limiting a credit limit to "marginally above or equal to that of the value of the transaction" will "reduce the chances of or prevent an unscrupulous trader using the credit card number to supply additional goods or services over those ordered or to increase the agreed charge." Flitcroft, 7:37-54. Flitcroft further discloses that, when the number of transactions is limited, "the fact that the number is in anybody else's hands is irrelevant." Flitcroft, 7:39-43.

178. A person of ordinary skill in the art would have found it straightforward to apply Flitcroft's teachings of limited-use credit card numbers downloaded periodically to Doughty's telecommunication device (as modified by Abe and optionally modified by Fox's teachings). A person of ordinary skill in the art would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

[6] I note that Flitcroft's "limited-use credit card numbers" are different than Abe's temporary rewriting keys in that Flitcroft's credit card numbers are used to identify a credit account, while Abe's rewriting keys are used to prevent duplication or falsification of temporary commercial transaction information. Flitcroft, 6:53-64, 10:67-11:14; Abe, [0186].

E. Grounds 7-8: Doughty in view of Abe and Bursch and Doughty in view of Abe, Fox, and Bursch (Claim 9)

179. To the extent it is argued that further disclosure is required of a transaction number used for each of the plurality of transactions, Bursch discloses a transaction number (*e.g.*, "single-use, transaction number"). Bursch Abstract, 2:22-32, 2:65-67, 5:53-60.

180. Bursch discloses methods for producing and applications for using "single-use, transaction numbers" to "make purchases of good and services." *See, e.g.*, Bursch, Abstract, 2:22-32, 2:65-67, 5:53-60, 5:61-65, 7:55-8:3. These transaction numbers are "single-use" because they are "only valid for a single transaction." Bursch, Abstract, 2:22-32, 5:53-60, 5:61-65. The "single-use transaction numbers" may be generated using a "transaction number generator" that "may be implemented in handheld devices" including "for example, a PDA or a telephone." Burch, 7:50-54, 3:61-62.

181. Like Doughty, Abe, and Fox, Bursch is analogous art, in the same field as the '174 patent, which includes electronic devices for performing transactions, and is reasonably pertinent to alleged problems addressed by the named inventors of the '174 patent involving the use of electronic devices to securely perform transactions using a network. '174 patent, 1:48-67, 5:29-37, 6:9-18, 12:41-64; Doughty [0002], [0003], [0004], [0007], [0008], [0038], [0040], [0041], [0046]; Abe Abstract, [0001], [0002], [0003], [0004], [0005], [0006], [0179], [0183], [0509],

[0510], [0511], [0512], [0513]; Bursch, 1:6-9, 1:13-2:18, 2:22-44, 5:66-6:10, 6:26-52, 7:50-54. For example, both Doughty and Bursch disclose methods of performing secure financial transactions in mobile devices. Doughty [0040], [0041], Fig. 3; Bursch 5:53-60, 5:60-65, 7:50-54.

182. In my opinion, a person of ordinary skill in the art would have been motivated to apply Bursch's teachings of single-use transaction numbers to Doughty's user device (as modified by Abe and optionally modified by Fox's teachings) such that the single-use transaction number would be transmitted with **Doughty's** disclosed binary data to enable a transaction in order to advantageously improve the security of its financial transactions. For example, Doughty explains that its user device is intended to "improve the effectiveness and security of a given card or device." Doughty, [0003], [0004], [0008]. Bursch discloses that its transaction numbers improve security because they "can be generated just prior to being used," which "minimiz[es] the amount of time during which they can be lost of stolen." Bursch, Abstract, 5:61-65. Further, the transaction numbers are secure because they are generated using "encryption technology" that makes it "very difficult if not impossible to predict what the next transaction number generated will be." Bursch, Abstract. The transaction numbers are "unique to [each] user" and can be "validated or authenticated by an issuing institution" or other party. Bursch, Abstract. Further, Bursch discloses that the use of "single-use transaction numbers"

further improves security by allowing for a "variety of invalidation actions" to be initiated if "the expected transaction number does not match the transaction number received. Bursch, 4:50-54.

183. A person of ordinary skill in the art would have found it straightforward and advantageous to apply Bursch's single-use transaction numbers teachings to Doughty's telecommunications device (as modified by Abe and optionally modified by Fox's teachings) and would have known such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

X. SECONDARY CONSIDERATIONS

184. The Challenged Claims of the '174 patent are rendered obvious by the grounds I discussed above. In my opinion, the strength of the obviousness grounds that I discuss above cannot be overcome by any alleged objective indicia.

185. There is no evidence in the '174 patent's prosecution history or elsewhere supporting any secondary considerations arguments, or evidence of any nexus to any particular claim of the '174 patent. *See generally* '174 File History. As demonstrated by the prior art I discussed above, any purported solutions to problems or unexpected results in the '174 patent were already well known. *Id.*

186. To the extent that Patent Owner contends that the accused products in the pending district court case are infringing and thus demonstrate commercial success, such allegations would not provide any indication that the Claims are non-

obvious. Such assertions would not demonstrate that Samsung's products infringe, let alone show any nexus between any alleged commercial success and the Claims, or that any alleged success is due to an allegedly claimed component instead of the many unclaimed features of the accused products.

187. To the extent Patent Owner asserts the existence of any additional secondary considerations in its responses, or presents additional evidence or arguments, I reserve my right to address any such evidence.

XI. CONCLUSION

188. In summary, I have concluded that the Challenged Claims are rendered obvious over the prior art references as discussed above. Specifically, in my opinion, for at least the reasons above, the Challenged Claims of the '174 patent obvious.

189. To the extent it is argued that any further disclosure is required for an element in the Challenged Claims that I have identified as being disclosed, a person of ordinary skill in the art would certainly have found that element obvious to include based on the sample explicit disclosure or inherent disclosures and analysis I have identified above.

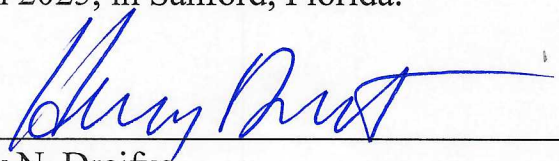
190. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me.

191. In signing this declaration, I recognize that the declaration will be filed

as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

192. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

193. Executed this 11th day of March 2025, in Sanford, Florida.



Henry N. Dreifus

APPENDIX A

HENRY N. DREIFUS

Chief Executive Officer
Dreifus Associates, Ltd., Inc.
1899 Lake Markham Preserve Trail
Sanford, Florida 32771
(407) 585 2840 telephone * (407) 256 8967 mobile
Henry.Dreifus@Dreifus.com

BACKGROUND

Founder and Managing Director of Dreifus Associates, Limited (DAL), an Identity technology and Personnel Assurance solutions development and integration organization. Accomplishments include holding a key patent on advanced smart cards and portable electronic transaction technology. Mr. Dreifus has more than 25 years of experience in the field including extensive experience on strategic engagements using all types of card technologies ranging from magnetic, optical and intelligent (smart card) for financial, security, consumer marketing and information applications. He is a recognized world expert in the card technology industry and provides vision for the application of enabling technologies to solve business problems. He is also a founding director of the Smart Card Industry Association and is a delegate to the International Standards Organization (ISO) and the American National Standards Institute (ANSI) developing worldwide standards for the smart card.

CURRENT BOARD POSITIONS

Wolverine Industries (formerly Wolverine Tube), Vice Chairman.

Institute for State Effectiveness (Non-profit).

Keel Digital.

Lucinity (Board Observer).

Preceptor Capital (Co-founder/Managing Partner).

Blokko (Advisory).

Bluerock Systems (Advisory).

FORMER BOARD POSITIONS

United States Department of Defense Business Board.

Domenici-Rivlin Debt Reduction Task Force, Senior Subject Matter Advisor.

Updated December 2024.

RDM Corporation (TSE: RC), sold to Deluxe Corporation (NYSE: DLX).

TelaDoc Corporation (NYSE: TDOC).

One Networks Corporation (d/b/a FINEXIO).

Viewzi Corporation.

Empire Financial Holding Corp. (AMEX: EFH).

Tranzfinity Corporation (Advisory).

Micromem Corporation (TSX, NASDAQ OTC: MMTIF).

Executives Without Borders (Advisory, Non-Profit).

Solution Design Group (Advisory).

Hypercom (Advisory) sold to Equinox.

AudeSi Technologies, sold to Wind River.

PROFESSIONAL EXPERIENCE

1991-Current

Founder/CEO of DAL, a specialty innovative consultancy and solutions integration company specializing in innovative low-cost solutions. Key clients include:

ZWIPE – Support development and design team for next generation integrated biometric enabled financial transaction card solutions for payment and ID access control applications. Scope includes development of intellectual property.

eBay / STUBHUB – Subject matter advisor supporting intellectual property and patent portfolio protection for e-commerce.

VALID SA – Supporting the leading Brazilian Electronic Identification and Security Solutions provider entry into the US market to a combined acquisitive and organic growth pathway. Drove the successful accretive acquisition of 9 US operating companies into the VALID SA portfolio, senior advisor – global strategy development.

VERAYO CORP – Supporting the development of next generation identification and security solutions based on uniquely identifiable features of semiconductors (Siometrics) and other advanced applications.

STATE OF INDIANA – Development of requirements, drafting and issuing/management for a statewide RFP for a debit/stored-value cashless electronic benefits distribution system for all state citizens. Program supports delivery of over $1 billion in benefits for unemployment, child support and other services.

SIEMENS AG – Leading the development team for accelerated product introduction of next generation capabilities for Infrastructure Logistics and Mobility business units. Work includes the product development, market identification and innovation including go-to-market execution of business and early-sale strategies with focus on US market introduction of global solutions.

OFFICE OF THE PRIME MINISTER, GOVERNMENT OF JAMAICA – Project executive leading best practices team of technical, data security, business processes improvement to architect and design a National Identification System to improve the identity assurance of all Jamaicans. The project includes assessments of key Identification processes including Passport, Civil Registries, Immigration/Naturalization and other stakeholders.

ORGANIZATION OF EASTERN CARRIBBEAN STATES (OECS) – Supporting the governments of the Commonwealth of Dominica, St. Lucia, St. Vincent and the Grenadines and Grenada for the needs assessment and design of a multi-application, multi-national citizen services card to include the delivery electronic government services, border crossing and other applications in support of the development of an Economic Union of the Island nations under a World Bank funded E-government/regional integration initiative.

MICROMEM CORPORATION – Lead strategic review of emerging nano-technology effort to perfect high-density magnetic memory and nano-senor arrays for large scale applications. Developed and refined market analysis pathways and initial channel partners. Our team is providing ongoing support the Board of Directors and the Technology committee in directing investment and initial product/market segmentation.

INTERNATIONAL POS MANUFACTURER – Developed next generation strategy and direction for the evolution of point-of-sale transaction card industry.

VISA USA/VISA INTERNATIONAL – Expert smart card witness in Department of Justice antitrust lawsuit. The team developed and provided smart card innovation and deployment expert testimony in the antitrust lawsuit in the United States.

DEPARTMENT OF VETERANS AFFAIRS – Lead team effort for the Secretary of the DVA to develop the VA into a Model Agency building a "Gold Standard" for data privacy and information protection after the May 2006 loss of a laptop containing all Veterans and Active-Duty Military personal information. Our team directly supported the Cabinet Secretary and the senior leadership team in building and implementing a best-practice sustainable outcome.

INTERNATIONAL BANK CARD COMPANY – Supported the market research and development and license distribution of an electronic purse system for selected markets. Defined market and commercial relationships and developed business agreements.

ETI S.A. – Reviewed national framework/strategy for the **Republic of Chile** for rollout of an enhanced smart card identification and access program for the country's banks and national telecom operator (CTC) for Chile.

SULTANATE OF OMAN – Provided third party independent review of the proposed smart card based national identification card being administered by the Royal Oman Police. Evaluated the proposed solutions and provided guidance/recommendations for implementation.

VIISAGE TECHNOLOGIES, INC. – Supported development of overall ID protection strategy and business enabling. Evaluated and developed market-enabling scenarios.

FUJI PHOTO FILM CORPORATION – Developed baseline strategy for entry into the ID management.

THESEUS LOGIC – Developed market entry strategy for next generation "clockless" microprocessors and security logic for smart card and advanced credentials for the identification markets.

INTERNATIONAL TRANSACTION CARD COMPANY – Developed market strategy for next step card technology platform and business approach for multi-function/multi-application card programs.

UNITED STATES DEPARTMENT OF DEFENSE – Numerous Projects including:

- Project advisor for Study Committee, United States Department of Defense, Office of the Secretary of Defense for advanced identification cards and technologies (AIT).
- Project manager for development of US Navy smart card baseline study for deployment of smart cards for multiple applications in the US DoD.
- Office of Secretary of Defense Advisor to Senior Steering Group (SSG) for policy and planning (including appropriations, budgeting, cost/evaluation) for DOD implementation of smart cards.
- Defense Manpower Data Center (DMDC) project manager to evaluate implementation strategies for smart card issuance and life-cycle management for smart cards for uniform, civilian and contractor personnel.
- Department of Defense – principal architect for the Common Access Card (CAC).
- US Navy Chief Information Officer (CIO) planning and strategy development for enabling smart card for use as secure token for public key infrastructure (PKI).
- Strategy and development of new next generation social media tools and technologies for non-kinetic constructive engagement.

WESTERN GOVERNORS' ASSOCATION (WGA) HEALTH PASSPORT PROJECT – Developed smart card-based health passport multi-application system for management of health and entitlement benefits for Wyoming, Nevada and Montana. System supports immunization, WIC, Food Stamp, head start and other programs.

INTERNATIONAL CREDIT CARD ASSOCIATION – Project support to establish business economics, technical pathways and strategy to introduce chip-based credit cards to member-owned association of banks and financial institutions. Developed, reviewed and supported technical and business requirements for introduction of chip cards for credit card and other value-added applications for world markets for board-level go/no-go decision.

NAVIGY – Performed independent market research study to evaluate the feasibility of new transactional methods for the health insurance/claims processing industry. Navigy is a joint-venture development arm of the Blue Cross federated state associations.

EASTMAN KODAK COMPANY – Explored business strategy/development of access security identification technology and integration into card authentication products.

INTERNATIONAL SECURITY ACCESS CARD AND SYSTEM MANUFACTURER – Developed business model and strategy/roadmap for access card technology including outsourcing options. Planning and implementation of road map for next-generation access card technology for tiered site security/access control applications including multi-application card services.

MULTINATIONAL CHIP CARD IC MANUFACTURER – Developed market research and demand estimates by industry for USA smart card requirements. Constructed card adoption models based on industry triggers by market segment. Provided detailed market potential estimates by major markets.

RAND MCNALLY CORPORATION – Developed market research and strategy for building next-generation products for DocuSystems Group, the media supplier for the airline and transportation industries. Team provided project resource planning and management oversight to new generation product line.

NATIONAL BANKING GROUP & NATIONAL TELEPHONE COMPANY – (Numerous projects) Developed national electronic commerce platform and implementation strategy for supporting electronic transactions based on smart card technology. Developed scenarios and planning to integrate existing card platforms into the national platform road map.

NORTHERN TELECOM, LTD. – (Numerous assignments) Ongoing project efforts for entry into advanced card-enabled business including next-generation public telephones (payphones), Internet opportunities, competitive analysis and market research.

NATIONAL GOVERNMENT INTER-BANKING ORGANIZATION – Advisor to executive management of the seven primary banks and monetary authority to study the feasibility and implementation of a multi-services common stored value/benefit card country-wide. Project involved the review of alternative technologies and systems, with particular attention to fraud and security procedures. System design and pilot development for pre-payment cards to be used and accepted as electronic money throughout the country.

MEDICAL SOFTWARE COMPANY – Project advisor for development of a card based electronic medical record for long-term management and tracking for patients. Pilot project involved heart transplant patients and individuals who receive medical implants (pacemakers, heart valves, artificial limbs, and other critical medical devices). Scope of project included development of the card strategy, technology selection and supplier selection.

INTERNATIONAL BANK CARD TRANSACTION PROCESSING COMPANY – Strategy and market development consultants to develop additional market share and next-generation products. Scope covers the SVC "chip-card" electronic purse application along with enhanced electronic money services.

MAJOR TELEPHONE OPERATING COMPANY – Supported the development of the market and business case for advanced card project. Built the business model and provided competitive and strategy support for venture.

DUTCH POST, TELEPHONE, & TELEGRAPH (PTT Post) – Business advisor to senior leadership team to privatize a major European PTT. Provided support in development and implementation of the strategic, competitive and tactical utilization of key assets including subscriber services. Project also focused the Postal other non-telecommunications uses and services of the capabilities and infrastructure.

MAJOR TELECOMMUNICATIONS EQUIPMENT MANUFACTURER – (Numerous projects) Project director to develop and install a credit card and smart card-based pay telephone including the infrastructure systems software, management and control procedures and security procedures. System design included the development of central office management and monitoring equipment, processes and procedures. The team explored development and market feasibility assessment of web-based access products (versus dial-tone based products).

MAJOR CARD MANUFACTURER – Advisor to the senior management on the strategy and pathways to develop new card-based products. The team is currently providing ongoing market assessment and market research on developing markets and applications.

EQUIPMENT MANUFACTURER – Project leader to develop a new set of products for the development and manufacturing of embedded smart card-based equipment for the professional, consumer and retail markets.

INTERNATIONAL CARD ASSOCIATION – Market readiness assessment of infrastructure to deploy and convert to smart cards from magnetic stripe cards. Studied feasibility and industry readiness and steps required to convert to smart card-based transactions.

MAJOR MULTINATIONAL FINANCIAL INSTITUTION – Card technology advisor for the development of an off-line secure corporate-treasury authorization system using advanced electronic cards. The project team determined alternative scenarios, economics and technology selection.

SIEMENS AG, INFINEON TECHNOLOGIES – Project director for market research and development of next-generation IC technology for chip cards. Project developed market research and forecasting for current and future generation applications. Developed focus group reviews for assessing product features, costs, capabilities and application requirements. Markets included set top box/conditional access, identification and security, telecommunications, banking, healthcare and government/defense.

OKI ELECTRIC COMPANY, LIMITED – Project advisor developing entry scenarios for portable electronic transaction systems. Development included work on electronic wallet and other hand-held portable delivery systems for electronic purse cards and other applications.

REMOTE MEMORY TELEPHONE CARD PROVIDER – Project consultant to establish and review business case for remote 1-800 memory telephone long-distance calling services. Developed and reviewed business case economics, systems, tariff and legal aspects as well as formulated growth and alliance plans.

COMMONWEALTH SECURITIES, INC. – Due diligence and market research to establish market potential and forecasts for pre-payment card utilization for Americas (North, Central and South) and Europe (East and West).

1988-1991

As the manager of the worldwide card technology practice for Andersen Consulting (now Accenture), Mr. Dreifus established and directed the worldwide Advanced Card Systems consultancy, developed a partnership-wide training program for designing and building systems based on advanced card technologies. Practice covered all card technologies from magnetic stripe, optical memory card, integrated circuit (smart) through radio frequency identification (RFID) cards.

Projects and clients included:

STATE OF WYOMING EBT FEASIBILITY STUDY – Project director for a study to explore the feasibility of using electronic benefit transfer (EBT) technology in the following programs:

- Aid for Dependent Children (AFDC)
- Women, Infants and Children (WIC)
- Food Stamps
- Medicaid Eligibility (Title XIX)

The project objective determined the viability of combining all programs onto a single information card.

MAJOR OVERSEAS BANK – Technical manager for the development of an off-line multi-services banking product to be launched Q4 '91.

MAJOR FINANCIAL INSTITUTION – Advisory manager for the development of an innovative smart card based commercial payment system.

ASIA/PACIFIC NATIONAL GOVERNMENT – Advisory manager to cabinet committee for the evaluation of alternative distribution methods for social welfare, health and other services through advanced technologies.

EUROPEAN GOVERNMENT DEPARTMENT OF SOCIAL SECURITY – Acted as quality assurance reviewer for the study of using Smart Cards to distribute social security benefits. Existing benefit payment systems were reviewed, and the feasibility of alternative distribution methods was examined.

DUTCH POST, TELEPHONE, & TELEGRAPH (PTT Post) – Participated with in development of courses of action and alternatives for the consideration of privatization of the PTT. Additionally, advised PTT management on the cost, benefits and opportunities for introducing smart cards (pre and post payment). Project work included definition of projects to design and implement country-wide smart card-based systems. Lead manager for this project.

STATE OF TENNESSEE – Advised the Department of Corrections on the feasibility and options for electronic tracking of inmates at correctional institutions. The project team explored the use of non-contact radio frequency identification tags for inmates and employees.

MIDLAND BANK (U.K.) – Technical advisor to the project team developing long-range information technology strategies post-1992. Project work included the review of banking automation products from ATMs through smart cards.

1992 SUMMER OLYMPIC GAMES/BANCO ESPANOL DE CREDITO – Developed overall strategy and feasibility for introducing and using a multi-service smart card at the 1992 Olympics for use by members of the Olympic family to include ticketing, cashless payment and security.

MAJOR LOCK MANUFACTURER – Conducted project development, planning and review for smart card based electronic stand-alone lock and related equipment. Led the evaluation of candidate market segment

requirements, smart card technology alternatives and system/product characteristics.

MAJOR RETAIL ENERGY COMPANY – Technical advisor for the development of future in-store retail automation systems.

MAJOR TELECOMMUNICATIONS COMPANY – Advised in the strategy for product development and distribution of smart card-based services. Study included the review of existing and new markets for smart card applications.

MULTINATIONAL FINANCIAL INSTITUTION – Advisory manager for the development of a cross-border banking system for high-net-worth individuals as they travel around the world.

1983-1988

Independent consultant and principal of a research and development company in smart cards and related transaction technology. Major projects included:

CITICORP – Responsible for assisting the bank in designing and planning corporate business strategies for various divisions.

- Developed strategic and tactical plans for the voice and data networks, contingency/recovery planning and network security for the North American Finance Group,

- Provided review and evaluation for business and technical requirements for the design and implementation of an expert system to automate the worldwide individual bank.

COMMITTEES AND SOCIETIES

Smart Card Industry Association **–** Founding director and member of the executive committee.

Health Care Work Group **–** Participating member in the Smart Card Forum's task force developing the national position on smart cards for health care services.

Smart Card Applications and Technologies (SCAT) Program Committee member, 1986-1990.

ANSI X3.B10 WG1 Integrated Circuit (Smart) Card standards committee. Committee Secretary 1986.

ANSI X3.B10 participating member for card related standards.

ANSI X9.A6 participating technical expert for the review of financial standards for integrated circuit (smart) cards.

ISO Technical Advisor to TC 97/SC 17 for development of international interchange standards for integrated circuit (smart) cards.

EDUCATION

Master of Business Administration, Washington University, St. Louis.
Beta Gamma Sigma honor society.

Bachelor of Science in Computer Science and Engineering, Moore School of Engineering, University of Pennsylvania. Member of the Moore School Student Council and ACM chapter chairman.

U.S. PATENT

Portable Electronic Transaction Device and System Therefor, an integrated smart card-based computer system. U.S. Patent # 4,575,621.

PUBLICATIONS & PRESENTATIONS

Mr. Dreifus has authored and presented numerous papers on the utilization of advanced technologies around the world. He coauthored the book *Smart Cards: A Guide to Building and Managing Smart Card Applications*, published by John Wiley & Sons. He is a noted speaker on several topics:

- Application of advanced card technologies
- Public telecommunications
- Electronic benefits transfer (EBT)
- Cyber and Data security
- Large scale identification

In addition, Mr. Dreifus has presented expert testimony to the U.S. Congress including assisting in developing the first landmark Federal anti-computer crime legislation, the Computer Fraud and Abuse Act.

Summary of Henry N. Dreifus Expert Witness Client Support

Type of Matter:	**Payment Patent Infringement**
Law Firm:	Ropes & Gray
Case Name:	iCashe vs. **Samsung**
Services Provided:	Research, analysis and evaluation of patent invalidity for mobile payment using magnetic stripe emulation and RF, research, analysis
Disposition:	Ongoing
Date:	2025

Type of Matter:	**E-Purse Funding and Payment Patent Infringement**
Law Firm:	Joint Defense: DLA Piper LLP, Ropes & Gray, et. al.
Case Name:	RFCyber vs. **Walmart,** Volkswagen, Shell Oil Products (Equilon Enterprises), Starbucks, Costco, Kroger, Electrify America
Services Provided:	Research, analysis
Disposition:	Pending (joint defense consolidation)
Date:	2024

Type of Matter:	**Payment Tokenization Patent Infringement**
Law Firm:	Wilson Sonsini Goodrich & Rosati
Case Name:	Cortex MCP, Inc. vs. **VISA**
Services Provided:	Research, analysis and evaluation of payment using tokens/tokenization, claim construction expert reports.
Disposition:	Case stayed due to IPR
Date:	2024

Type of Matter:	**Trade Secret Misappropriation**
Law Firm:	Quinn Emanual
Case Name:	Mad Mobile Inc. vs. **Meijer Stores**
Services Provided:	Research, analysis and evaluation of retail POS transaction payment processing modernization and business framework, expert declarations, rebuttal, deposition, arbitration testimony.
Disposition:	Favorably settled for the client.
Date:	2023 – 2024

Type of Matter:	**Patent Infringement and Validity for Self-Service Payment Vending**
Law Firm:	Wilson Sonsini Goodrich & Rosati
Case Name:	**Payrange** vs. CSC
Services Provided:	Research, analysis and evaluation of patents and evaluation analysis of infringement by CSC's POS transaction system hardware and software.
Disposition:	Favorably settled for client.
Date:	2024

Type of Matter:	**Payment Cards retail processing transactions framework dispute**
Law Firm:	Jones Day
Case Name:	4699 Investment Corporation vs. **Marathon Petroleum Corporation, LP**
Services Provided:	Research, analysis and evaluation of retail POS transaction payment processing system and business framework, expert report.
Disposition:	Favorably settled for client
Date:	2023

Type of Matter:	**Patent Validity and Infringement regarding NFC contactless and Secure Electronic Transactions**
Law Firm:	Ropes & Gray
Case Name:	Aire Technology vs. **Apple Computer Corp.**
Services Provided:	Analysis of prior invalidating art, non-infringement
Disposition:	Favorably settled for client
Date:	2022

Type of Matter:	**Patent Validity and Infringement regarding Mobile Wallet Application**
Law Firm:	DLA Piper, LLP
Case Name:	Fintiv vs. **Apple Computer Corp.**
Services Provided:	Research and analysis of prior invalidating art, non-infringement, and preparation, drafting and submission of expert reports, technological comparability rebuttal, depositions.
Disposition:	Summary Judgement in favor of client
Date:	2020

Type of Matter:	**Trade Secret Misappropriation**
Law Firm:	Kutack Rock, LLP
Case Name:	**Chase Global Services** vs. Protech Solutions
Services Provided:	Analysis of trade secret misappropriation / preparation and submission of expert report, deposition.
Disposition:	Case stayed due to the pandemic
Date:	2020

Type of Matter:	**Patent Validity and Infringement regarding multi-function card**
Law Firm:	Fish & Richardson
Case Name:	Alexsam vs. **CIGNA et. al.**
Services Provided:	Analysis of prior invalidating art, non-infringement and preparation / submission of expert report, deposition.
Disposition:	Summary Judgement in favor of client
Date:	2020-2021

Type of Matter:	**Smart Card Personalization**
Law Firm:	Stinson LLP
Case Name:	Entrust Datacard vs. **Zeiser GmbH, et. al.**
Services Provided:	Analysis of prior invalidating art and preparation / submission of expert report, deposition.
Disposition:	Settled in favor of client
Date:	2019

Type of Matter:	**Co-Branded Credit Card implementation**
Law Firm:	Williams, Porter, Day & Neville, P.C.
Case Name:	**BLACK CARD** vs. Visa USA
Services Provided:	Review and analysis of payment specifications and standards for issuing and operating a co-branded credit card for affluent cardholders. conformance of product to payment card industry specification and requirements. Provided research, analysis and expert report.
Disposition:	Adjudged
Date:	2017

Type of Matter:	**Patent Validity regarding Electronic Passports and Travel Documents**
Law Firms:	Stephen Norman Weiss and Fleit Gibbons Gutman Bongini & Bianco PL
Case Name:	United States Department of Justice v. **Iris Corporation Behrad**
Services Provided:	Research, analysis, submission of an expert report, deposition.
Disposition:	IPR challenge terminated in favor of client
Date:	2016

Type of Matter:	**Evaluation and Analysis of Payment Card Solutions for Financial Services**
Law Firm:	Snell & Wilmer
Case Name:	FiTeq vs. **Venture Corporation**
Services Provided:	Review and analysis of conformance of product to payment card industry specification and requirements. Provided expert reports, deposition, court testimony.
Disposition:	Adjudged favorably for the client
Date:	2014-2017

Type of Matter:	**Patent Infringement and Validity of Advanced Security Features of Driver Licenses**
Law Firm:	Morgan, Lewis & Bockius
Case Name:	**MorphoTrust** v. CBN Secure Technologies
Services Provided:	Research, analysis of rebuttal positions for patent validity, submission of expert report.
Disposition:	Settled in favor of client
Date:	2016

Type of Matter:	**Patent Validity and Infringement regarding Electronic Wireless Payment**
Law Firm:	Paul Hastings
Case Name:	**eBay** v. Purple Leaf Holdings
Services Provided:	Search and analysis of prior invalidating art, preparation / submission of expert report in support of a Petition before the PTAB for review.
Disposition:	PTAB Decision to institute; favorably settled for client
Date:	2014-2016

Type of Matter:	**Patent Validity and Infringement regarding Near Field Communications (NFC) Smart Cards**
Law Firm:	Ropes & Gray
Case Name:	**NXP** (now Qualcomm) vs. France Brevets, et. al.
Services Provided:	Research and Technical Analysis including Patent validity, client strategy, prior art research, patent invalidity analysis
Disposition:	Declaratory Judgement in favor of client
Date:	2015

Type of Matter:	**Patent Validity regarding Universal Credit Card Apparatus**
Law Firm:	Finnegan Henderson
Case Name:	**Square** v. e-Charge Licensing LLC
Services Provided:	Analysis of prior art and preparation / submission of expert report, deposition.
Disposition:	PTAB Decision to institute, ruled all patents invalid in favor of client
Date:	2014-2015

Type of Matter:	**Patent infringement and validity regarding Secure Data Transfer for Electronic Transactions**
Law Firm:	Hunton & Williams, et. al.
Case Name:	Maxim Integrated Products v. **Capital One Financial Corporation, et. al.**
Services Provided:	Research and Technical Analysis including Patent validity, client strategy
Disposition:	Settled in favor of client
Date:	2012-2015

Type of Matter:	**Patent Infringement and Validity regarding Prepaid Card Solutions**
Law Firms:	Alston & Bird, Paul Hastings
Case Name:	**e2Interactive, Inc. et al** v. Blackhawk Network, Inc.
Services Provided:	Research and technical analysis on patent validity and patent comparability analysis declaration and expert report, deposition and court testimony on patent technological comparability.
Disposition:	Jury verdict including damages awarded in favor of client
Date:	2011-2012

Type of Matter:	**Product Infringement of Point-of-Sale Wireless Solution and Software**
Law Firm:	Nixon Peabody, LLP
Case Name:	Communication Transaction Solutions, Inc. v. **VeriFone Holdings, Inc.**
Services Provided:	Research and technical analysis, expert declaration, deposition.
Disposition:	Settled
Date:	2007-2008

Type of Matter:	**Patent Infringement regarding Prepaid Phone Cards**
Law Firm:	Sidley Austin LLP
Case Name:	TGIP Inc. v. **AT&T Corporation, et al**
Services Provided:	Research and technical analysis, patent validity/infringement research, client strategy
Disposition:	Adjudged/Judgment as a Matter of Law (JMOL) in favor of client
Date:	2006-2007

Type of Matter:	**Trade Secret Misappropriation/Patent infringement of Biometric Smart Cards**
Law Firm:	Stoel Rives LLP
Case Name:	E-Smart Technologies, Inc., IVI Smart Technologies, Inc. v. **Wayne Drizin, Michael Gardiner, Electronic Plastics Corporation, A Card Company**
Services Provided:	Research and technical analysis, expert report preparation, client strategy
Disposition:	Settlement discussions/stayed
Date:	2006-2008

Type of Matter:	Sherman **Antitrust Act**
Law Firm:	Heller-Ehrman
Case Name:	United States v. **Visa USA,** Visa International and MasterCard International
Services Provided:	Expert analysis for Visa on Payment Systems Innovation and Smart Cards, prepared expert report, deposition
Disposition:	Adjudged
Date:	1999-2001

APPENDIX B

APPENDIX B (LIST OF MATERIALS CONSIDERED)

Exhibit No.	DESCRIPTION
1001	U.S. Patent No. 11,270,174 ("'174")
1002	File History of U.S. Application No. 17/021,347 ("'174FH")
1004	U.S. Patent App. Pub. 2011/0240748 ("Doughty-CON")
1005	U.S. Patent App. Pub. 2004/0133787 ("Doughty")
1008	Redline Between Doughty and Doughty-CON
1009	U.S. Patent No. 5,943,624 ("Fox")
1010	U.S. Patent No. 7,917,444 ("Bursch")
1011	U.S. Patent App. Pub. 2005/0086171 ("Abe")
1012	U.S. Patent App. Pub. 2006/0165060 ("Dua")
1013	U.S. Patent No. 6,636,833 ("Flitcroft")
1014	Plaintiff iCashe's Infringement Contentions, Including Appx. H-1
1028	U.S. Patent App. Pub. 2006/0017626 ("Kannan")
1029	U.S. Patent No. 6,400,965 ("Phillips")
1030	U.S. Patent No. 4,877,947 ("Mori")
1032	U.S. Patent No. 5,466,919 ("Hovakimian")
1036	U.S. Patent No. 6,670,796 ("Mori")
1041	U.S. Patent App. Pub. 2007/0236350 ("Nystrom")
1042	Periodically, Merriam-Webster's Collegiate Dictionary (11th ed., 2003)
1043	U.S. Patent App. Pub. 2006/0168418 ("Adusumilli")

Exhibit No.	DESCRIPTION
1044	U.S. Patent App. Pub. 2003/0004811 ("Omori")

* I also considered any additional materials referenced in my declaration.