

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 IPR2025-00644

Patent No. 9,208,423

**DECLARATION OF HENRY N. DREIFUS IN SUPPORT
OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 9,208,423**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. QUALIFICATIONS.....	4
III. LEGAL UNDERSTANDING.....	9
IV. BACKGROUND OF THE TECHNOLOGY.....	15
V. THE '423 PATENT	18
A. The '423 Patent Overview.....	18
B. Prosecution History	20
1. The '423 Patent Prosecution	20
2. The '174 Patent Prosecution	21
VI. LEVEL OF ORDINARY SKILL IN THE ART	36
VII. CLAIM CONSTRUCTION.....	37
VIII. GROUNDS OF UNPATENTABILITY.....	38
IX. SPECIFIC GROUNDS FOR CHALLENGE	39
A. GROUND 1: Doughty in view of Bursch (Claims 1-5, 8-18)	39
1. Overview of Doughty (Ex. 1005, U.S. Patent App. Pub. 2004/0133787)	39
2. Overview of Bursch (Ex. 1010, U.S. Patent 7,917,444).....	41
3. Motivation to Apply Bursch's Teachings to Doughty	42
4. Invalidity of Claims 1-5, 8-18 Over Doughty in view of Bursch	46
B. Ground 2: Doughty in view of Bursch and Fox (U.S. Patent 5,943,624) (Claims 1-5, 8-18).....	93
X. SECONDARY CONSIDERATIONS	95
XI. CONCLUSION	96

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. 9,208,423 (“the ’423 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 1-5 and 8-18 of the ’423 patent (“Challenged Claims”) are obvious over the prior art references identified below.

2. I understand that the ’423 patent is titled “Mobile Device with Time-Varying Magnetic Field and Single Transaction Account Numbers,” 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 ’423 patent. I understand that the ’423 patent has been provided as Ex. 1001.

3. I understand that the file history of the ’423 patent has been provided as Ex. 1002. I have considered this file history, and I will refer to it as “the ’423 File History.”

4. I understand that the ’423 patent is a continuation of U.S. Patent Application No. 14/833,113 (“the ’113 Application”) , 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 ’423 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 ’423 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 ’423 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 '423 patent; my own knowledge and experiences gained from my work experience in the field of the '423 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 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.
- **U.S. Patent No. 5,943,624 (“Fox”)** to Thomas M. Fox et al. (“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.

9. I understand that there is a pending district court litigation between Petitioners and iCashe, Inc. (“Samsung Litigation”) involving the ’423 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 discussed 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.

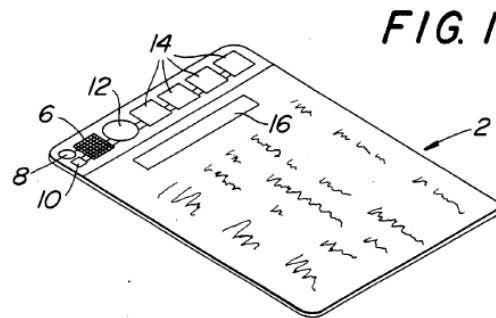
15. I received a Bachelor of Science in Computer Science and Engineering from the Moore School of Engineering at the University of Pennsylvania in 1982, where I was a member of the Engineering Student Council and Chairman of the Association of Computing Machinery (ACM) Chapter. I also obtained a Master 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 '423 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 '423 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 '423 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), including a single transaction account number. '423 patent, 2:62-3:6, 3:40-51, 4:61-5:8, 13:24-29, claims 1, 9, 15. In order to overcome a rejection over the prior art, the Applicant amended the claims to change “mobile device” to “mobile phone,” and argued the Examiner improperly took official notice that having single transaction account numbers was known. Ex. 1002, 1507-09, 1528.

41. But these concepts were already known in the art. For example, the Examiner recognized during prosecution of a later related application sharing the same specification—U.S. Application No. 17/021,347 (“the ’347 Application”), which issued as U.S. Patent No. 11,270,174 (Ex. 1006, “the ’174 patent”)—that a mobile phone that mimics a swipe of a magnetic card (e.g., credit card) by producing a time-varying magnetic field was known. During prosecution of the ’174 patent, the Examiner rejected claims directed to this same subject matter over U.S. Patent App. Pub. 2011/0240748 (“Doughty-CON”) (Ex. 1004), which is a continuation of and—as I explain below—has substantially the same disclosures as Doughty (Ex. 1005).¹

42. According to the ’174 patent Examiner, Doughty-CON (and thus

¹ As I note below in Section V.B.2, the differences between Doughty and Doughty-CON are immaterial to the Examiner’s analysis during prosecution of the ’347 Application.

Doughty) discloses a “mobile phone” with circuitry “producing a time-varying magnetic field that represents transaction data.” ’174 File History (Ex. 1007), 1454, 1457. For example, as the Examiner found, Doughty-CON (and thus Doughty) discloses a “telecommunications device” with magnetic field generator 308—which includes “control circuit 554” that produces “emulated time-varying magnetic stripe data” used to “emulat[e] the swipe of a magnetic stripe through the magnetic card reader”—and “device processor 314,” coupled together. Ex. 1007, 1454, 1457; Doughty-CON, [0009], [0046], [0051], Figs. 3 (elements 308, 312, 314), 5B (element 554). In response to these rejections by the Examiner during prosecution of the ’174 patent, the Applicant did not dispute these disclosures, but instead amended the claims to recite limitations that do not appear in the ’423 Patent Claims. Ex. 1007 1517-19, 1539, 1544-45. Just like Doughty-CON, Doughty discloses each of these limitations of the ’423 Patent Claims.

43. Additionally, Bursch (Ex. 1010) discloses single-use transaction numbers to perform transactions, which “can be generated just prior to being used” to improve security by “minimizing the amount of time during which they can be lost or stolen.” Bursch, Abstract. Bursch teaches that each transaction number is unique to each user, can be authenticated by an issuing institution or other party, and includes a predefined “exact sequence unique to the transaction number generator.” Bursch, Abstract, 2:33-44. A person of ordinary skill in the art would have been

motivated to apply these teachings to Doughty as they improve transaction security.

44. As I discuss below, the claims of the '423 patent are obvious over the 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 '423 PATENT

A. The '423 Patent Overview

45. The '423 patent generally relates to an “intelligent electronic device” (e.g., “mobile phone”) that internally communicates with an “electronic transaction card.” Abstract, 2:16-34. 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.” '423 patent, 4:61-67, 3:54-56, 10:53-65. “Electronic transaction card 104 may then be used with a magnetic stripe or smartcard based merchant point-of-sale terminal to effect a transaction.” '423 patent, 3:56-59. According to the '423 patent, “the term ‘transaction’ refers to any beneficial use of an electronic transaction card.” '423 patent, 3:40-41.

46. As shown in Figure 20, 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.” ’423 patent, 11:6-8, 11:48-12:3, Fig. 20.

The ’423 patent discloses in another embodiment that a “processing device” “may execute program instructions that influence communications between” the device and “a magnetic card reader.” ’423 patent, 6:42-46.

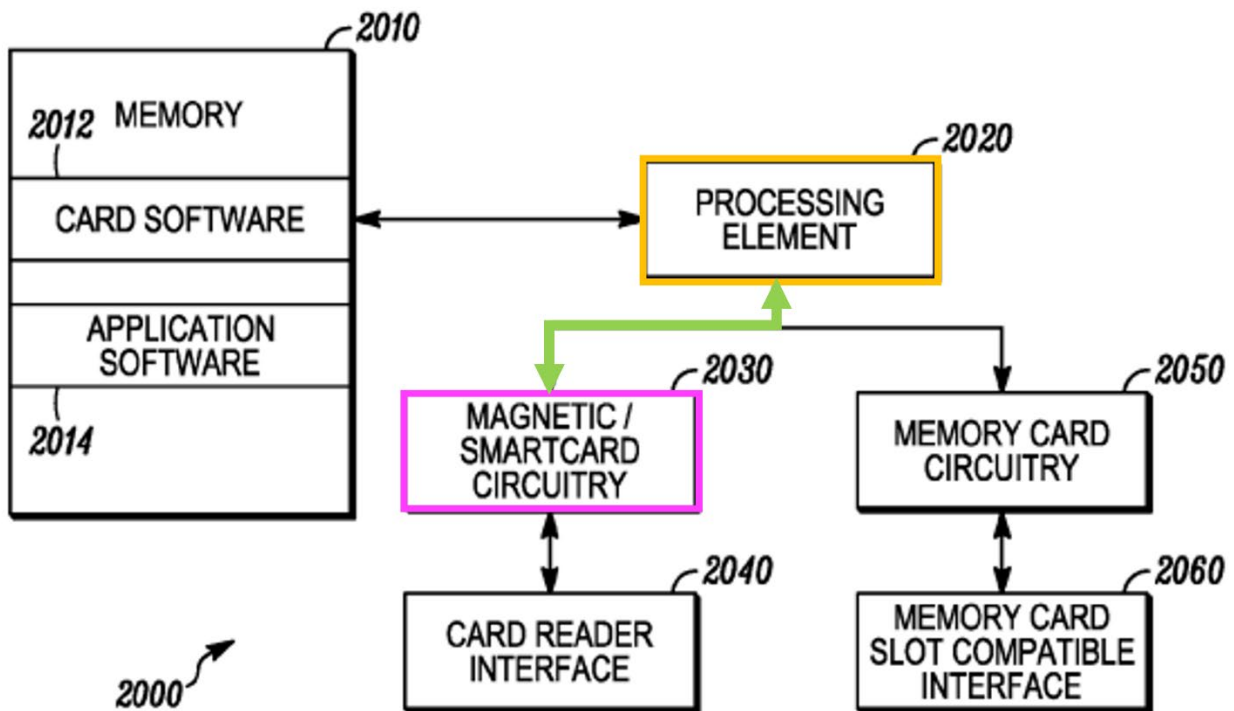


FIG. 20

47. The electronic transaction card “may be programmed to have one number, similar to how a credit card uses the same number repeatedly” or else may be “programmed to use a different number for each transaction.” ’423 patent, 5:2-7. “These numbers are referred to [] as ‘single transaction account numbers.’” ’423 patent, 5:7-8. “Single transaction account number generation software” may be

installed on the mobile phone. '423 patent, 12:15-21, Fig. 20.

B. Prosecution History

1. The '423 Patent Prosecution

48. In formulating my opinions, I also considered the contents of the prosecution history of the '423 patent. *See* Ex. 1002.

49. The '423 patent issued from U.S. Pat. App. 14/833,113 (“the '113 Application”), filed August 23, 2015.

50. During prosecution of the '423 patent, the Examiner rejected claims 1-20 on the ground of nonstatutory double patenting over grandparent-patent claims 1-20 of U.S. Patent No. 9,092,708. Ex. 1002, 1505. The Examiner also rejected claim 1 under Section 102 as being anticipated by U.S. Patent No. 4,791,283 (“Burkhardt”) and rejected claims 3-10 and 12-16 under Section 103 as being obvious in view of Burkhardt. Ex. 1002, 1507-08. While the Examiner acknowledged that Burkhardt does not specifically disclose a “credit card” used for financial transactions, the Examiner took Official Notice that “magnetic stripe credit cards, with discrete and individual account numbers for use in financial transactions are old and well known,” and found that Burkhardt does disclose the use of financial transaction cards, including credit cards, in background discussions. Ex. 1002, 1508. The Examiner concluded that it would have been obvious to a person of ordinary skill in the art at the time of the invention to use the card of Burkhardt as a credit card in a

financial transaction to meet then pending claims 3-10 and 12-16. *Id.*

51. In response, Applicant amended the claims to change the preamble from “mobile device” to “mobile phone” and argued that the Examiner improperly took official notice that “individual account numbers for use in financial transactions are old and well known” to overcome the Sections 102 and 103 rejections over Burkhardt. Ex. 1002, 1507-09, 1525-29. Additionally, Applicant filed a terminal disclaimer to overcome the nonstatutory obvious-type double patenting rejection over the grandparent patent. Ex. 1002, 1525-29. The claims were subsequently allowed on October 28, 2015. Ex. 1002, 1533.

2. The '174 Patent Prosecution

52. The '423 patent claims overlap extensively with the claims of the related '347 Application, which issued as the '174 patent. '174 patent (Ex. 1006), 1:7-44. During prosecution of the '347 Application, the Examiner found that Doughty-CON anticipated identical and/or very similar limitations to the challenged claims of the '423 patent. Ex. 1007, 1454-57. To overcome the Examiner's anticipation rejection based on Doughty-CON, the Applicant amended the claims of the '347 Application to recite a “network interface for connecting the mobile phone to a network” limitation—which is not present in any of the '423 Patent Challenged Claims—to secure allowance. *Id.*, 1517-19 (amending 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”),
1539, 1544-45.

53. 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.

54. The below chart compares the language of the challenged '423 Patent Claims with identical or substantially identically claim limitations that were found by the Examiner to be disclosed by Doughty-CON during prosecution of the '347 Application, including the cited portions of Doughty-CON upon which the Examiner relied.²

'423 Challenged Claims	'347 Application	Doughty-CON (Disclosure Relied
------------------------	------------------	-----------------------------------

² While the limitations of claims 5, 10, 13-14, and 16-18 and element [15.b] of the '423 patent, along with certain language of the '423 patent limitations identified by ellipses in the chart below do not have corresponding language in the '347 application, Doughty or Bursch discloses these limitations as I explain below in Section IX.

		Upon By Examiner) ³
[1.pre] A mobile phone comprising:	[1.pre] A mobile phone comprising:	Doughty-CON [0046]
[1.a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card; and	[1.b] current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions; [5] The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.	Doughty-CON Fig. 3, 308 (“Magnetic Field Generator”); [0051]
[1.b] a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field....	[1.b] current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions; [1.c] a driver to excite the current carrying conductor;	Doughty-CON Fig. 3, 308 (“Magnetic Field Generator”), 314 (“Device Processor or Controller”); Fig. 5B, 554 (“Control Circuit”); [0051]

³ 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.d] a processor coupled to control the driver.	
[2] The mobile phone of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction. [5] The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.	Doughty-CON [0008], [0038], [0051]
[3] The mobile phone of claim 1 wherein the single transaction account number represents financial data.	[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Doughty-CON [0008], [0038]
[4] The mobile phone of claim 3 wherein the financial data comprises credit card data.	[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Doughty-CON [0008], [0038]
[8] The mobile phone of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.	[2] The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	Doughty-CON [0008], [0095]-[0097]
[9.pre] A mobile phone comprising:	<i>See above analysis corresponding to '423 patent, [1.pre]</i>	
[9.a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	<i>See above analysis corresponding to '423 patent, [1.a]</i>	
[9.b] ...circuitry for performing transactions...; and	[1.b] current carrying conductor capable of producing a time-varying magnetic field that represents	Doughty-CON Fig. 3, 308 (“Magnetic Field Generator”); [0051]

	the transaction data in the plurality of transactions; [11] The mobile phone of claim 7 wherein the time-varying magnetic field emulates a swipe of a magnetic card.	
[9.c] a processor coupled to...the circuitry to produce a time-varying magnetic field.	[1.b] current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions; [1.c] a driver to excite the current carrying conductor; [1.d] a processor coupled to control the driver.	Doughty-CON Fig. 3, 308 (“Magnetic Field Generator”), 314 (“Device Processor or Controller”); Fig. 5B, 554 (“Control Circuit”); [0051]
[11] The mobile phone of claim 9 wherein the transactions are financial transactions.	[2] The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction. [4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Doughty-CON [0008], [0038], [0095]-[0097]
[12] The mobile phone of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.	[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Doughty-CON [0008], [0038], [0051]

	[5] The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.	
[15.pre] A mobile phone comprising:	<i>See</i> above analysis corresponding to '423 patent, [1.pre]	
[15.a] circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card;	<i>See</i> above analysis corresponding to '423 patent, [1.a]	
[15.c] a processor coupled to the circuitry to produce a time-varying magnetic field....	<i>See</i> above analysis corresponding to '423 patent, [1.b]	

Ex. 1006, 1454-1457.

55. In this regard, I have 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 through paragraphs cited, and compare the language in Doughty and Doughty-CON.

56. 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	[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.	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.
--	--

57. 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. 1007, 1454-57.

58. 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	[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	stripes such that the data within the tracks of the stripe can be <i>spatially</i> 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 <i>of if</i> 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
--	--

basic transaction authorized by the owner.	the magnetic stripe data following the basic transaction authorized by the owner.
--	---

59. 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. 1007, 1454-56.

60. 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.

61. 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. 1007, 1455-57.

62. 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 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	[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~~ 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.

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.	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.
---	--

63. 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. 1007, 1457.

64. 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	[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	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.	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.
---	--

65. The only difference is the removal of “spatially distributed,” but the Examiner did not rely on “spatially distributed” in the rejection. Ex. 1007, 1454-57.

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

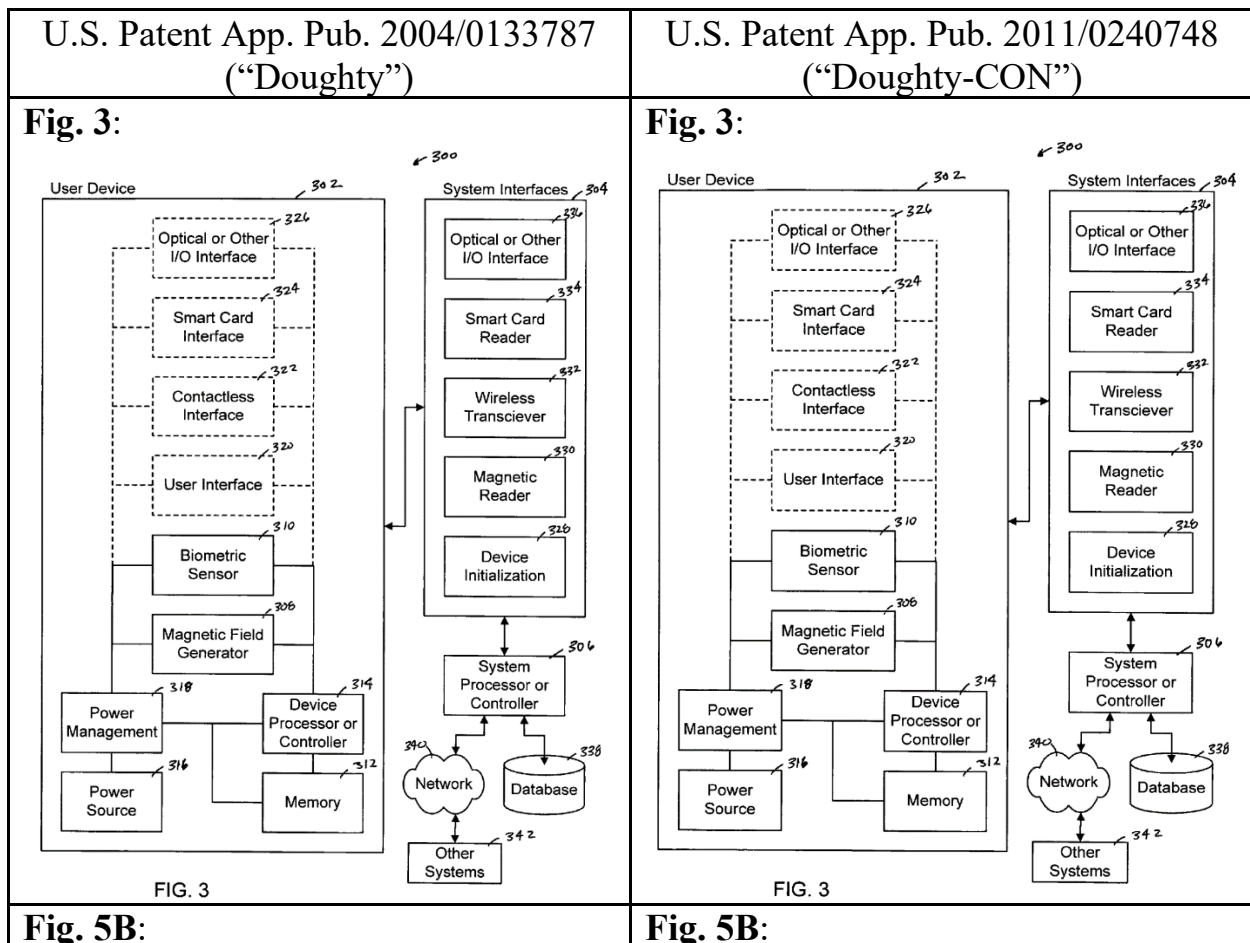
U.S. Patent App. Pub. 2004/0133787 (“Doughty”)	U.S. Patent App. Pub. 2011/0240748 (“Doughty-CON”)
[0095] Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment 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.

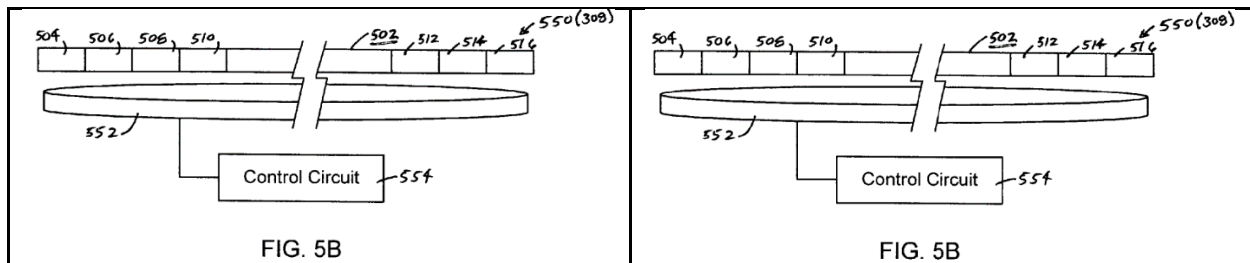
[0096] Payments for retail purchases are generally accomplished in one of three ways: with cash; with a check; or with a credit or debit card. In a cash transaction, there is generally no need for validating the identification of the buyer. In a transaction where a check is used, there generally is a 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 availability for, and legitimacy of, the check presented for payment.	[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.
[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	[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.

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.

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





VI. LEVEL OF ORDINARY SKILL IN THE ART

68. 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.

69. 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.

70. Upon consideration of these factors, and based on my knowledge and experience in the field and my review of the '423 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.

71. 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 '113 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

72. I have been instructed that the Challenged Claims of the '423 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.

73. I understand that presently the parties have not proposed constructions for the '423 patent in the Samsung Litigation.

VIII. GROUNDS OF UNPATENTABILITY

74. 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 represents a single transaction number to mimic the swipe of a magnetic card was well-known in the art.

75. 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	US2004/0133 787	10/7/2003	7/8/2004
Bursch	1010	US7,917,444	10/29/2002	3/29/2011
Fox	1009	US5,943,624	07/15/1996	8/24/1999

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

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

- **Ground 1:** Challenged Claims 1-5 and 8-18 of the '423 patent are rendered obvious by Doughty in view of Bursch.
- **Ground 2:** Challenged Claims 1-5 and 8-18 of the '423 patent are rendered obvious by Doughty in view of Bursch and Fox.

77. It is my opinion that Challenged Claims of the '423 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

78. As I explain above in Section IV, although the '423 patent purports to have invented the concept of using a mobile phone to perform transactions by producing a time-varying magnetic field that represents a single transaction number to mimic 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.

79. In this section, I explain why claims 1-5 and 8-18 of the '423 patent are rendered obvious by the teachings of Doughty together with Bursch and optionally Fox. 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.

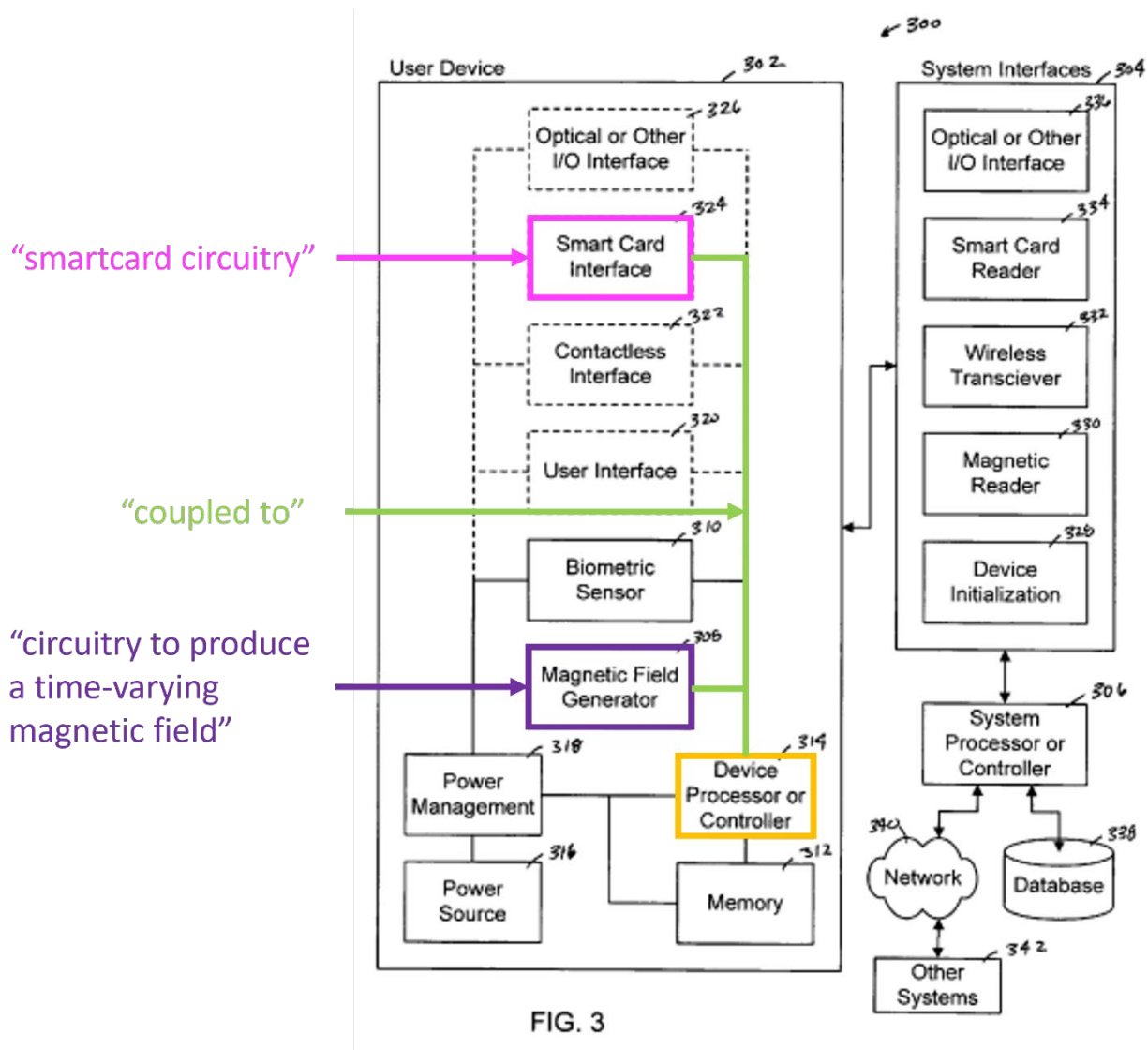
A. GROUND 1: Doughty in view of Bursch (Claims 1-5, 8-18)

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

80. Doughty discloses a user device 302 mounted on a substrate that is incorporated into a mobile device such as a “telecommunications device.” [0046]. “The device 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].

81. As shown in Figure 3, the user device 302 includes a “**device processor or controller 314**” coupled to “**magnetic field generator 308**.” Doughty, [0040], Fig. 3. **Magnetic field generator 308** creates “a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.” Doughty, [0010]. And “**smartcard interface 324**” communicates with a “smart card reader 334.” Doughty, [0047]. **Smart card interface 324** is **coupled to** the **processor 314** as shown in Fig. 3 (annotated below). “The **magnetic field generator 308**” is “communicably coupled to the device **processor 314**” to “activate the magnetic field generator 308 when the user is verified.” Doughty, [0040]. “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.” Doughty, [0041].



2. Overview of Bursch (Ex. 1010, U.S. Patent 7,917,444)

82. 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. Burch’s “single-use transaction numbers” may have a predefined “exact sequence unique to the transaction number generator.” Bursch, 2:33-44.

83. The “single-use, transaction numbers” disclosed in Bursch “contain...an account number” that “is used by the issuing institution to uniquely identify the person or entity to which the transaction number is associated and to identify the account to which all transactions are debited or credited.” Bursch, 3:17-37.

3. Motivation to Apply Bursch’s Teachings to Doughty

84. Doughty and Bursch are analogous art, in the same field as the ’423 patent, which includes electronic devices for performing transactions, and are reasonably pertinent to purported problems addressed by the named inventors of the ’423 patent involving the use of electronic devices to securely perform transactions. ’423 patent, ’423, 1:7-25, 4:61-5:8, 6:3-21; Doughty [0002], [0003], [0004], [0007], [0008], [0038], [0040], [0041], [0046], Fig. 5B; 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.

85. 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 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 or 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.

86. A person of ordinary skill in the art would have also been motivated to apply Bursch's teachings of generating single-use transaction numbers in a pre-defined order. For example, Bursch teaches that because the single-use transaction numbers are generated in a pre-defined order, "the issuing institution can generate

transaction numbers that are identical to the transaction numbers that the institution expects to receive from the authorized user of the transaction number generator.” 2:33-44. This allows the issuing institution to validate transaction numbers, thereby improving the security of the transactions. Bursch, 2:33-44. For example, “when the expected transaction number does not match the transaction number received in conjunction with a transaction” the issuing institution can “have the user account shut down or invalidated.” Bursch, 4:50-54.

87. A person of ordinary skill in the art would, in my opinion, have found it straightforward to apply Bursch’s teachings of single-use transaction numbers to Doughty’s telecommunications device. For example, Bursch discloses that its single-use transaction numbers can be created via a “transaction number generator” that “may be implement[ed] in handheld devices” including “for example, a PDA or a telephone,” such as the telecommunications device disclosed in Doughty. Bursch, 7:50-54. Moreover, Doughty discloses circuitry that produces a time-varying magnetic field representing non-limiting forms of transaction data, and “includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc.” Doughty, [0008], [0041]. Bursch discloses that single-use transaction numbers “may have the same format as a credit card number” or a charge card number. Bursch, 3:11-16. A person of ordinary skill in the art would have found it straightforward to use Bursch’s single-use transaction

numbers as part of Doughty's transaction data. For example, Bursch teaches single-use transaction numbers for payment transaction accounts in the form of credit card format, which is a type of user number that is used by the payment industry to identify a user's account. For example, U.S. Patent No. 5,955,961 (issued September 21, 1999) discloses that "credit cards" include "[d]ata for identifying the customer, such as an account number or other identifying data is magnetically stored on the card." Ex. 1037, 1:16-20. For example, Bursch discloses that single-use transaction numbers "may have the same format as a credit card number" or a charge card number. Bursch, 3:11-16. Moreover, in my opinion, a person of ordinary skill in the art would have found it straightforward to use the single-use transaction numbers in a predefined order in Doughty's telecommunications device, as Bursch teaches how to coordinate between a user device and a financial institution to ensure that transactions can be performed. Bursch, 2:33-44.

88. 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 and would have known such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

4. Invalidity of Claims 1-5, 8-18 Over Doughty in view of Bursch

89. As I discuss below, Claims 1-5 and 8-18 are disclosed or rendered obvious by Doughty in view of Bursch. In addition to my discussion in Sections IX.A.1-3, the following discussion identifies example disclosures followed by bulleted excerpts from Doughty and Bursch that each disclose Claims 1-5 and 8-18.

a. Element [1.pre]

90. **Element [1.pre]** recites “**A mobile phone comprising.**” This element is met by Doughty.

91. **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:**

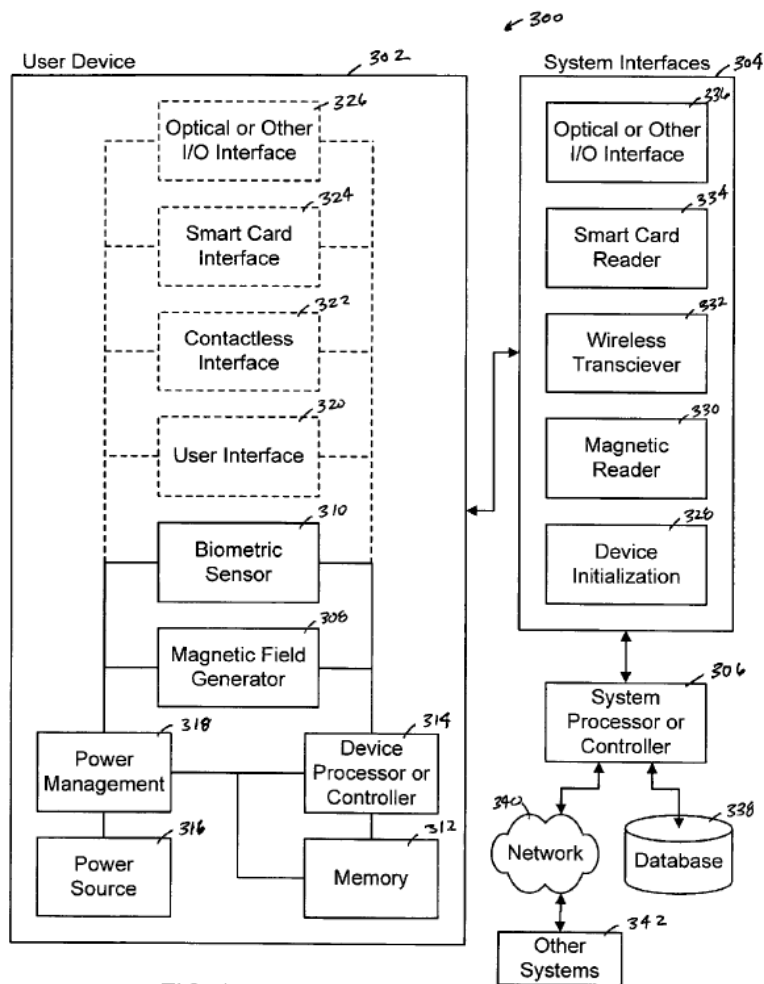


FIG. 3

- [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 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....*** 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.”

92. 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 (and thus a mobile device).⁴ A mobile phone is used for telecommunications, and it is also personal to a user for communications. At minimum, a person of ordinary skill in the art would have found it obvious to implement the user device 302 in a mobile phone to advantageously take advantage of a mobile device that a user carries around (including to locations where transactions would occur), reduced risk of theft or loss, the ability to access

⁴ 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.

information on the smartcard using the phone, and the ability to update information on the smartcard using the phone functionality. For example, it was well-known that the use of a portable device such as a “cellular telephone” provides “ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system.” Fox, Abstract, 2:21-29.

b. Element [1.a]

93. **Element [1.a] recites “circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card.”** This element is met by Doughty.

94. **Doughty discloses circuitry (e.g., “magnetic field generator 308”) to produce a time-varying magnetic field (e.g., “create a time-varying magnetic signal”) that mimics a swipe of a magnetic card (e.g., “emulating data obtained from swiping a magnetic stripe card”).** *E.g.*, Doughty:

- **Fig. 3:**

“circuitry to produce a time-varying magnetic field”

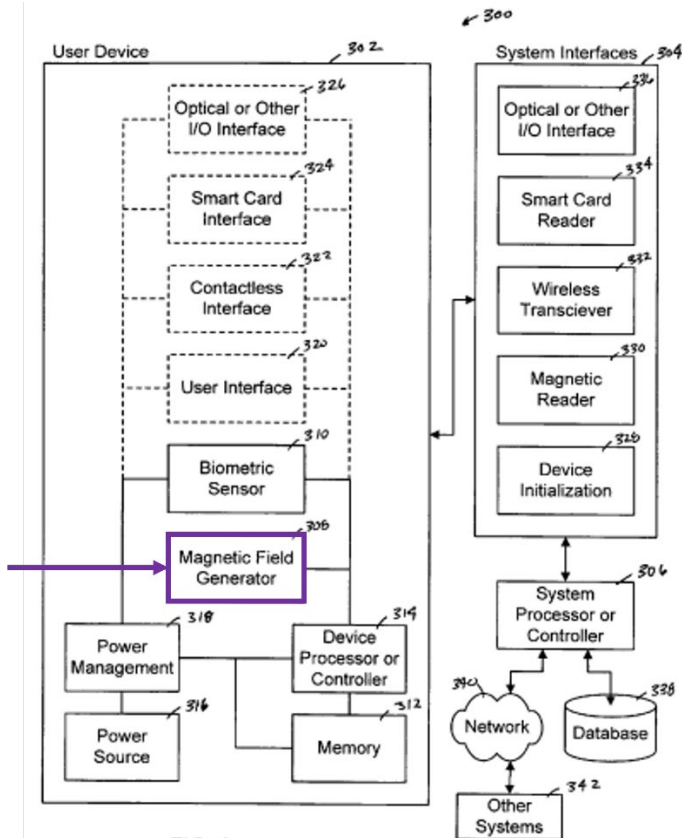


FIG. 3

- [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, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory.... The 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.... 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.”

95. See my discussion of element [1.pre] above (Section IX.A.4.a).

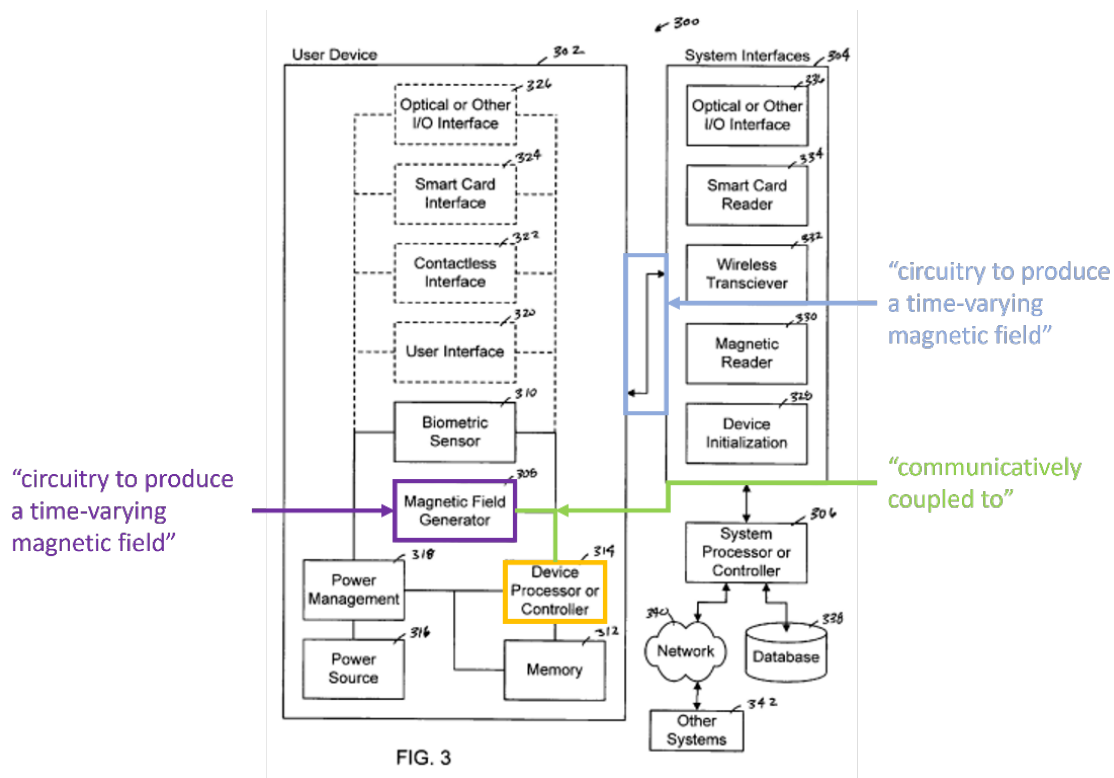
96. Doughty further discloses that “user device 302” includes a “magnetic field generator 308” in the form of a “magnetic stripe” that “create[s] a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.” [0010], [0040], [0041], [0051], Fig. 3.

c. Element [1.b]

97. Element [1.b] recites **“a processor coupled to the circuitry to cause the circuitry to produce a time-varying magnetic field that represents a single transaction account number.”** This element is met by Doughty in view of Bursch.

98. **Doughty discloses a processor** (e.g., “device processor or controller 314”) **coupled to the circuitry** (e.g., “communicably coupled to” “magnetic field generator 308”) **to cause the circuitry to produce a time-varying magnetic field** (e.g., “to...activate the magnetic field generator 308” to “creat[e]...a time-varying magnetic signal”) **that represents transaction data** (e.g., “includes binary data to enable a transaction”). E.g., Doughty:

- **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. **Each user device 302 includes** a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a **device processor or controller 314** and a power source 316. **Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit.** The device processor 314 may also include a

smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. ***The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314.... The 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. ... 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.”***
- [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.”***

99. See my discussion of elements [1.pre]-[1.a] above (Sections IX.A.4.a-

b).

100. Doughty further discloses that the user device 302 includes “device

processor or controller 314” that is “communicably coupled” to and activates “the magnetic field generator 308.” [0040], Fig. 3. The magnetic field generator 308 generates “a time-varying magnetic signal” that includes “binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc.” [0040], [0041], [0051].

101. **Bursch discloses a single transaction account number** (e.g., “single-use, transaction number” including “account number”). E.g., Bursch:

- **Abstract:** “Methods for producing and applications for single-use transaction numbers. *The transaction numbers are single-use in that the numbers are only valid for a single transaction. The transaction numbers can be generated just prior to being used, minimizing the amount of time during which they can be lost or stolen.* The transaction numbers can be generated using encryption technology such as dynamic password technology. The encryption technology makes it very difficult if not impossible to predict what the next transaction number generated will be. The transaction numbers are unique to the user and can be validated or authenticated by an issuing institution that maintains an ability to generate the same transaction numbers issued to the user.”
- **2:22-32:** “*The present invention addresses one or more of the problems identified above by providing for secure, single-use, transaction numbers.* A transaction number generator is utilized to create transaction numbers one at a time. The sequence of transaction numbers generated is unique for each transaction number generator. Encryption technology can be used to make it difficult, if not impossible, to predict the next transaction number that will be generated. *Transaction numbers according to the present invention are single-use in that once a specific transaction number is used in a transaction it will not be validated for any other transaction.*”
- **2:65-67:** “The present invention allows a *consumer to generate a secure, single-use, transaction number that can be used to make purchases of goods and services.*”

- **2:67–3:3:** “Transaction numbers according to the present invention have the same format as business account numbers of the prior art and *can be used in the same manner as business account numbers.*”
- **3:17-18:** “Transaction numbers contain a routing number, *an account number*, and an authenticating number.”
- **5:53-60:** “Transaction numbers according to the present invention are single-use. For each purchase a different number is generated and compared to the number generated by the issuing institution (that is, the expected number). *If anybody, including the legitimate user of the generator, attempts to use the same number twice, it would be rejected on the second attempted use because the issuing institution would have generated a new expected number for the second attempted purchase.*”
- **5:60-65:** “*The fact that transaction numbers according to the present invention are single-use is an important security feature of the present invention. A lost or stolen transaction number that has been used according to the present invention cannot be used again.*”

102. Bursch discloses that “single-use, transactions numbers” are “used to make purchases of goods and services” such that each transaction number is “only valid for a single transaction.” Abstract, 2:22-32, 2:65-67, 5:53-60. Further, these “transaction numbers contain a routing number, an account number and an authenticating number.” 3:17-18. Further, the transaction numbers “can be used in the same manner as business account numbers.” 2:67-3:3.

103. As I explain in Section IX.A.3, a person of ordinary skill in the art would, in my opinion, have been motivated to apply Bursch’s teachings of using single-use transaction numbers to Doughty’s telecommunications device such that Doughty’s time-varying magnetic field represents single transaction account numbers.

d. Claim 2

104. Claim 2 recites “The mobile phone of claim 1 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.” This element is met by Doughty.

105. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-c). Doughty discloses that the time-varying magnetic field mimics a swipe of a magnetic credit card (e.g., “time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card,” such as “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.*”
- [0010]: “The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator ...*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.”
- [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).”
- [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.... *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.”
- [0052]: “In addition, the magnetic reader 330 (FIG. 3) may have a start sentinel that signals a detector on the card to alert the card that it is in the presence of the card reader 330 (FIG. 3). Once the card is alerted that it is being swiped through the reader 330 (FIG. 3), it *begins transmission of the emulated time-varying data from the device processor to the inductive coils 552, thereby generating an exact emulation and transmission to the reader 330 (FIG. 3) of the data that would have been produced by swiping the card through the reader 330 (FIG. 3) with spatially varying data included in the individual data cells 504-516.*”

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

107. Doughty further discloses that the time-varying magnetic field is “for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.” [0041], Fig. 3. Additionally, 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].

e. Claim 3

108. **Claim 3 recites “The mobile phone of claim 1 wherein the single transaction account number represents financial data.”** This element is met by Bursch.

109. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-c). **Bursch discloses that the single transaction account number represents financial data** (*e.g.*, “single-use transaction number” contains “a routing number” and “account number” that are used “to make a purchase”). *E.g.*, Bursch:

- **3:17-27: “*Transaction numbers contain a routing number, an account number, and an authenticating number.*”** The authenticating number is discussed below. *A routing number identifies the institution or organization that maintains the account associated with the transaction number, frequently a bank or other financial institution.* This institution may or may not be the same institution that opened an account on behalf of a customer. For purposes of the present specification the institution identified by the routing number will be referred to as the issuing

institution. By way of example, usually the first 4 digits of a credit card number comprise the routing number.”

- **3:28-37:** *“The account number is used by the issuing institution to uniquely identify the person or entity to which the transaction number is associated and to identify the account to which all transactions are debited or credited.* For example, in a credit card number the account number is usually comprised of the 7 digits immediately following the 4-digit routing number. When a purchase is made using a transaction number, the issuing institution records purchase information (amount, date, and merchant identification, for example) on the account of the user indicated by the account number.”
- **7:55-8:3:** *“In one embodiment, a transaction number generator is used to generate a single-use transaction number having the same format as a credit card number.* That is, the single-use transaction number consists of 16 digits. *Four of the 16 digits constitute a routing number and identifies the issuing institution and 7 of the digits constitutes an account number that identifies the user's account.* The transaction number generator is implemented utilizing dynamic password technology capable of generating a 5 digit dynamic password...*The user can then use this transaction number just like a credit card number to make a purchase.”*

110. Bursch further explains that “[t]ransaction numbers contain a routing number, an account number, and an authenticating number.” 3:17–27. The routing number “identifies the institution or organization that maintains the account associated with the transaction number, frequently a bank or other financial institution.” 3:19-27. “The account number is used by the issuing institution to uniquely identify the person or entity to which the transaction number is associated and to identify the account to which all transactions are debited or credited.” 3:28-37. “The user can then use this transaction number just like a credit card number to make a purchase.” 7:55-8:3.

111. In my opinion, as discussed in Section IX.A.3, a POSITA would have been motivated to apply Bursch’s teachings of single-use transaction numbers (which represent financial data) to Doughty’s user device to advantageously improve the security of its financial transactions.

f. Claim 4

112. **Claim 4 recites “The mobile phone of claim 3 wherein the financial data comprises credit card data.”** This element is met by Bursch.

113. See my discussion of claim 3 above (Section IX.A.4.e). **Bursch discloses that the financial data comprises credit card data** (e.g., “single-use, transaction number” includes a “routing number” and “account number” used to “identify an account to be credited”). *E.g.*, Bursch:

- **3:10-16:** “Transaction numbers may comprise any number of alphanumeric characters. *For example, a transaction number may have the same format as a credit card number, which typically are comprised of 16 digits.* Additionally, a transaction number may have a 15-digit format like many charge card numbers or a 10-digit format like many phone card numbers.”
- **3:28-33:** “*The account number is used by the issuing institution to uniquely identify the person or entity to which the transaction number is associated and to identify the account to which all transactions are debited or credited.* For example, in a credit card number the account number is usually comprised of the 7 digits immediately following the 4-digit routing number. When a purchase is made using a transaction number, the issuing institution records purchase information (amount, date, and merchant identification, for example) on the account of the user indicated by the account number.”

- **7:55-8:3:** “In one embodiment, a transaction number generator is used to generate a single-use transaction number *having the same format as a credit card number*. That is, the single-use transaction number consists of 16 digits. *Four of the 16 digits constitute a routing number and identifies the issuing institution and 7 of the digits constitutes an account number that identifies the user's account*. The transaction number generator is implemented utilizing dynamic password technology capable of generating a 5 digit dynamic password. *When a user requests a single-use transaction number, the generator first creates a 5 digit dynamic password consisting of 5 digits. This dynamic password is then combined with the 7 digit account number and the 4 digit routing number to produce a 16 digit, single-use, transaction number. The user can then use this transaction number just like a credit card number to make a purchase.*”

114. Bursch further discloses that the “routing number” and “account number” in the “single-use, transaction number” is used “to identify the account to which all transactions are debited or credited.” 3:28-33. The “transaction number,” which “may have the same format as a credit card number,” is then used “just like a credit card number to make a purchase.” 3:10-16, 7:55-8:3. 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.

115. In my opinion, as discussed in Section IX.A.3, a POSITA would have been motivated to apply Bursch’s teachings of single-use transaction numbers

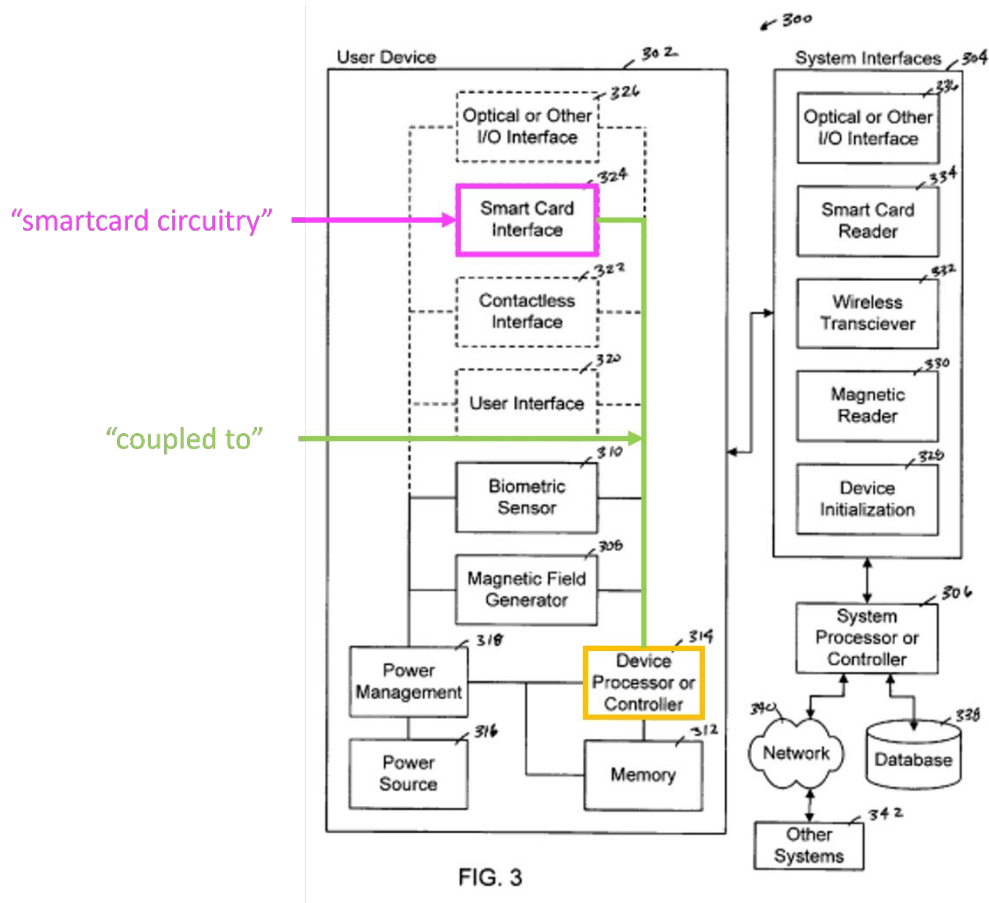
(which includes a credit card number) to Doughty's user device to advantageously improve the security of its financial transactions.

g. Claim 5

116. **Claim 5 recites “The mobile phone of claim 1 further comprising smartcard circuitry coupled to the processor.”** This element is met by Doughty.

117. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-c). **Doughty discloses that the mobile phone further comprises smartcard circuitry** (*e.g.*, “smart card interface 324”) **coupled to the processor** (*e.g.*, “device processor or controller 314”). *E.g.*, Doughty:

- **Fig. 3:**



- [0040]: “[T]he 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.”
- [0045]: “**The device 302 may also include a user interface 320 that is communicably coupled to the device processor 314** and electrically connected to the power source 316 (via power management unit 318). The user interface 320 may include a touch pad, one or more buttons, a display, a voice sensor or other known user interfaces. **The device 302 may also include a contactless interface 322 that is communicably coupled to the device processor 314** and electrically connected to the power source 316 (via power management unit 318). The contactless interface 322 may include an antenna for wireless communication, an optical transceiver or other known contactless communication methods. **In addition, device 302 may also include a smart card interface 324 that is communicably coupled to the device processor 314** and electrically connected to the

power source 316 (via power management unit 318). *Moreover, device 302 may include an optical or other type of input/output (VO) interface 326 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318).*”

- [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.”
- [0047]: “The *one or more system interfaces 304* may include a device initialization interface 328, magnetic reader 330, a wireless communications interface (transceiver) 332, *a smart card reader 334*, or an optical or other input/output interface 336. *The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly*, depending on the desired application and implementation...”
- [0054]: “*Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown.* The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. *The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.* The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), *detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3)* or receiving data from a user interface

(e.g., 320 FIG. 3). ... If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716.”

- **[0055]:** “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.”

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

119. Doughty further discloses that the user device 302 includes “smart card interface 324.” Fig. 3, [0040], [0045], [0046]. In this regard, Doughty further discloses that “smart card interface 324” is a smartcard chip, as illustrated in Figure 4A. Doughty, [0048], Fig. 4A. At minimum, a person of ordinary skill in the art would have at least found it obvious to use a smartcard chip for the smart card interface 324 as a known mechanism for communicating with a smartcard reader. For example, U.S. Patent App. Pub. 2004/0235450 (filed May 19, 2004 and published November 25, 2004), discloses that “Smartcard chips” will “interact[] with a Smartcard reader using software applications stored on the chip.” Ex. 1031, [0004] (also recognizing that “[t]he operating system and breadth of applications on the smart chip are not necessarily important . . . as long as it is an open platform that can interface with a Smartcard reader and provide payment information to the

merchant's POS terminal”).

120. Doughty also discloses that the user device 302 communicates with “one or more system interfaces 304,” including “smart card reader 334.” Fig. 3, [0040], [0047]. Thus, “smart card interface” 324 enables “user device 302” to communicate with “smart card reader 334.”⁵

121. Doughty further discloses that “smart card interface 324” is “communicably coupled to the device processor 314.” Fig. 3, [0045].

122. To the extent it is argued that further disclosure is required for the smartcard circuitry, the user device 302 is smartcard card circuitry that performs transactions. As I noted above, the user device performs transactions using the smart card interface 324. In this situation, the processor 314 is coupled to all other circuitry in the device 302 such that processor 314 is coupled to the smartcard circuitry, as illustrated in Fig. 3.

h. Claim 8

123. **Claim 8 recites “The mobile phone of claim 1 wherein the time-varying magnetic field is used to perform point-of-sale transactions.”** This element is met by Doughty.

⁵ I note that this is consistent with the '423 patent disclosure of “smartcard circuitry.” For example, the '423 patent discloses that “[m]agnetic/smartcard circuitry 2030 may include circuits to produce...signals compatible with a smart card reader.” '423 patent, 11:8-10.

124. See my discussion of the elements of claim 1 above (Sections IX.A.4.a-c). **Doughty discloses that the time-varying magnetic field** (*e.g.*, “time-varying magnetic signal”) **is used to perform point-of-sale transactions** (*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. 19:**

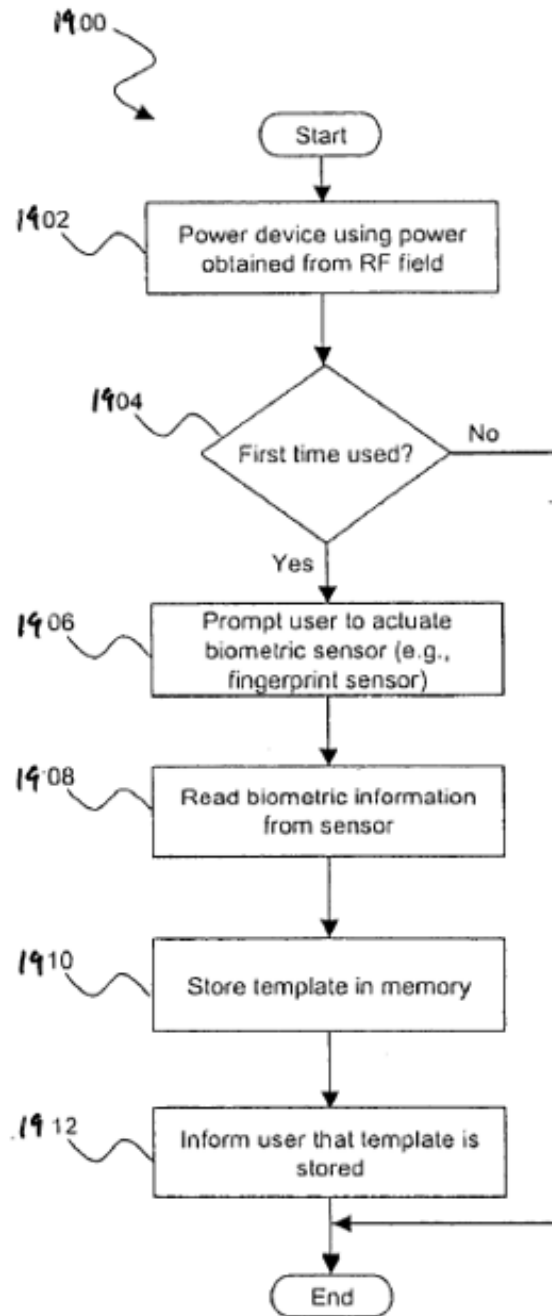


Fig. 19

- **Fig. 20:**

“point-of-sale
transactions”

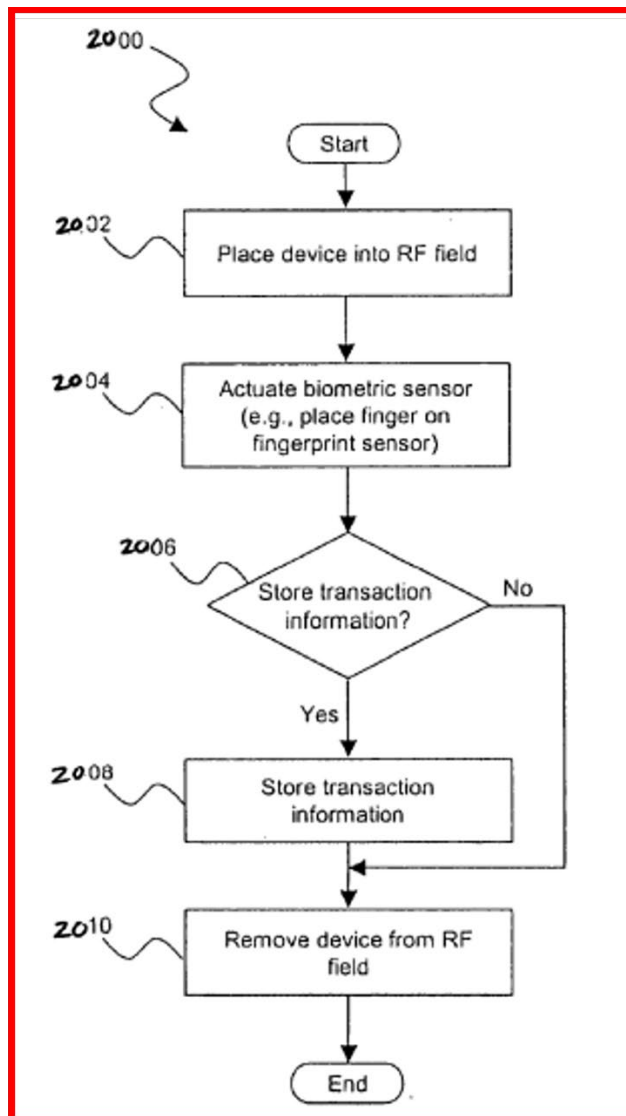


Fig. 20

- [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 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.”

- [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.”

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

126. Doughty discloses that “the present invention provides a secure and flexible system for security and/or commercial transactions using...credit...cards and/or devices.” [0038]. For example, the financial data includes data “such as a user name, user number, device expiration date,” which is credit card data. [0041]. In my

opinion, a person of ordinary skill in the art would have understood and at minimum found obvious that this “binary data to enable a transaction” comprises credit card data to advantageously use the device for commercial transactions involving credit cards, especially because 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. Furthermore, a person of ordinary skill in the art would have understood that credit card transactions are performed using point of sale terminals. For example, U.S. Patent No. 5,466,919 (issued November 14, 1995) discloses that credit cards are used to perform transactions at point of sale terminals. Ex. 1032, 3:1-4 (disclosing “established goods and services networks [which] include a series of merchant point of sale terminals [] located at sites where holders of credit cards may seek to obtain goods or services.”).

127. 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]-[0097]. 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.

128. 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, 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.

i. Element [9.pre]

129. **Element [9.pre] recites “A mobile phone comprising.”** This element is met by Doughty.

130. See my discussion of the element [1.pre] above (Section IX.A.4.a).

j. Element [9.a]

131. **Element [9.a] recites “circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card.”** This element is met by Doughty.

132. See my discussion of the element [1.a] above (Section IX.A.4.b).

k. Element [9.b]

133. **Element [9.b] recites “smartcard circuitry for performing transactions using single transaction account numbers.”** This element is met by Doughty in view of Bursch.

134. **Doughty discloses smartcard circuitry** (*e.g.*, “smart card interface 324”; *see* [5] (Section IX.A.4.g)) **for performing transactions** (*e.g.*, “enable any type of transaction”). *E.g.*, Doughty:

- **Fig. 3:**

"smartcard circuitry"

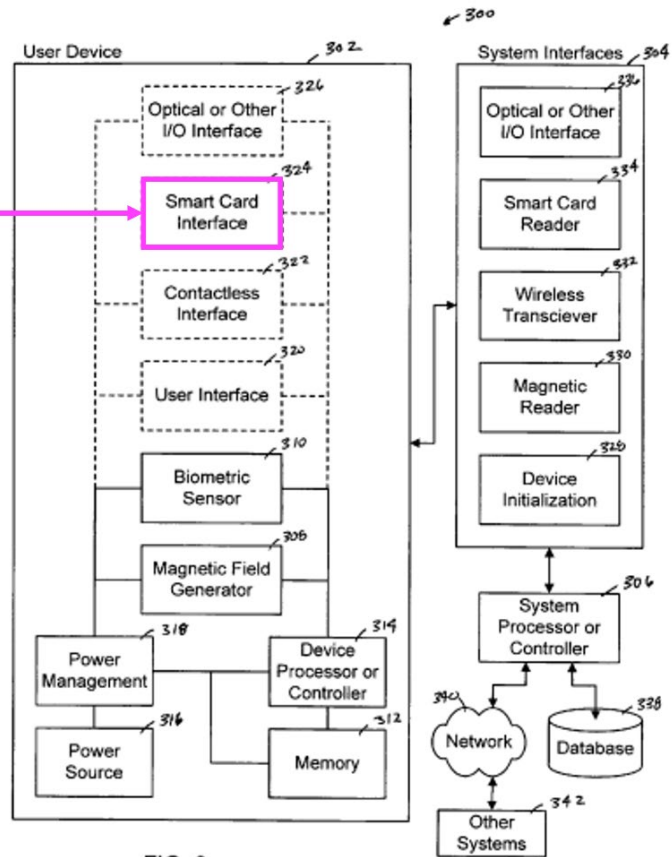
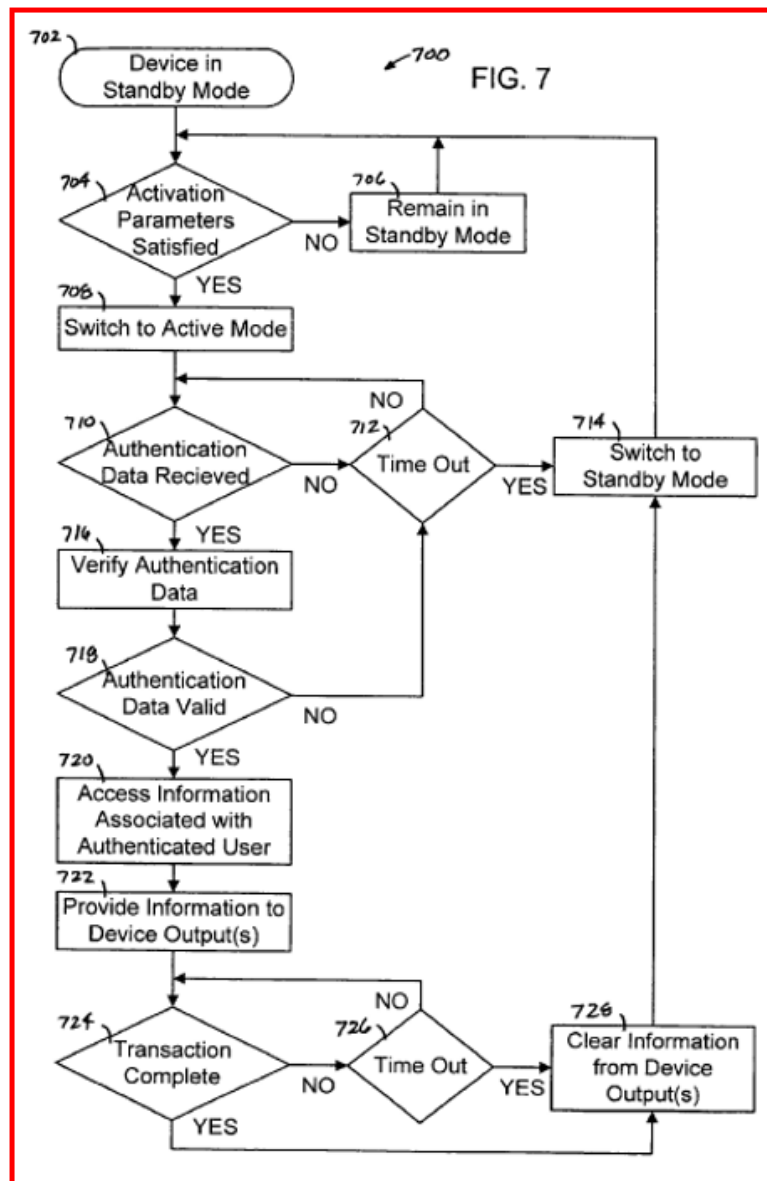


FIG. 3

- Fig. 7:

“performing transactions” →



- [0047]: “*The one or more system interfaces 304 may include a device initialization interface 328, a magnetic reader 330, a wireless communications interface (transceiver) 332, a smart card reader 334, or an optical or other input/output interface 336. The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly, depending on the desired application and implementation.*”
- [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.”

- [0054]: “Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. ***The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.*** The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), ***detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3)*** or receiving data from a user interface (e.g., 320 FIG. 3). ... If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716.”
- [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....*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.”

135. See my discussion of element [1.b] and claims 4, 5, and 8 above (Sections IX.A.4.c, f, g, and h).

136. Doughty further discloses that smart card interface 324 is for “detecting an external signal” and acting as a “device output” for communication with another device, such as a “smart card reader 334.”⁶ [0047], [0054], [0055], Fig. 3.

⁶ I note that implementation of a smartcard circuit as communicating with a smartcard reader is consistent with the ’423 patent. In the ’423 patent, the only description of “smart card circuitry” “for performing transactions” is that “smartcard circuitry 2030” includes “circuits to produce...signals compatible with a smart card reader.” ’423 patent, 11:8-10.

137. Moreover, Doughty discloses that the “device 300 [*sic*, 302]”⁷ from “FIG. 3” uses smart card interface 324 in “an exemplary authentication method 700” to “enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.” [0054], Fig. 7. For example, Doughty discloses that, in block 722 of the transaction method, “the information associated with the authenticated user,” such as information “required to enable or complete the transaction,” is “provided to the device outputs,” including smart card interface 324, and then in the subsequent block 724, the transaction is complete. [0055].

138. In my opinion, to the extent it is argued that further disclosure is required for the smartcard circuitry, the user device 302 is smartcard card circuitry that performs transactions. As I noted above, the user device performs transactions using the smart card interface 324.

139. **Bursch discloses performing transactions using single transaction account numbers** (*e.g.*, “single-use transaction numbers” are used to “make purchases of goods and services”). *E.g.*, Bursch:

⁷ Earlier, Doughty refers to “system 300,” but when “device 300” is raised later in Doughty in the context of Figure 7, it identifies this as an example of a “device,” and not a system. [0054].

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

141. As I discussed in Section IX.A.3, a person of ordinary skill in the art would have been motivated to apply Bursch's teachings of using single-use transaction numbers to perform transactions to Doughty's telecommunications device to perform transactions using single transaction account numbers.

I. Element [9.c]

142. **Element [9.c] recites “a processor coupled to the smartcard circuitry and the circuitry to produce a time-varying magnetic field.”** This element is met by Doughty.

143. **Doughty discloses a processor** (*e.g.*, “device processor or controller 314”) **coupled to the smartcard circuitry** (*e.g.*, “smart card interface 324”; *see* [9.b] (Section IX.A.4.k)) **and the circuitry to produce a time-varying magnetic field** (*e.g.*, “magnetic field generator 308”; *see* [1.a] (Section IX.A.4.b)).

144. See my discussion of elements [1.a]-[1.b] and [9.a]-[9.b] and claim 5 above (Sections IX.A.4.b, c, g, j and k).

145. Doughty further discloses the processor 314 is coupled to smart card interface 324 and magnetic field generator 308 as illustrated in Fig. 3.

146. In the case where the user device 302 is smartcard circuitry, the processor 314 is coupled to all other circuitry in the device 302 such that processor 314 is coupled to the smartcard circuitry, as illustrated in Fig. 3.

m. Claim 10

147. **Claim 10** recites “**The mobile phone of claim 9 wherein the smartcard circuitry is configured to perform point-of-sale transactions.**” This element is met by Doughty.

148. See my discussion of the elements of claim 9 above (Sections IX.A.4.i-l). **Doughty discloses that the smartcard circuitry** (*e.g.*, “smart card interface 324”) **is configured to perform point-of-sale transactions** (*e.g.*, “any type of transaction” including transactions with a “point-of-sale device”). *E.g.*, Doughty:

149. See my discussion of elements [1.b] and [9.c] and claim 8 above (Sections IX.A.4.c, h, and l).

150. As I explain in connection with claim 8 (Section IX.A.4.h), Doughty discloses device 302 is used for point-of-sale transactions. Doughty also discloses that any of the interfaces of device 302 (including smart card interface 324) is usable to perform a transaction. [0054]-[0055]. Thus, for the same reasons I discuss above for claim 8 with respect to the time-varying magnetic signal of Doughty being used for point-of-sale transactions, in my opinion, a person of ordinary skill in the art would have understood, or at minimum found it obvious, that the “smart card interface 324” is similarly used to perform transactions, such as point-of-sale transactions.

151. In the case where the user device 302 is smartcard circuitry, as I explain

in the previous paragraph, the device 302 is configured to perform point-of-sale transactions.

n. Claim 11

152. **Claim 11** recites “**The mobile phone of claim 9 wherein the transactions are financial transactions.**” This element is met by Doughty.

153. See my discussion of claims 3, 9, and 10 above (Sections IX.A.4.e, i-l, and m).

o. Claim 12

154. **Claim 12** recites “**The mobile phone of claim 9 wherein the time-varying magnetic field mimics a swipe of a magnetic credit card.**” This element is met by Doughty.

155. See my discussion of the claims 2 and 9 above (Sections IX.A.4.d and i-l).

p. Claim 13

156. **Claim 13** recites “**The mobile phone of claim 9 wherein the single transaction account numbers have a pre-defined sequence.**” This element is met by Bursch.

157. See my discussion of the elements of claim 9 above (Sections IX.A.4.i-l). **Bursch discloses that the single transaction account numbers (see [1.b]) have a pre-defined sequence (e.g., “exact sequence unique to the transaction number generator”).** *E.g.*, Bursch:

- **2:33-44:** *“For each transaction number generator issued by an issuing institution to an authorized user, the issuing institute maintains a copy of the transaction number generator referred to as a transaction number validator. This transaction number validator is capable of generating the exact sequence unique to the transaction number generator. In this manner, the issuing institution can generate transaction numbers that are identical to the transaction numbers that the institution expects to receive from the authorized user of the transaction number generator. The issuing institution uses the transaction number validator to validate or invalidate transaction numbers as they are received in conjunction with intended transactions.”*
- **5:9-27:** *“To prevent invalidating legitimately used transaction numbers, an issuing institution could generate and maintain a list of expected transaction numbers for each authorized user. Whenever the issuing institution receives a transaction number corresponding to a proposed purchase, the institution compares the received transaction to each transaction number in the list of expected transaction numbers. If any of the transaction numbers in the list of expected transaction numbers matches the received transaction number, then the transaction is validated or allowed. If none of the expected numbers matches the received number, then the transaction is invalidated or not allowed. Each time a received transaction number is validated it can be removed from the list of expected numbers and replaced by the next transaction number generated. As long as the size of the list of expected transaction numbers is small relative to the number of different transaction numbers in each user's unique sequence of transaction numbers, the probability of an unauthorized person guessing a valid number remains very small.”*

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

159. Bursch further discloses that a user generates a sequence of single-use transaction numbers that is identical to a sequence generated by an issuing institution, confirming that the numbers have a pre-defined sequence. 2:33-44. For example, Bursch discloses that an issuing institute maintains a “transaction number validator” for “each transaction number generator” issued to a user, and that the

transaction number validator and the transaction number generator generate identical sequences of transaction numbers. 2:33-44. Because both the user's device and the issuing institute produce numbers in the same predetermined order, the issuing institute is able to validate transactions performed by the user. 2:33-44.

160. As I discussed in Section IX.A.3, a person of ordinary skill in the art would have been motivated to apply Bursch's teachings of using single-use transaction numbers in a predefined order to perform transactions to Doughty's telecommunications device.

q. Claim 14

161. **Claim 14 recites “The mobile phone of claim 9 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.”** This element is met by Bursch.

162. See my discussion of the elements of claim 9 above (Sections IX.A.4.i-1). **Bursch discloses that the single transaction account numbers** (*see* [1.b] (Section IX.A.4.c)) **comprise pre-assigned single-use transaction numbers** (*e.g.*, “single-use, transaction number” are created from an “exact sequence unique to the transaction number generator”). *E.g.*, Bursch:

163. See my discussion of element [1.b] and claim [13] above (Sections IX.A.4.c and p). As I explain for claim [13] (Section IX.A.4.p), the “single-use, transaction numbers” are “preassigned” by the issuing institution.

164. As I discussed in Section IX.A.3, a person of ordinary skill in the art would have been motivated to apply Bursch's teachings of using single-use transaction numbers in a predefined order to perform transactions to Doughty's telecommunications device.

r. Element [15.pre]

165. **Element [15.pre]** recites **"A mobile phone comprising."** This element is met by Doughty.

166. See my discussion of the element [1.pre] above (Section IX.A.4.a).

s. Element [15.a]

167. **Element [15.a]** recites **"circuitry to produce a time-varying magnetic field that mimics a swipe of a magnetic card."** This element is met by Doughty.

168. See my discussion of the element [1.a] above (Section IX.A.4.b).

t. Element [15.b]

169. **Element [15.b]** recites **"circuitry to enable use of single transaction account numbers."** This element is met by Doughty in view of Bursch.

170. **Doughty discloses circuitry** (*e.g.*, "smart card interface 324") **to enable transactions** (*e.g.*, "enable any type of transaction"). *E.g.*, Doughty:

- **Fig. 3:**

"smartcard circuitry"

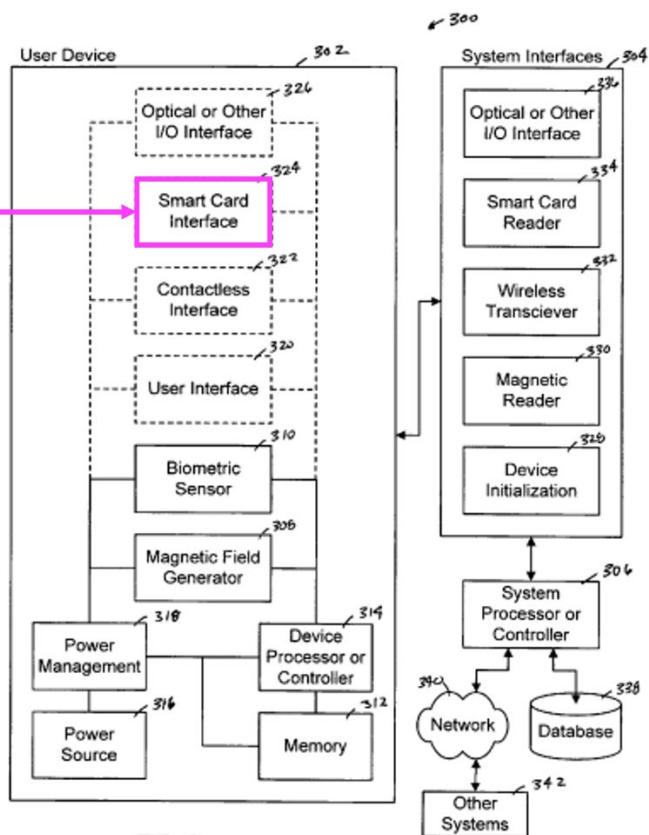
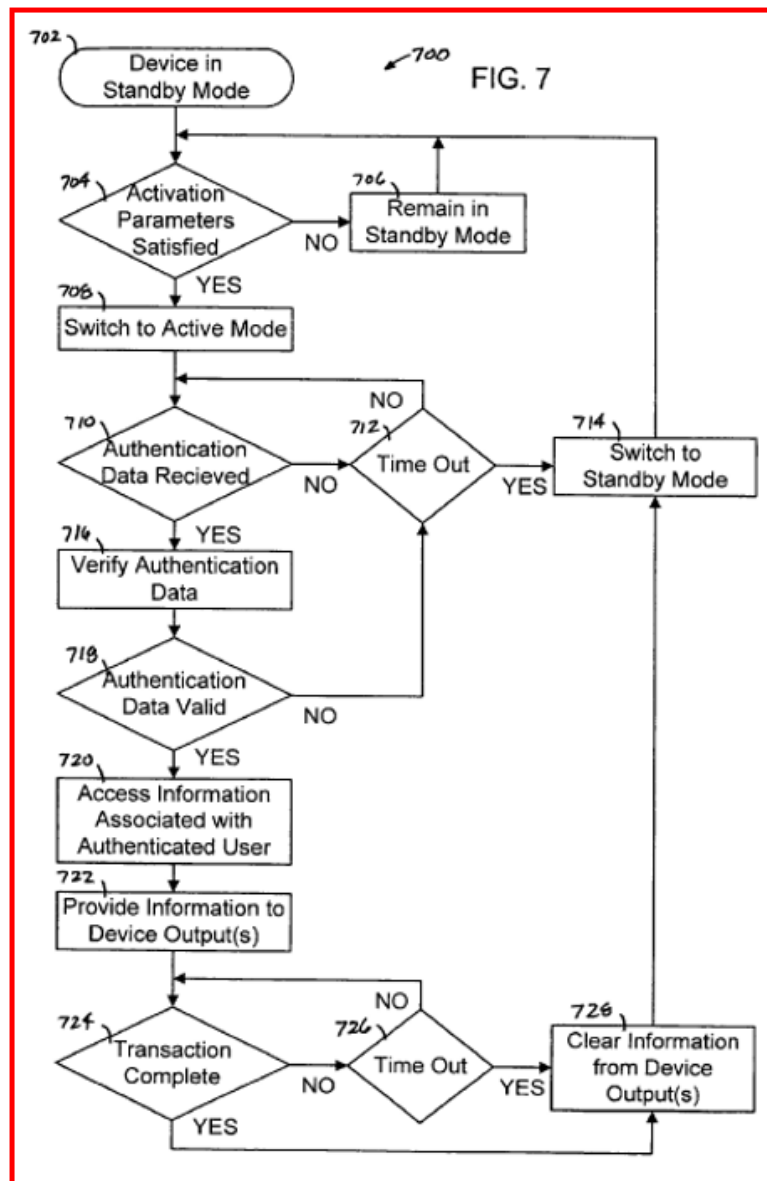


FIG. 3

- Fig. 7:

“performing transactions” →



- [0047]: “*The one or more system interfaces 304 may include a device initialization interface 328, a magnetic reader 330, a wireless communications interface (transceiver) 332, a smart card reader 334, or an optical or other input/output interface 336. The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly, depending on the desired application and implementation.*”
- [0054]: “*Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG.*

- 3), *in accordance with the present invention is shown*. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. *The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.* ... The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), *detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3)* or receiving data from a user interface (e.g., 320 FIG. 3). ... If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716.”
- [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....*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.”

171. See my discussion of element [1.a] and claims [4], [5], and [8] above (Sections IX.A.4.b, f, g, and h).

172. Doughty further discloses that smart card interface 324 is for “detecting an external signal” and acting as a “device output” for communication with another device, such as a “smart card reader 334.” [0047], [0054], [0055], Fig. 3.

173. Moreover, Doughty discloses that the “device 300 [*sic*, 302]” from “FIG. 3” uses smart card interface 324 in “an exemplary authentication method 700” to “enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.” [0054], Fig. 7. For example, Doughty discloses that, in block 722 of the transaction method, “the information associated with the authenticated user,” such as information “required to enable or complete the transaction,” is “provided to the device outputs,” including smart card interface 324, and then in the subsequent block 724, the transaction is complete. [0055].

174. **Bursch discloses transactions using single transaction account numbers** (*e.g.*, “single-use transaction numbers” are used to “make purchases of goods and services”). *E.g.*, Bursch:

175. See my discussion of elements [1.b] and [9.b] above (Sections IX.A.4.c and k).

176. As I discussed in Section IX.A.3 above, a person of ordinary skill in the art would have been motivated to apply Bursch’s teachings of using single-use transaction numbers to perform transactions to Doughty’s telecommunications device.

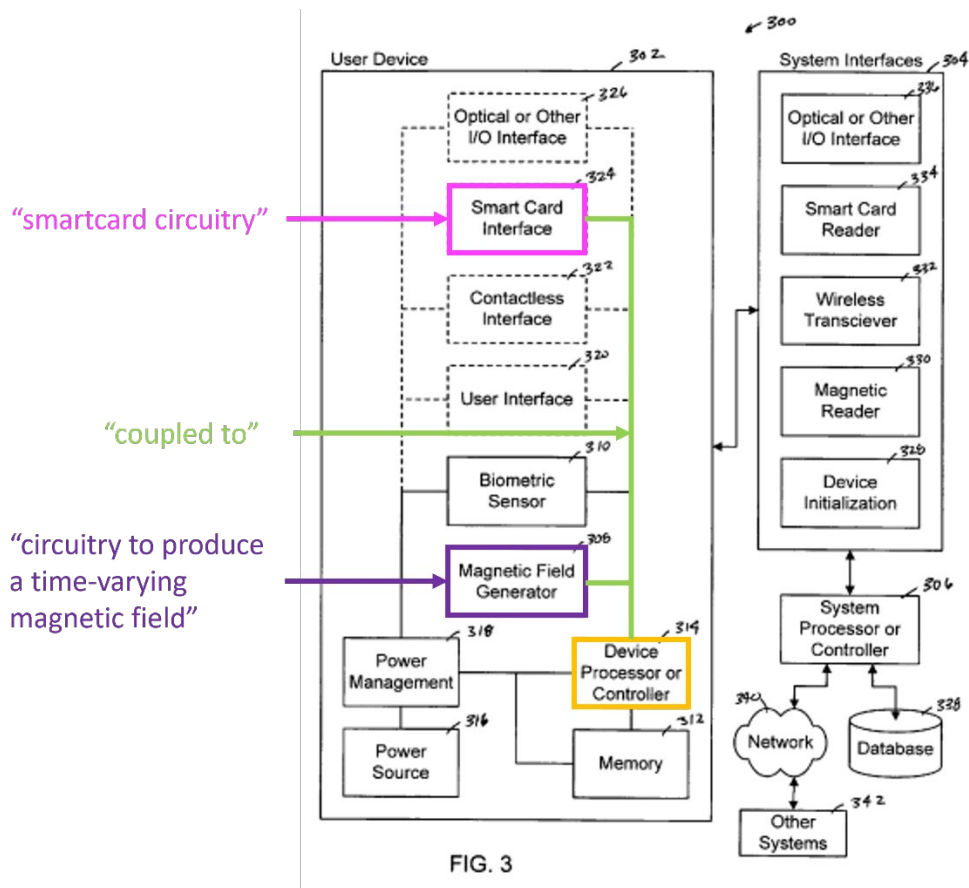
u. Element [15.c]

177. **Element [15.c] recites “a processor coupled to the circuitry to**

produce a time-varying magnetic field and to the circuitry to enable use of single transaction account numbers, the processor configured to cause a time-varying magnetic field to be produced that represents a single transaction account number.” This element is met by Doughty in view of Bursch.

178. **Doughty discloses a processor** (*e.g.*, “device processor or controller 314”) **coupled to the circuitry to produce a time-varying magnetic field** (*e.g.*, “magnetic field generator 308”; *see* [1.b] (Section IX.A.4.c)) **and to the circuitry to enable transactions** (*e.g.*, “smart card interface 324” to “enable any type of transaction”; *see* [15.b] (Section IX.A.4.t)), **the processor configured to cause a time-varying magnetic field to be produced** (*e.g.*, “to...activate the magnetic field generator 308” to “creat[e]...a time-varying magnetic signal”; *see* [1.b] (Section IX.A.4.c)). *E.g.*, Doughty:

- **Fig. 3:**



179. See my discussion of elements [1.a]-[1.b], [9.a]-[9.b] and [15.a]-[15.b] and claim 5 above (Sections IX.A.4.b-c, g, j-k and s-t). Doughty further discloses the processor 314 is coupled to smart card interface 324 and magnetic field generator 308 as illustrated in Fig. 3.

180. **Bursch discloses transactions using single transaction account numbers** (e.g., “single-use transaction numbers” are used to “make purchases of goods and services”). E.g., Bursch:

181. See my discussion of elements [1.b] and [9.b] above (Sections IX.A.4.c and k). As I discussed in [1.b] (Section IX.A.4.c) and [9.b] (Section IX.A.4.k) above,

a person of ordinary skill in the art would have been motivated to apply Bursch's teachings of using single-use transaction numbers to perform transactions to Doughty's telecommunications device.

v. Claim 16

182. **Claim 16 recites “The mobile phone of claim 15 wherein the circuitry to enable use of single transaction account numbers comprises smartcard circuitry.”** This element is met by Doughty in view of Bursch.

183. See my discussion of the element [9.b] and claim [15] above (Sections IX.A.4.k and r-u).

w. Claim 17

184. **Claim 17 recites “The mobile phone of claim 15 wherein the single transaction account numbers have a pre-defined sequence.”** This element is met by Doughty in view of Bursch.

185. See my discussion of the claims [13] and [15] above (Sections IX.A.4.p and r-u).

x. Claim 18

186. **Claim 18 recites “The mobile phone of claim 15 wherein the single transaction account numbers comprise pre-assigned single-use transaction numbers.”** This element is met by Doughty in view of Bursch.

187. See my discussion of the claims [14] and [15] above (Sections IX.A.4.q and r-u).

B. Ground 2: Doughty in view of Bursch and Fox (U.S. Patent 5,943,624) (Claims 1-5, 8-18)

188. To the extent it is argued that further disclosure is required for a mobile phone (claims 1-5, 8-18), Fox discloses that the mobile device is a mobile phone (e.g., “cellular telephone 10”).

189. 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, Abstract, 2:10-29.

190. Like Doughty and Bursch, Fox is analogous art, and in the same field as the ’423 patent, which includes securely performing electronic transactions on mobile devices, and are reasonably pertinent to purported problems addressed by the named inventors of the ’423 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.

191. In my opinion, a person of ordinary skill in the art would have been motivated to apply Fox’s teaching of implementing smartcard functionality in a mobile telephone to Doughty’s “telecommunications device” (as modified by Bursch). 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 Fox, which teaches examples of such

telecommunications devices in which to implement smartcard functionality, including a mobile telephone. Doughty, [0038], [0040]. For example, Fox explains that integration of smartcard functionality into a mobile phone provides numerous advantages, including “ease of use of the smartcard, enhanced security from theft or loss, the ability to read and access information stored within the smartcard by utilizing the cellular telephone display for displaying available smartcard functions, and the ability to update/change information stored within the smartcard by utilizing the cellular telephone functions to electronically communicate with an external system.” Fox, 2:21-29. For example, 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 carry the smartcard functionality in 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, in my opinion, have found it straightforward and advantageous to apply Fox’s teachings to Doughty (as modified by Bursch) given Doughty’s teaching that its system could be implemented in a variety of mobile devices, including a “telecommunications device.” Doughty, [0046].

192. It therefore is my opinion that a person of ordinary skill in the art would have had a reasonable expectation of success applying Fox’s teachings to Doughty’s

telecommunications device (as modified by Bursch), and would have known such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

X. SECONDARY CONSIDERATIONS

193. The Challenged Claims of the '423 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.

194. There is no evidence in the '423 patent's prosecution history or elsewhere supporting any secondary considerations arguments, or evidence of any nexus to any particular claim of the '423 patent. *See generally* '423 File History. As demonstrated by the prior art discussed above, any purported solutions to problems or unexpected results in the '423 patent were already well known. *Id.*

195. 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.

196. 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

197. In summary, I have concluded that the Challenged Claims are rendered obvious over the prior art references as I discussed above. Specifically, in my opinion, for at least the reasons above, the Challenged Claims of the '423 patent obvious.

198. 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.

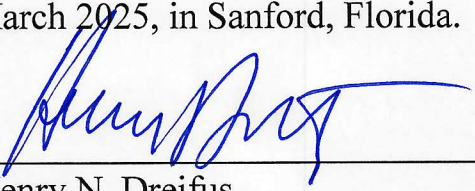
199. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me.

200. 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.

201. 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.

202. Executed this 10th 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.

HENRY N. DREIFUS

Page 2.

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-sensor 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' ASSOCIATION (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.

HENRY N. DREIFUS

Page 11.

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 Emanuel
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

Summary of Henry N. Dreifus Expert Witness Client Support

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

Summary of Henry N. Dreifus Expert Witness Client Support

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

Summary of Henry N. Dreifus Expert Witness Client Support

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. 9,208,423 (“’423”)
1002	File History of U.S. Application No. 14/833,113 (“’423FH”)
1004	U.S. Patent App. Pub. 2011/0240748 (“Doughty-CON”)
1005	U.S. Patent App. Pub. 2004/0133787 (“Doughty”)
1006	U.S. Patent No. 11,270,174 (“’174”)
1007	File History of U.S. Application No. 17/021,347 (“’174FH”)
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”)
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”)
1031	U.S. Patent App. Pub. 20040235450 (“Rosenberg”)
1032	U.S. Patent No. 5,466,919 (“Hovakimian”)
1037	U.S. Patent No. 5,955,961 (“Wallerstein”)

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