

**IN THE UNITED STATES PATENT
AND TRADEMARK OFFICE**

**BEFORE THE PATENT TRIAL AND APPEAL
BOARD**

GOOGLE LLC,
Petitioner

v.

CARDWARE INC.,
Patent Owner

U.S. Patent No. 10,339,520
Issued: July 2, 2019

Title: MULTI-FUNCTIONAL CREDIT CARD
TYPE PORTABLE ELECTRONIC DEVICE

DECLARATION OF MICHAEL I. SHAMOS, PH.D.

TABLE OF CONTENTS

	Page
I. INTRODUCTION AND QUALIFICATIONS	1
II. SUMMARY OF MY OPINIONS	4
III. UNDERSTANDING OF THE GOVERNING LAW	4
A. Invalidity By Obviousness	4
B. Relevant Time Period for the Obviousness Analysis.....	7
C. Materials Considered.....	8
IV. RELATED LITIGATION	8
V. OVERVIEW OF THE '520 PATENT	8
VI. THE '520 PROSECUTION HISTORY	11
VII. LEVEL OF ORDINARY SKILL IN THE ART IN THE RELEVANT TIMEFRAME	12
VIII. TECHNOLOGY BACKGROUND.....	14
A. Cryptographic Hashing	15
B. Near-Field Communication (NFC) Interfaces	16
C. Touch Sensor Arrays	18
D. Static and Limited-Use Numbers	20
E. Sequence Counters	23
F. Payment Method Types.....	24
G. Contactless ATMs	25
IX. CLAIM CONSTRUCTION	31
X. OVERVIEW OF PRIOR ART REFERENCES.....	31
A. U.S. Patent Application Publication 2015/0134540 (“Law”).....	31
B. U.S. Patent 9,600,808 (“Gomez”).....	36
C. U.S. Patent Application Publication 2012/0123937 (“Spodak”).....	39
D. U.S. Patent 9,098,846 (“Gill”)	42
E. U.S. Patent Application Publication 2013/0232083 (“Smith”)	45
F. U.S. Patent Application Publication 2013/0124410 (“Kay”)	47
XI. THE CHALLENGED CLAIMS ARE INVALID.....	48

TABLE OF CONTENTS

(continued)

Page

A.	Ground 1A: Claims 10-13 of the '520 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Law in view of Gomez.....	48
1.	Motivation to Combine Law and Gomez	48
2.	Claim 10.....	53
3.	Claim 11	72
4.	Claim 12	73
5.	Claim 13	76
B.	Ground 1B: Claims 14-17 of the '520 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Law in view of Gomez and Spodak.....	76
1.	Claim 14	76
2.	Claim 15.....	79
3.	Claim 16.....	80
4.	Claim 17	81
C.	Ground 2A: Claims 18-24 of the '520 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gill in view of Smith, Kay, and Gomez.....	82
1.	Motivation to Combine Gill, Smith, Kay, and Gomez.....	82
2.	Claim 18.....	94
3.	Claim 19	117
4.	Claim 20.....	120
5.	Claim 21	121
6.	Claim 22	122
7.	Claim 23	124
8.	Claim 24.....	127
XII.	JURAT	127

I, Dr. Michael I Shamos, hereby declare as follows:

I. INTRODUCTION AND QUALIFICATIONS

1. I have been retained by Google LLC (“Google”) to provide my opinions concerning the validity of claims 10-24 (“Challenged Claims”) of U.S. Patent No. 10,339,520 (“’520 Patent” or the “Patent”) in support of Google’s Petition for *Inter Partes* Review of the Patent (the “Petition”).

2. I am being compensated at a rate of \$625 per hour for my work in this proceeding and my compensation is in no way contingent on the nature of my findings, the presentation of my finding in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding or in Patent Owner. It is conceivable that I may own investments in mutual funds which themselves own shares in Patent Owner. I have no knowledge of any such holder, which, in any event, would not constitute a material portion of my net worth.

3. A detailed description of my professional qualifications, including a listing of my specialties/expertise and professional activities, is contained in my curriculum vitae, a copy of which is provided as Exhibit 1014. Below is a short summary of my professional qualifications.

4. I have a A.B. degree from Princeton University in Physics (1968), a M.A. degree from Vassar College in Physics (1970), a M.S. degree from American University in Technology of Management (1972), a M.S. degree from Yale

University in Computer Science (1973), a M. Phil. from Yale University in Computer Science (1974), a Ph.D. from Yale University in Computer Science (1978), and a J.D. degree from Duquesne University (1981).

5. I currently hold the title of Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. I am a member of two departments in that School, the Institute for Software Research and the Language Technologies Institute. I was a founder and Co-Director of the Institute for eCommerce at Carnegie Mellon from 1998-2004 and from 2004-2018 was Director of the eBusiness Technology graduate program in the Carnegie Mellon University School of Computer Science. Since 2018, I have been Director of the M.S. in Artificial Intelligence and Innovation degree program at Carnegie Mellon.

6. I have taught graduate courses at Carnegie Mellon in Electronic Commerce from 1999-present, including eCommerce Technology, Electronic Payment Systems, Electronic Voting, Internet of Things, Ubiquitous Computing, Electronic Payment Systems and eCommerce Law and Regulation, as well as Analysis of Algorithms. Since 2007, I have taught an annual course in Law of Computer Technology. I currently also teach Artificial Intelligence and Future Markets.

7. From 2001-2021, I was a Visiting Professor at the University of Hong Kong, where I taught an annual course in Electronic Payment Systems. This was one

of only a handful of graduate courses taught on this subject in the world.

8. I was the Director of Carnegie Mellon's graduate degree program in eBusiness Technology from 1999-2018 and am now a faculty member in the Privacy Engineering degree program at Carnegie Mellon. My course on Law of Computer Technology is required for all students in that program and in the Societal Computing Ph.D. program. My principal role currently is as Director of the graduate program in Artificial Intelligence and Innovation.

9. From 1979-1987 I was the founder and president of two computer software development companies in Pittsburgh, Pennsylvania, Unilogic, Ltd. and Lexeme Corporation.

10. I am an attorney admitted to practice in Pennsylvania and have been admitted to the Bar of the U.S. Patent and Trademark Office since 1981. I have been asked to render opinions in this Declaration as a technical expert. I have not been asked to offer any opinions on patent law in this proceeding.

11. I am a named co-inventor on the following six issued patents relating to electronic commerce: U.S. Patent Nos. 7,330,839, 7,421,278, 7,747,465, 8,195,197, 8,280,773, and 9,456,299.

12. I have previously served as an expert in over 400 cases concerning computer technology. In particular, I have been involved in more than 45 cases involving electronic payment systems.

13. The statements made and opinions provided in this Declaration are based on my own personal knowledge and, if called as a witness, I could and would testify in a manner consistent with this Declaration.

II. SUMMARY OF MY OPINIONS

14. It is my understanding that the following table summarizes the grounds of challenge (“Grounds”) raised in the Petition:

15. Ground 1A: Claims 10-13 are unpatentable under 35 U.S.C. § 103 as being obvious in view of Law (EX1032) and Gomez (EX1007).

16. Ground 1B: Claims 14-17 are unpatentable under § 103 as being obvious in view of Law, Gomez, and Spodak (EX1009).

17. Ground 2A: Claims 18-24 are unpatentable under § 103 as being obvious in view of Gill (EX1034), Smith (EX1035), Kay (EX1036), and Gomez.

18. After a review of the ’520 Patent and the prior art asserted by Petitioner, it is my opinion that the Challenged Claims are invalid for obviousness. My opinions, and the bases therefor, are detailed throughout this Declaration.

III. UNDERSTANDING OF THE GOVERNING LAW

A. Invalidity By Obviousness

19. I understand that obviousness of a claim requires that the claim as a whole be obvious from the perspective of a person of ordinary skill in the relevant art (“POSITA”), at the time of invention. A claim is unpatentable for obviousness

under 35 U.S.C. § 103 “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” Obviousness may be based upon a combination of references.

20. If a patented invention is a combination of known elements, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue by considering the teachings of prior art references, the effects of demands known to people working in the field or present in the marketplace, and the background knowledge possessed by a POSITA. Identifying a reason the elements should be combined is important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, was already known. The prior art references themselves may provide a suggestion, motivation, or reason to combine, but the nexus linking two or more prior art references is sometimes simple common sense.

21. An obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the pertinent art; and (4) any objective indicia of non-obviousness, such as commercial success, long-felt but unresolved

need, failure of others, industry recognition, copying, and unexpected results.

22. If a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond their skill.

23. Practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. A POSITA looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. An obviousness analysis therefore considers the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

24. A proper obviousness analysis focuses on what was known or obvious to a POSITA at the time of invention, not to the patentee. Accordingly, 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.

25. Prior art teachings are properly combined if one of ordinary skill, having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the

time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

26. I understand that in an *inter partes* review, “the petitioner shall have the burden of proving a proposition of unpatentability,” including a proposition of obviousness, “by a preponderance of the evidence.” 35 U.S.C. §316(e).

B. Relevant Time Period for the Obviousness Analysis

27. I understand that the ’520 Patent claims priority to U.S. Provisional Patent Application 61/794,891 (“’891 Provisional”), filed on March 15, 2013. I have been asked, for purposes of this proceeding only, to treat March 15, 2013 as the Critical Date in my analysis. However, my opinions as to the obviousness of claims 10-24 of the ’520 Patent would remain substantially unchanged even if a later date were deemed to be the Critical Date and if AIA §§ 102 and 103 were to apply. I understand that Petitioner does not concede that any of the Challenged Claims enjoy priority to the ’891 Provisional. However, I have been asked to assume, for purposes of this proceeding only, that pre-AIA 35 U.S. §§ 102 and 103 apply.

28. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the ’520 Patent. Unless otherwise stated, my testimony below refers to the knowledge of a POSITA as of the Critical Date, or before. Any annotated Figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the ’520

Patent and the prior art discussed below.

C. Materials Considered

29. In forming my opinions, I have reviewed and am familiar with the '520 Patent and its prosecution history, the materials cited herein, and exhibits to the Petition.

IV. RELATED LITIGATION

30. I am aware that the parties are engaged in contemporaneous litigation styled *CardWare Inc. v. Google LLC*, Case No. 7:24-cv-00278 (W.D. Tex.) (the “Litigation”). In the Litigation, Patent Owner has accused Petitioner’s mobile phones as infringing the Challenged Claims, despite the fact that the Patent does not disclose any mobile phone invention, but instead is drawn to a payment card that can be read by a magnetic stripe reader. This accusation has compelled Patent Owner to interpret various claim terms in a manner that is at odds with the intrinsic evidence. I have therefore made occasional use of Patent Owner’s reading of the claims in forming my opinions.

V. OVERVIEW OF THE '520 PATENT

31. The '520 Patent was filed on September 11, 2017 and issued on July 2, 2019. Through a series of continuation and divisional applications and a provisional application, it claims priority to March 15, 2013. The '520 Patent discloses “a credit card device capable of generating a programmed magnetic field of alternating

polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card.” EX1001, Abstract. However, the Challenged Claims are not drawn to any such device, and do not claim “generating a programmed magnetic field” or any “emulation” of a “standard credit card.”

32. The '520 Patent discloses generating a “limited-duration number” for use in a payment transaction. EX1001, 2:24-29, 2:50-62, 10:3:11-55. Such a number is claimed as a “limited-use number,” whose use may be limited by time or number of transactions in which it may be used. FIG. 7 of the Patent is a flowchart illustrating a process for generating a limited-use number:

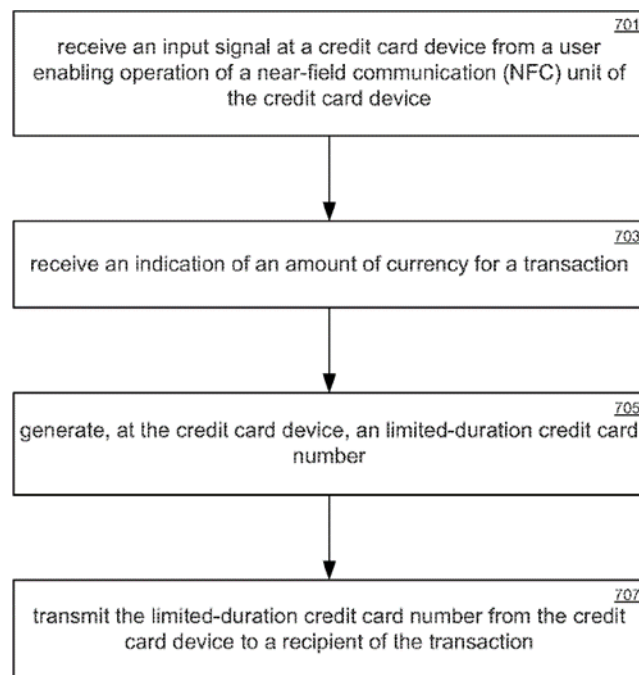


FIG. 7

EX1001, FIG. 7.

33. Various other portions of the Specification give further details of the generation of a limited-use number. For example, “[t]he credit card device comprises a real-time clock that is able to produce a cryptographically protected timestamp for each interaction.” *Id.*, 10:7-9. “The power source is able to activate the processor unit such that a unique number may be generated by the credit card device and verified by the credit authority according to the timestamp and the transmitted user information.” *Id.*, 10:9-13. “The limited duration credit card number is able to be produced at the time the credit card device is performing a transaction, and is able to be generated according to the user’s private information, a bank information, information regarding the facility performing the transaction, and the time of day.” *Id.*, 10:13-18. Further, the “limited-duration credit card number is able to be limited to only one transaction, a finite number of transactions, or may be limited to a specified period of time—e.g., 2 minutes, 10 minutes, 3 hours—after which time that particular limited-duration number would become invalid.” *Id.*, 10:18-23.

34. The Specification further explains how “the number on the front of the card” can be static, dynamic, or a combination of static and dynamic digits. *Id.*, 10:32-52. “For example, the first four and last four digits of the credit card number are able to be fixed, while the remaining eight digits can be dynamically generated.” *Id.*, 10:37-41.

VI. THE '520 PROSECUTION HISTORY

35. I have reviewed the prosecution history of the '520 Patent (EX1002) and those of its ancestors, all of which have the same specification.

36. The '520 Patent issued from Application No. 15/701,261, filed September 11, 2017, which was a continuation of the '884 Patent. The same Examiner issued a statutory double patenting rejection, which was overcome by amendment of December 11, 2018. Without issuing any further rejection, the Examiner allowed all pending claims on February 5, 2019, writing:

Sebastian et al. (US 2013/0297509) teaches a mobile payment using dynamic code. However, none of prior art teaches an electronic device to perform operations comprising accepting a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information, wherein the memory comprises device-specific and user-specific information, and, wherein the issuer provided payment information is communicated wirelessly, and, wirelessly receiving a static device account number payment information for storage on the electronic device, and wherein at least a portion of the payment information is a limited-use number for limited-use by the device, in place of a [sic] issuer provided payment information, and, dynamically-generating a one-time limited-use number based on at least one of a set of information including user-identifying information, user secrets, device information, device secrets, time, merchant, facility location, sequence count, payment information, account information, amount, and transaction information, and using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a

payment transaction, and using the electronic device for conducting transaction with an ATM as set forth in the claims.

'520 Prosecution History, Notice of Allowability, 2/5/2019, 2-3.

37. None of the prior art cited in the Petition was considered by the Examiner.

VII. LEVEL OF ORDINARY SKILL IN THE ART IN THE RELEVANT TIMEFRAME

38. The '520 Patent defines its field of invention as follows:

Embodiments according to the present disclosure generally relate to electronic or smart credit card devices and, more specifically, to more secure, smart credit card devices.

EX1001, 1:26-28.

39. The '520 Patent Specification asserts a need for security in credit cards that employ RFID technology:

A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

A concern with each of these types of credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise. Therefore, these types of credit cards have security limitations. Further, cards employing smart integrated circuit chips and RF technology are not in wide use at present because they are incompatible with existing

credit card infrastructure, which still predominantly supports conventional plastic credit cards.

EX1001, 1:56-2:4.

40. The Specification describes generating limited-use credit card numbers and using them to engage in secure payment transactions, including the use of cryptograph hash algorithms.

41. The claims of the '520 Patent recite features generally directed to communicating payment information using limited-use numbers.

42. In my opinion, in order to understand the Specification and make and use the claimed invention without undue experimentation at or near the Critical Date, one of ordinary skill in the art of the '520 Patent would have been someone with (1) a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and; (2) in addition, one to two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technologies such as RFID. Graduate education could substitute for professional experience, or significant experience in the field could substitute for education.

43. I qualify as at least a POSITA as of March 15, 2013, and I have a sufficient level of knowledge, experience and education to provide an opinion in the field of the '520 Patent. I am familiar with what a person of ordinary skill in the art knew in 2013 because of my lengthy experience with subjects similar to those of the

concepts presented in the '520 Patent. In addition, I was teaching such subjects prior to 2013. My analysis and opinions in this Declaration are made from the perspective of a POSITA as of March 15, 2013.

VIII. TECHNOLOGY BACKGROUND

44. In this section, I discuss the state of the art as of the Critical Date with respect to certain technologies relevant to the subject matter of the '520 Patent.

45. The art of credit card payments is extremely crowded and extensive. Prior to the Critical Date, over 50,000 U.S. patent applications and issued U.S. patents had been published containing the strings “credit card” and “payment.” Furthermore, major credit-card networks, such as Visa, MasterCard, Europay and EMV (“Europay-MasterCard-Visa”) had collaborated to develop industry-wide standards for credit card processing. Such standardization was necessary to enable the use of cards at tens of millions of merchants around the world, given that many different types of point-of-sale (POS) terminals were in use at various establishments. These standards set forth requirements for equipment and software used to process card payments.

46. One major standardization effort was undertaken by the Payment Card Industry (PCI), an association of organizations that store, process and transmit cardholder data. In 2006, American Express, Discover Financial Services, Japan Credit Bureau, MasterCard and Visa International formed the Payment Card

Industry Security Standards Council (PCI SSC) which, by 2014, included 688 “participating organizations.” PCI SSC issued a series of published security standards. As of the Critical Date, Version 2.0 of the PCI security standards were in effect, as described in “PCI Data Security Standard (PCI DSS) Version 2.0 January 2013,” (EX1022) and “Payment Card Industry (PCI) Data Security Standard Navigating PCI DSS Version 2.0 October 2010.” (EX1026)

A. Cryptographic Hashing

47. The PCI Standards describe the requirement of cryptographic hashing of card numbers. For example:

Protect Cardholder

Data Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

EX1026, 28.

3.4.a Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if

applicable). Verify that the PAN is rendered unreadable using any of the following methods: One-way hashes based on strong cryptography.

EX1026, 32.

48. A POSITA familiar with payment processing would have been familiar with these standards.

B. Near-Field Communication (NFC) Interfaces

49. A fundamental problem in electronic payments is how to communicate digital information, such as a credit card number, from the card itself or another device held by the user, to a POS device operated by a merchant. An early method was to provide the card with a magnetic stripe with encoded data including the credit card number. The user or merchant would then “swipe” the card through a magnetic reader of the POS device.

50. A later method was to build a processor chip into the card. The user or merchant would insert the card into a slot in the POS device, where electrical contact would be made with the chip, and payment data, including a credit card number, would be sent to the POS device.

51. A third method was to provide the card with a radio frequency identification (RFID) chip so that it could communicate wirelessly. The user would bring the card close to the POS device, and card information would be transmitted by radio waves over the very short distance between the card and the POS device.

The '520 Patent uses the terms “radio frequency identification,” “RFID,” “near-field communication” and “NFC” interchangeably. It acknowledges that RFID credit cards were “in circulation”:

A different type of credit card device in circulation employs radio frequency identification (“RFID”). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

EX1001, 1:56-62.

52. Indeed, NFC credit cards were well-known in the industry. I personally was teaching about RFID credit cards in my Electronic Payment Systems course as early as 2002. A 2009 paper by Kadambi et al., “Near-Field Communication-Based Secure Mobile Payment Service,” was published by the Association of Computing Machinery in the Proceedings of the 11th International Conference on Electronic Commerce in August 2009 (“Kadambi,” EX1025). Kadambi notes that:

Unfortunately, innovating in the Point of Sale (PoS) space is hard because the protocols have been standardized, tightly constraining new ideas. Using mobile phones as payment devices opens up some opportunities, but any solution must minimize changes in the back-end processing. This paper describes a Near Field Communication (NFC) based mobile phone payment solution in a service-oriented environment, which provides the needed data protection without requiring costly changes to the payment processing infrastructure.

EX1025, Abstract.

53. I note that Kadambi discloses a mobile phone used as an NFC payment device.

C. Touch Sensor Arrays

54. The term “touch sensor array” in the ’520 Patent apparently refers to a touchscreen or keypad:

Embodiments of the present disclosure provide a credit card device having a region for receiving human input, e.g., touch sensors which are able to be formed by contacts that a user can press (e.g., the touch sensor array 245 of FIGS. 2A-2B). FIGS. 4A-4B illustrate a user interacting with a credit card device 401 via a keypad or touch sensor array 445.

EX1001, 9:19-25; FIG 4A.

55. Mobile phones have had touchscreens for display since at least 1992, with the introduction of the IBM Simon. EX1031, 2-3. More recently, the Apple iPhone 1 in 2007 had a touchscreen. *Id.*

56. The March 2010 issue of Information Display contained an article by Walker et al. entitled “LCD In-Cell Touch,” that explains the history and operation of touchscreens, including “[t]he concept of putting a light-sensing element into each pixel,” ascribed to TMD Technology in 2003. EX1041, 9. It describes “in-cell,” “on-cell” and “out-cell” touch sensor arrays, all of which were used in touchscreens. EX1041, 8. It discloses, e.g.:

Charge Sensing (On-Cell): This technology, also called “capacitive sensing,” is basically the same as today’s

projected capacitive. It uses an X-Y array of capacitive-sensing electrodes on the top surface of the color-filter substrate. The screen can be touched only with a finger. A cover-glass can be used to protect the LCD's surface.

Id., 9.

Out-Cell Touch

Out-cell is basically just the integration of a touch solution at the LCD-module manufacturer. This is not fundamentally different than the touch integration that is often performed by third-party integrators today. . . . Table 1 categorizes all current touch technologies in terms of the difficulty of integrating them as out-cell touch.

As shown in Table 1, resistive and projected-capacitive touch screens are the most likely candidates for out-cell integration. These two most commonly used technologies accounted for over 95% of the total number of touch screens shipped in 2009.

Id.

57. A POSITA would thus have understood that touchscreens have touch-sensor arrays.

58. Cards also had touch sensor arrays prior to the Critical Date. On November 9, 2012, the Sydney Morning Herald, an Australian newspaper, published an article entitled, "New credit card has LCD screen, touch-sensitive buttons" (EX1029). It states:

MasterCard is billing a new credit card it is issuing in Singapore as the "next generation of payment cards."

With security in mind, the Display Card has an LCD screen and touch-sensitive buttons that let the user employ a one-time password (OTP). Such OTPs are often

delivered via text messages or chip-based authentication devices.

The card is designed for “banking institutions that necessitate a higher level of security for their online banking services require the use of a separate authentication token or device,” according to a press release from MasterCard.

EX1029, 1-2.

59. The photo below is from the same article:



Id., 1.

D. Static and Limited-Use Numbers

60. The use of a surrogate or “token” in place of an actual credit card number was a well-known security practice long before the Critical Date. It was long known that fraud can occur if an unauthorized party obtains a user’s credit card number. Unfortunately, in older credit card transactions, there was no way to prevent the merchant itself from obtaining the user’s credit card number, as the merchant had to present that number to a credit card network in order to be paid.

61. In 2001, the idea of token was introduced by the company TrustCommerce, which replaced the primary account number (PAN) with a randomized number, called a token. When a merchant needed to process a payment, it could use the token and TrustCommerce would process the payment on their behalf, replacing it with the true credit card number before introducing the transaction into the credit card network. In this manner, the merchant never learns the user's credit card number.

62. Shift4 Corporation released a system to the public during an industry Security Summit in Las Vegas, Nevada in 2005. Shift4 stated that "The concept of using a non-decryptable piece of data to represent, by reference, sensitive or secret data. In payment card industry (PCI) context, tokens are used to reference cardholder data that is managed in a tokenization system, application or off-site secure facility."

63. Tokenization was adopted by PCI, which established a Tokenization Taskforce. In August 2011, it published "PCI DSS Tokenization Guidelines" (EX1030) to supplement Version 2.0 of the PCI Data Security Standard. It explains different ways of generating tokens, stating:

One of the primary goals of a tokenization solution should be to replace sensitive PAN values with non-sensitive token values. For a token to be considered non-sensitive, and thus not require any security or protection, the token must have no value to an attacker. Tokens come in many sizes and formats. Examples of some common token formats are included in the following table.

Table 1: Selected Examples of Token Formats*

PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cwl5x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

** Note: This table provides a selection of examples only, and does not include all possible token formats.*

EX1030, 5.

64. The Tokenization Guidelines go on to explain the difference between single-use and multi-use tokens:

Tokens can be generally identified as either single-use or multi-use. A single-use token is typically used to represent a specific, single transaction. A multi-use token represents a specific PAN, and may be used to track an individual PAN across multiple transactions. A multi-use token always maps a particular PAN value to the same token value within the tokenization system. Determining whether single-use or multi-use tokens, or a combination of both, are appropriate for a particular merchant environment will depend on the merchant's specific business need for retaining tokens.

Id.

65. I note that the last row of the table above shows generating a token by taking a portion of the credit card number (PAN) to yield a truncated PAN and replacing the middle digits with “alphabetic and numeric characters.” This bears on

the method claimed in limitation [10h] of the Patent, with the truncated PAN being a “static device account number” and the “alphabetic and numeric characters” being a “dynamically generated one-time limited-use number.”

E. Sequence Counters

66. The '520 Patent claims a “sequence count” (limitation [10g]) and “sequence counters” (claim 12). None of these are described, or even mentioned, in the Specification and all were added through amendment during prosecution.

67. There is disclosure of a “transaction count,” however:

As detailed above, if an expired limited-duration credit card is attempted to be used for a transaction, the transaction is denied and an automatic notification is able to be made to a credit authority in order to notify the user and to prevent transactions on the account. The transaction count is able to be determined through the action of passing the card through magnetic reader, and the process of transmitting said card number to said card reader.

EX1001, 10:23-31.

68. It appears from the Specification that the “transaction count” is to be used to determine whether the card has been used a given number of times, after which it can no longer be used. The term “transaction count” is not used in any of the claims.

69. I believe a POSITA would understand “sequence count,” “sequence counter,” “sequence counters” and “sequence code” to be synonymous because the Patent appears to use them that way (and provides no other explanation). I take the

terms to refer to some kind of sequential counter, which could include a transaction count or a transaction number.

F. Payment Method Types

70. Claim 14 recites, “rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name.” There is no antecedent basis for “the payment method types,” so I believe a POSITA would understand “the payment method types” to mean just “payment method types,” e.g., credit card types.

71. Displaying payment method types with images, alphanumeric characters and iconography including bank logos or issuer logos was common with digital wallets before the Critical Date. For example, Google Wallet was introduced on Android phones in 2011. An article by Z. Honig dated September 19, 2011 published by Engadget entitled, “A week with Google Wallet” (EX1023) discloses:

Google Wallet works in much the same way, using a built-in Near Field Communication (NFC) chip to communicate wirelessly with a payment terminal. To make a payment, you'll first need to activate a card (only one card can be active at one time). One card is always active by default, but you can easily switch between payment options with a single flick and tap.

72. The image below from that article shows a Google Wallet screen with alphanumeric characters and iconography including an issuer logo:



G. Contactless ATMs

73. Challenged Claims 18-24 are drawn to ATM transactions conducted wirelessly, that is, in which digital information is communicated between the payment card and the ATM instead uses RFID, NFC, or similar methods. EX1001, 14:15.

74. First, it would have been obvious to use a contactless payment card and contactless reader in any application for which magnetic stripe or chip cards had been used, for the simple reason that contactless cards were designed to be

replacements for traditional payment cards.

75. Second, contactless ATMs were known long before the Critical Date.

76. For example, in 1988, 25 years prior to the Critical Date, the National Institute of Standards and Technology issued NIST Special Publication 500-157, entitled “Smart Card Technology: New Methods for Access Control” (EX1019). It discusses uses of magnetic stripe cards and explains the advantages of using smart cards, both contact and contactless, in their place, including in ATMs:

Applied in banking, telephone services, medical records systems, and other areas, smart cards can provide users with both a secure medium for storing and carrying personal information and a means for accessing resources in a network of computers.

EX1019, 1.

On a superficial level, a smart card system resembles conventional data storage card systems, such as automated teller machine (ATM) systems which use magnetic stripe cards. However, because smart cards have computing powers and greater capacity for protected data storage, smart card systems can provide increased flexibility and security in many applications.

Id., 3.

77. Fig. 5 of EX1019 illustrates the difference between contact type and contactless smart cards:

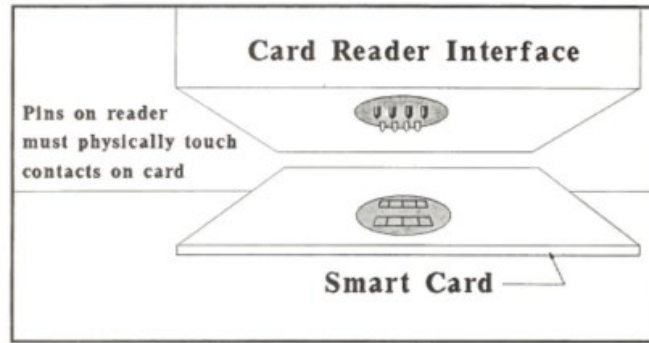


Figure 4. Contact-Type Smart Card Interface

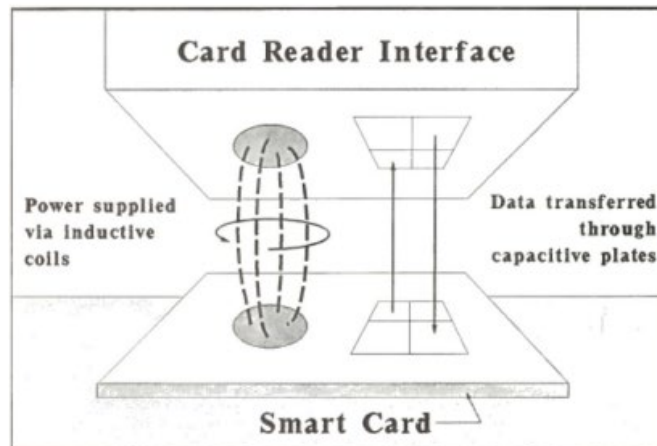


Figure 5. Non-Contact-Type Smart Card Interface

78. On September 9, 1994, Moskowitz et al., assignors to IBM, filed an application that issued as U.S. Patent 5,538,222 on June 18, 1996, entitled “Radio Frequency Circuit and Memory in Thin Flexible Package” (EX1018). It discloses a Radio Frequency Identification (RFID) contactless card that could be used as an ATM or credit card:

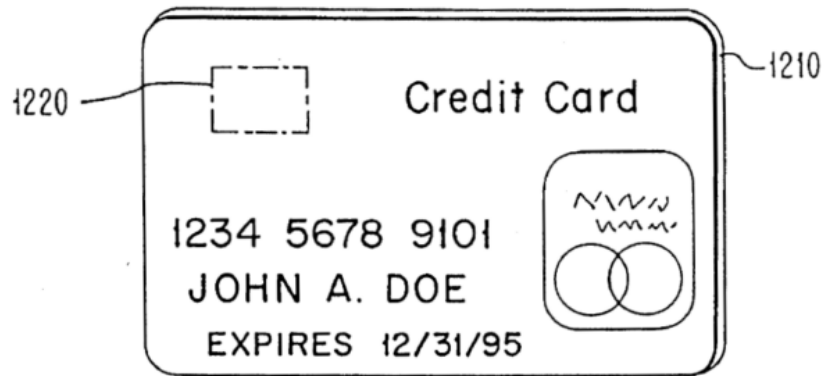


FIG. 12 shows ISO standard credit card 1210 containing an RF tag 1220. The credit card may serve as an ATM card, frequent flyer card, library card, phone card, employee ID, medical ID card, gasoline credit card or any credit or debit card.

EX1018, FIG. 12; 7:20-24.

79. Not surprisingly, the financial community began to devise uses for contactless cards. In 1995, the Federal Reserve Bank for New York began publishing “Current Issues in Economics and Finance.” The very first article in the first issue was entitled “The Electronic Purse,” by Wenninger et al. (EX1038). It describes the choice between contact and contactless cards as a design choice:

System designers must choose, for example, between two distinct types of smart card representing incompatible technologies: contact cards, which touch a card reader when registering a transaction, and contactless cards, which need only come in proximity to a card reader.

EX1038, 2.

80. It also describes an “electronic purse” for use at an ATM:

An electronic purse system might work as follows. A bank

issues stored value cards to its customers, who then transfer value from their accounts to the cards at an ATM, a personal computer, or a specially equipped telephone. The electronic purse card might also function as an ATM card or a credit card. When making purchases, customers pass their cards through a vendor's point of sale terminal.

EX1038, 1.

81. The foregoing passage reinforces the idea that credit cards and ATM cards can be used interchangeably.

82. On April 24, 1995, Kenneth et al. filed an application that issued as U.S. Patent 5,594,233 on January 14, 1997, entitled "Multiple Standard Smart Card Reader" (EX1017). It discloses a card reader that could read all three of magnetic stripe cards, contact smart cards and contactless smart cards, specifically to be used at an ATM:

This invention relates to card readers and to card reader writers and a method of operation thereof. The invention has application, for example, to a card reader for use in a transaction terminal such as an automated teller machine (ATM).

EX1017, 1:4-8.

These cards can be used, in association with an appropriate read/writer, in a vast array of different environments. For example, user identification cards are used in association with a personal identification number (PIN) to provide access to an ATM. Also financial service cards such as credit or debit cards are used to contain information on a user's bank or building society accounts so that transactions can be attributed to those accounts merely by reading the card.

Id., 1:18-25.

83. In 2000, the Australian Human Rights and Equal Opportunity Commission sponsored a report by Noonan entitled “Barriers to Using Automatic Teller Machines: A Review of the Useability of Self-Service Banking Facilities for Australians with Disabilities” (EX1039). It noted at p. 23 that, for ATM transactions, “blind and partially sighted users would like to use a contactless card.”

84. Lest there be any doubt that contactless ATMs were well-known prior to the Critical Date, on April 1, 2003, Douglass, assignor to Diebold, a well-known manufacturer of ATMs, filed a provisional application which, through a subsequent regular application, became U.S. Patent 7,004,385 on February 28, 2006, entitled “Currency Dispensing ATM with RFID Card Reader” (EX1040).

The foregoing objects are accomplished in an exemplary embodiment of the present invention by providing an automated banking machine with a contactless card reader. An RFID card and RFID card reader arrangement can be used instead of or as an adjunct to a conventional card and contact type card reader arrangement. A contactless card reader may be installed in new automated banking machines or in existing machines without further Substantial modifications to the machines. Security risks may be reduced. As service issues could be reduced without the wear due to card reader head/card contact, use of a contactless card reader enables enhanced machine reliability at a modest cost.

EX1040, 2:31-42.

85. Concluding this section, all of the technology claimed in the Challenged

Claims predates the Critical Date and would have been within the knowledge of a POSITA.

IX. CLAIM CONSTRUCTION

86. I understand that claim terms, in the absence of an express definition or disclaimer, are given their ordinary and customary meaning, as would have been understood by a POSITA at the time of the alleged invention.

87. In considering the meaning of the claims, however, I understand that one must consider the language of the claims in light of “the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.” 37 C.F.R. § 42.100(b).

88. I have applied these principles in interpreting the Challenged Claims for purposes of my analysis in this Declaration.

89. I understand that Petitioner does not assert that any claim terms require express construction in this proceeding.

X. OVERVIEW OF PRIOR ART REFERENCES

A. U.S. Patent Application Publication 2015/0134540 (“Law”)

90. Law et al. U.S. Patent Application Publication 2015/0134540 (EX1032) is entitled “Systems and Methods for Facilitating a Transaction Using a Virtual Card on a Mobile Device,” and lists Simon Law as first inventor.

91. Law was filed on October 17, 2014 and published on May 14, 2015, but claims priority to U.S. Provisional Application 61/673,096 (“Law Provisional”), filed July 18, 2012. I understand that it is prior art to the ’538 Patent under pre-AIA 35 U.S.C. §§ 102(a), 102(b) and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2), provided that (1) at least one claim of Law is supported by the Law Provisional, and (2) the subject matter relied upon in Law is also disclosed in the Law Provisional.

92. The table below demonstrates that both conditions (1) and (2) are satisfied.

Law Claim 4	Exemplary Disclosures in the Law Provisional (EX1033)
4. A computer-implemented method comprising:	Whether or not the preamble is limiting, it is disclosed by the Law Provisional. <i>See, e.g.</i> , EX1033, [0033], [0034], [0063].
registering a funding card comprising storing a funding card number;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0050]-[0053], [0110], FIG. 10.
receiving a message from a mobile device indicating a desire to make a payment using the registered funding card;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0054], [0066]-[0072], [0079].
computing data for a virtual card, wherein the data for the virtual card comprises a virtual card number that is different than the funding card number;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0072]-[0073], [0076]-[0079], [0100], [0113]-[0114].
storing the data for the virtual card in association with the funding card number;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0051]-[0052], [0109]-[0114].
sending information related to the data for the virtual card to the mobile device;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0051]-[0052], [0062], [0070]-[0073], [0111]-[0113].
receiving a first payment authorization request from a merchant or a merchant acquirer, the first payment authorization request comprising the data for the virtual card and a requested payment amount;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0054], [0084]-[0088].
retrieving the funding card number based on the data for the virtual card;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0054], [0086]-[0091].

Law Claim 4	Exemplary Disclosures in the Law Provisional (EX1033)
sending a second payment authorization request to a funding card issuer, the second payment authorization request comprising the funding card number and the requested payment amount;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0054], [0087]-[0093].
receiving a payment authorization response from the funding card issuer; and	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0055], [0087]-[0093].
sending the payment authorization response to the merchant or the merchant acquirer.	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, [0048], [0087]-[0093].

93. Law discloses “facilitating a payment transaction at a merchant location using a virtual card on a mobile device.” EX1032, [0002]; EX1033, [0001]. Law explains that an “NFC-enabled mobile device can be equipped with a ‘software payment card’ (e.g. a software implementation of a contactless payment card) application running inside the mobile device. The software payment card uses the compatible contactless communication capabilities of the device to interact with contactless-enabled POS terminal to facilitate payment transactions.” EX1032, [0062]; EX1033, [0034].

94. Law explains that when “a contactless funding card credential is used to facilitate a payment transaction, the transaction most often includes dynamic data from the card to securely authenticate the payment credential. The dynamic data changes values every time the credential is used. If the dynamic data received on the

funding card issuing server matches the expected value computed by the server for the card, the authentication of the payment credentials is deemed successful and the payment authorisation can continue.” EX1032, [0069]; EX1033, [0041].

95. Law further teaches that a static number may be acquired by the mobile device and used in place of a user’s actual credit card number. See EX1032, [0082] (“In an example embodiment of the registration, for each funding card the user wishes to register, the user enters in (e.g. types in) card details into the mobile device (e.g. card details include the name printed on the funding card, the PAN¹ printed on the funding card, the expiry date printed on the funding card, and the static security code printed on the funding card). The mobile device sends this data, plus a user provided PIN and the mobile device ID to the payment gateway server. For each funding card, the payment gateway server computes a funding card identifier which identifies the given funding card. . . . In an example embodiment, the funding card identifier is a value that is different from the PAN, expiry date or static security code of the funding card.”); EX1033, [0052].

96. The Law system also discloses the use of transaction counters, key

¹ Law describes the PAN as a primary account number (i.e., the user’s actual credit card number). EX1032, [0043]; EX1033, [0023]. “PAN” is a standard abbreviation in the trade for “primary account number.”

values and cryptographic hashing, among other values, in producing dynamic data for a payment transaction. EX1032, [0142]-[0155]; EX1033, [00109]-[00122].

97. Law is applied below in Grounds 1A-1B. The analysis for each claim limitation in Grounds 1A-1B includes supporting citations to the Law Provisional.

B. U.S. Patent 9,600,808 (“Gomez”)

98. Gomez Sr. et al. U.S. Patent 9,600,808 (EX1007) is entitled “Secure Payment Card, Method and System,” and lists William Gomez. Sr. as the first named inventor.

99. Gomez was filed June 22, 2012 and published on March 21, 2017. I understand that it is prior art to the ’579 Patent under pre-AIA 35 U.S.C. § 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

100. Gomez discloses a payment card system that purports to address “[t]he problems of fraud and identity theft that result from the use of payment cards, such as credit and debit cards” when cardholders conduct a payment transaction that “leave[s] behind all the information necessary for another person to be able to make an unauthorized transaction.” EX1007, 1:32-48.

101. Gomez proposes a payment card “utiliz[ing] a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card, and which expires within a short period of time thereafter.” *Id.*, 1:58-63. Because the authentication cryptogram is time-limited, “the information that can be gleaned from

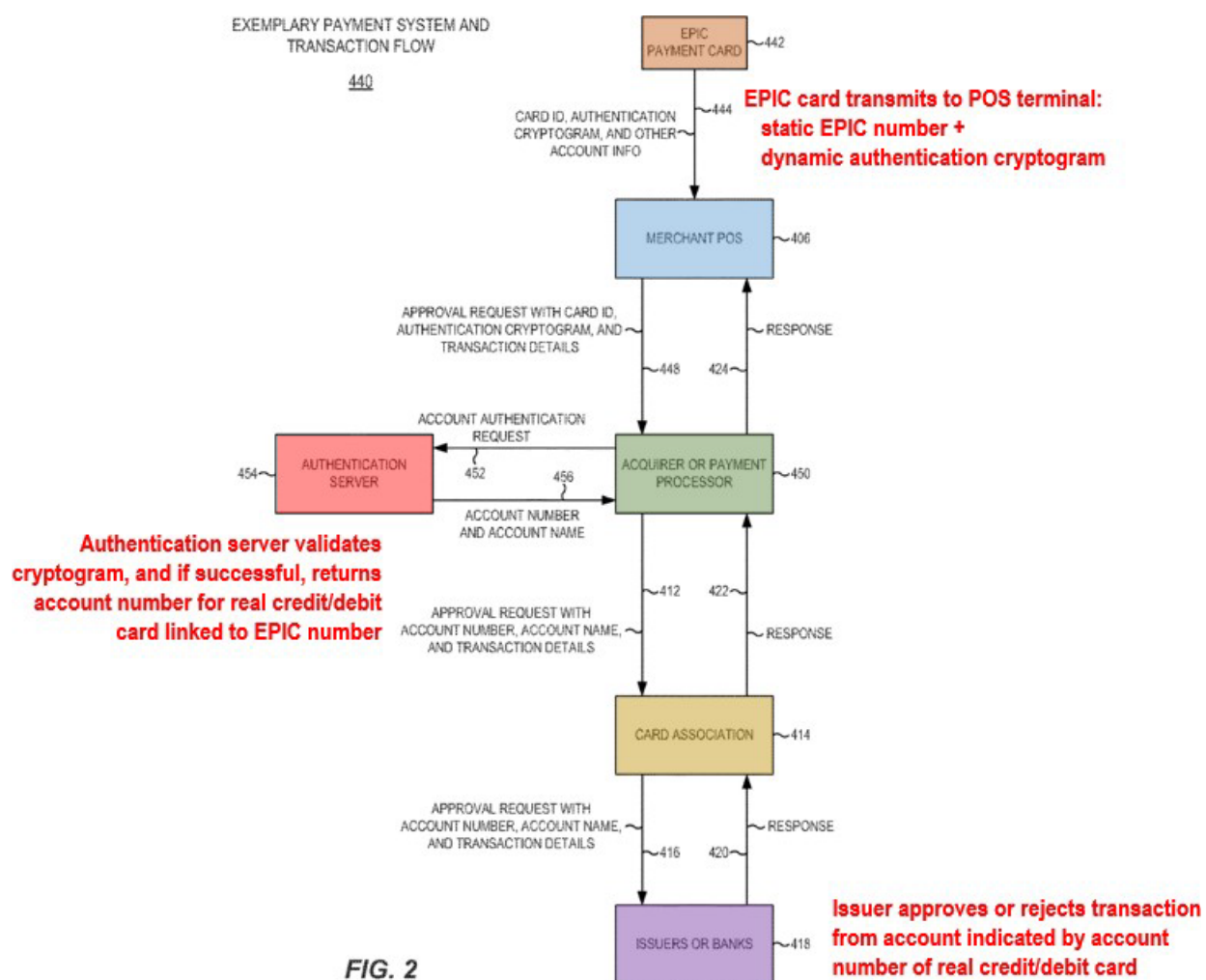
a payment card ... is rendered useless for making an unauthorized subsequent transaction.” *Id.*, 5:7-11, FIG. 7.

102. Customers of the system described in Gomez are issued an electronic payment card, referred to as an “EPIC” card. *Id.*, 2:19-39. The EPIC card has a static payment card identifying number corresponding to the customer’s EPIC account. *Id.* The customer can link one or more actual credit/debit cards to his or her EPIC account by entering the account numbers and other pertinent information of these credit/debit cards into an online EPIC portal, which the EPIC system then stores and links to the customer’s static EPIC payment card identifying number. *Id.*, 20:1-29. The customer can then use the EPIC card to make payment transactions with any of the linked card accounts. In this manner, “there is no need to carry the actual credit cards, they may be stored safely at home or in a safe deposit box.” *Id.*, 2:35-37.

103. When a customer initiates a transaction with an EPIC card, the card dynamically generates an “authentication cryptogram” based on a unique “seed value” stored securely in the card and a “temporal signal” that changes with each attempted use or transaction. *Id.*, 7:17-48. The payment card transmits the static EPIC number and the dynamically-generated authentication cryptogram to the point-of-sale (POS) terminal, which is then conveyed to an authentication server (e.g., EPIC) before the transaction request is sent to an issuer or bank for approval. *Id.*, 7:49-8:2. The authentication server authenticates the transaction using the

cryptogram, and if successful, the authentication server returns the actual account number for one of the customer's linked credit/debit cards to the acquirer or payment processor, which information is then forward to the appropriate card association and issuer or bank for approval. *Id.*, 18:4-42, FIGS. 17-18.

104. Below is Fig. 2 from Gomez, annotated in color, illustrating a payment transaction approval process:



105. Gomez also discloses cryptographic hash functions:

At step 294 the message is processed, such as by using a

cryptographic hash function, to generate a message “digest.” A cryptographic hash function is typically viewed as a deterministic procedure that takes an arbitrary block of data, known as a “message,” and returns a fixed-size string, known as a hash value or “message digest.” Such that any change to the message will change the message digest. Such functions are well known in the art, and include MD5, SHA-1, and SHA-2. For example, MD5 returns a 128-bit message digest, while SHA-1 returns a 160-bit digest.

Id., 8:42-51.

106. Gomez also discloses a sequence code:

At step 256 a temporal signal value is generated which corresponds to the instance of attempted use. In some embodiments such a temporal signal value may reflect the date/time of the attempted use. The date and time may be determined by a real-time clock device included within the payment card, or may be communicated by the merchant POS terminal to the payment card, or by some other technique. **In some embodiments such a temporal signal value may reflect the sequence value (or sequential number) of the attempted use.**

Id., 7:17-26 (emphasis added).

C. U.S. Patent Application Publication 2012/0123937 (“Spodak”)

107. Spodak U.S. Patent Application Publication 2008/0319905 (EX1009) is entitled “Portable e-wallet and universal card,” and lists Douglas Spodak as sole inventor.

108. Spodak was filed January 26, 2012 and published on May 17, 2012. I understand that it is prior art to the ’579 Patent under pre-AIA 35 U.S.C. §§ 102(a)

and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

109. Spodak discloses a “universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.” EX1009, [0002]. The universal card is similar to a mobile device such as a phone except that the universal card is shaped like a credit card.

Also depicted in FIG. 1 is a universal card 110. The universal card 110 may include components such as a display 112, a power source 113, a processor 114, and memory 115. Each of those components are similar in function to the corresponding components of the mobile device 100, except that the component of the universal card 110 may be physically configured differently so as to fit in the shape of the universal card 110. For example, the display 112 of the universal card 110 may be integrated into universal card 110 via hot lamination processes and standard inlay constructs so that the universal card 110 will be the approximate shape and size of a traditional credit card and generally compliant with ISO 7810 standards.

Id., [0027], [0034].

110. The universal card includes both a dynamic magnetic stripe and a short range transceiver. *Id.*, [0033], [0035]. The universal card can use the dynamic magnetic stripe to communicate with a traditional credit card magnetic stripe reader, and the short range transceiver to communicate with a contactless payment terminal such as via NFC:

The instructions sent from the mobile device 1591 to the

universal card 1593 can include instructions for the universal card to emulate either or both of a magnetic stripe of the traditional card and a contactless payment form of the traditional card.

Id., [0088].

In one embodiment, the universal card 110 configures both the dynamic magnetic stripe 111 to emulate the magnetic stripe of the selected traditional credit card and the short range transceiver 116 to emulate the selected traditional credit with a contactless payment terminal. In this manner, the user needs only to select the desired traditional card using the e-wallet software 105, without having to make a selection of magnetic stripe or contactless payment, and the user can use the traditional card with either a magnetic swipe terminal or a contactless payment terminal.

Id., [0089]. The universal card can include a display. *Id.*, [0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A.

111. To emulate the magnetic stripe and authenticate the transaction, the universal card generates a dynamic authentication value in the field typically used for a CVV value:

In another embodiment, the traditional card may have a field on the static magnetic stripe for a CVV value. When the universal card is configured to emulate the traditional card that normally has a static CVV value field, the universal card may generate a dynamic authentication value and write the dynamic authentication value in the field typically used for the static CVV value. The dynamic authentication value could have the same format as the static CVV and be located in the same location that the static CVV field would be located in the static magnetic stripe of the traditional card. In this scenario, there would be no need to reconfigure the terminal with the magnetic

stripe reader because it would already be configured to read a value from the static CVV field location. Using dynamic authentication values with traditional magnetic stripe reader terminals allows for the added security of the dynamic authentication value authentication without requiring terminals to add a contactless payment terminal to the magnetic stripe reader.

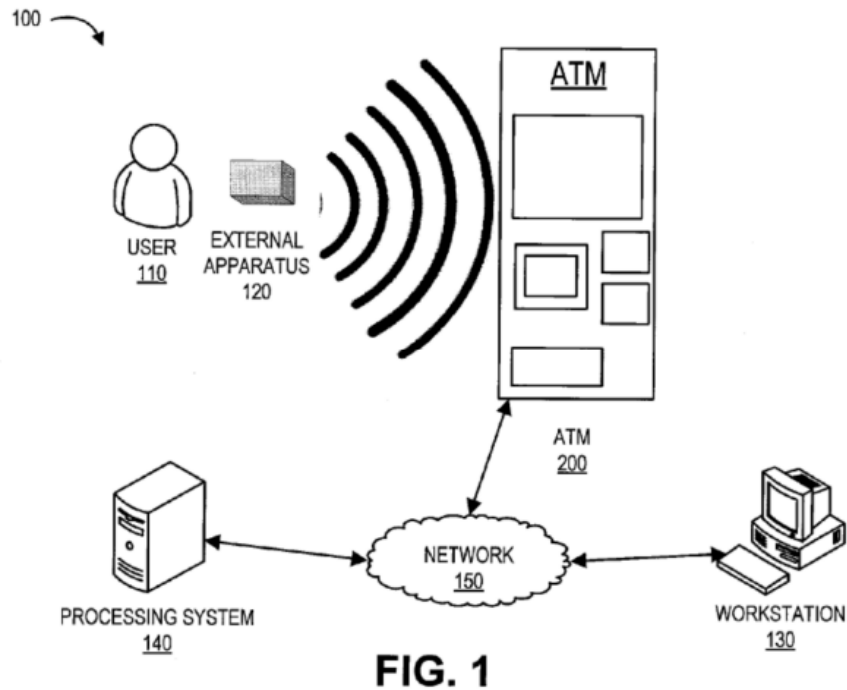
Id., [0094].

D. U.S. Patent 9,098,846 (“Gill”)

112. Gill et al. U.S. Patent 9,098,846 (EX1034) is entitled “Contactless Automated Teller Machine,” and lists Sara Gill as first named inventor. Gill was filed May 6, 2011 and published on September 6, 2012. I understand that it is prior art to the ’520 Patent under pre-AIA 35 U.S.C. §§ 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

113. Gill describes systems and methods for performing contactless transactions at an ATM. EX1009. “An ATM machine is provided that has been equipped with a contactless interface for interacting with an external apparatus such as a debit/credit card, mobile device, and/or contactless transmission equipped stickers.” EX1034, Abstract.

114. Figure 1 of Gill illustrates the use of an “external apparatus 120,” which is wireless, at an ATM:



EX1034, FIG. 1.

115. External apparatus 120 is “operated by a user 110 who may be a customer who wants to make an ATM 200 transaction.” EX1034, 5:25- 27. “Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received (i.e. account information, for example, account number, name, expiration date, debit/credit, etc.) and require further security authorization in order to access the desired financial account at the ATM.” *Id.*, 5:13-18.

116. Figure 7 depicts example interactions between an external apparatus 120 and an ATM in performing a contactless transaction (e.g., via NFC), as taught in Gill:

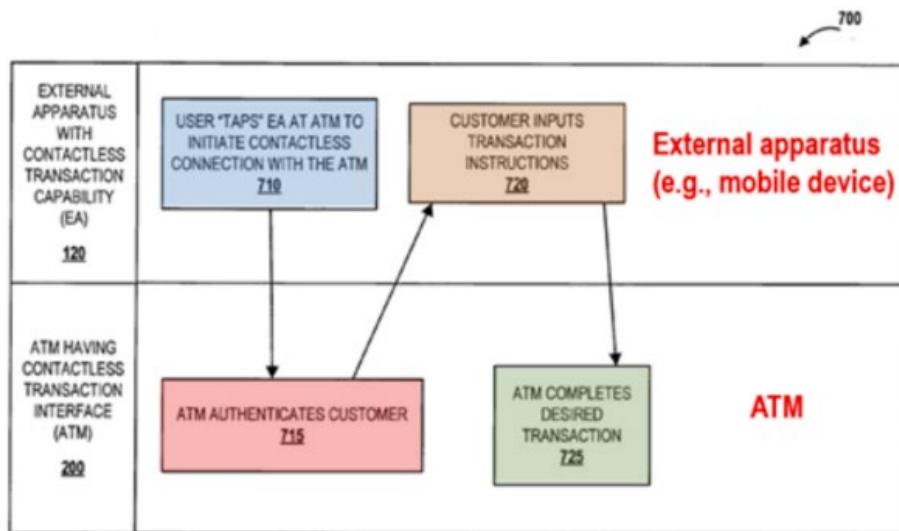


FIG. 7

Id., FIG. 7 (annotated).

117. As shown in FIG. 7, a user (customer) “taps the external apparatus 120 at the ATM 200 to initiate a contactless connection with the ATM,” e.g., “by positioning the external apparatus 120 within close proximity of the contactless interface of the ATM 200.” *Id.*, 14:1-8. At block 715, the ATM 200 “authenticates the customer” by requiring the user to present a valid credential such as a PIN. *Id.*, 14:9-13. In some embodiments, rather than directly entering credentials at the ATM after establishing a connection, “the customer may first authenticate himself prior to the contactless connection being established” by “input[ing] authentication information and such transfer such data [sic] to the ATM 200 upon establishing the contactless connection.” *Id.*, 14:13-20. The customer can further input instructions for the transaction at the external apparatus 120 (block 720), and the apparatus 120

in turn transmits the instructions to the ATM over the contactless connection (e.g., NFC). *Id.*, 14:31-38, 17:56-62.

E. U.S. Patent Application Publication 2013/0232083 (“Smith”)

118. Smith et al. U.S. Patent Application Publication 2013/0232083 (EX1035) is entitled “Systems and Methods for Mapping a Mobile Cloud Account to a Payment Account,” and lists Theresa L. Smith as first named inventor. Smith was filed March 1, 2013 and published on September 5, 2013. I understand that it is prior art to the ’520 Patent under pre-AIA 35 U.S.C. §§ 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

119. Like Gill, Smith describes techniques for conducting contactless payment transactions with a mobile device. EX1035, [0002]. Smith discloses a mobile device that maintains “mobile cloud accounts” in a virtual wallet, where any of the mobile cloud accounts can be used to conduct a contactless transaction. EX1035, [0032]-[0037]. Smith discloses the use of a token (MCA) to substitute for a credit card number (RCA): “A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA).” *Id.*, [0034]. “The RCA may correspond to a payment account issued to the user by an issuer 112,” and “[t]he MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding

to the RCA.” *Id.* “As a result, the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.” *Id.* This tokenization process is illustrated in Figure 6:

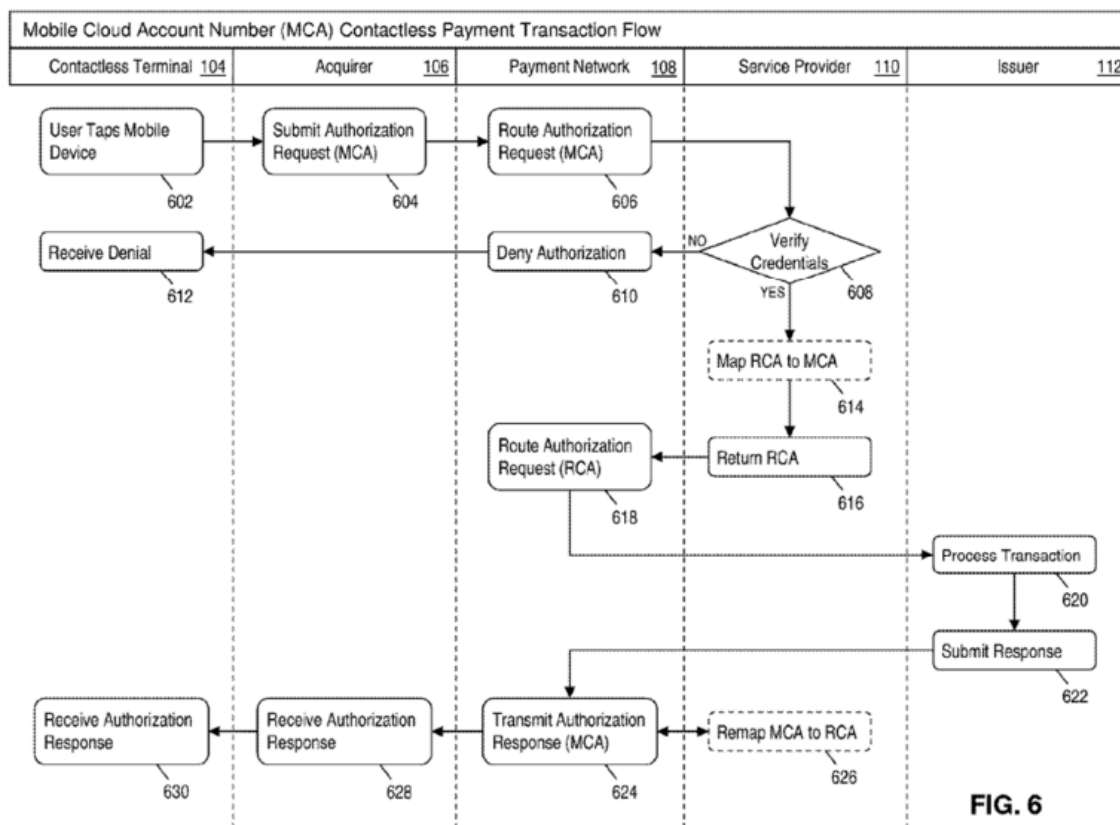


FIG. 6

EX1035, FIG. 6.

120. As shown in Figure 6, Smith discloses that a user initiates a contactless transaction by tapping his/her mobile device at a terminal. *Id.*, [0066]-[0067]. The mobile device then transmits to the terminal “payment credentials” for the transaction, where the “payment credentials” include the “MCA” for the account desired for the transaction and a “payment cryptogram” such as “an authorization request cryptogram or dynamic card validation code.” *Id.*, [0067]-[0068]. The

payment credentials are received by an acquirer, which in turn forwards the credentials to a service provider that “verif[ies] (e.g., validate[s]) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art.” *Id.*, [0070]. Authorization for the transaction may be denied if the verification fails. *Id.* However, “[i]f the credentials are successfully verified, then[] ... the service provider 110 may identify the RCA corresponding to the MCA” and returns the corresponding RCA to the payment network for further processing. *Id.*, [0071]. “[T]he payment network 108 may route the authorization request with the RCA in place of the MCA to the issuer 112,” and “the issuer 112 may approve and process the financial transaction.” *Id.*, [0072].

F. U.S. Patent Application Publication 2013/0124410 (“Kay”)

121. Kay et al. U.S. Patent Application Publication 2013/0124410 (EX1036) is entitled “System and Method for Conducting a Transaction at a Financial Transaction Terminal Using a Mobile Device,” and lists Christopher Erin Kay as first named inventor.

122. Kay was filed November 15, 2011 and published on May 16, 2013. I understand that it is prior art to the ’520 Patent under pre-AIA 35 U.S.C. § 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

123. Kay discloses techniques to “allow greater access to a banking platform

via a mobile device.” EX1036, Abstract. For example, “the customer can initiate a financial transaction using a mobile device,” and the mobile device provides a user interface with which the user can interact to facilitate the transaction. *Id.*; *see also id.*, [0038]-[0043], FIGs. 4A-4D.

124. Kay further discloses displaying a time, a passcode (PIN) and a currency amount on a mobile phone payment interface. *See, e.g.*, EX1036, FIGs. 4A- 4D.

XI. THE CHALLENGED CLAIMS ARE INVALID

A. Ground 1A: Claims 10-13 of the '520 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Law in view of Gomez

125. In my opinion, the combination of Law and Gomez renders obvious claims 10-13 of the '520 Patent for at least the reasons discussed below.

1. Motivation to Combine Law and Gomez

126. A POSITA would have beneficially applied the teachings of Gomez to Law to modify Law's mobile payment system to include multiple improvements, as explained below, that complement Law's focus on secure cryptogram generation for payment transactions. The teachings of Law and Gomez would have rendered obvious and provided each element of claims 10-13 for the reasons discussed below.

127. It would have been obvious and beneficial to augment the payment information communicated by the device in a contactless transaction as taught in

Law with a tokenized static payment card identifying number like that taught in Gomez (such that the presented payment information would include both a static number and limited-use authentication cryptogram dynamically generated for each transaction). EX1007, 1:58-63, 6:23-38, 7:17-65, 8:3-41, FIGS. 2-5, 17-18. Law discloses wirelessly receiving a funding card identifier (i.e., a tokenized static account number which identifies a user's actual credit card account). EX1032, [0082]; EX1033, [0052]. Law's funding card identifier is held on the payment application on a user's mobile device in place of the user's actual credit card number for security purposes. *Id.* During the payment transaction process, Law uses the funding card identifier to create limited-use payment information such as a cryptographically hashed one-time use number. EX1032, [0147], [0149]-[0154]; EX1033, [0114]. Law does not expressly disclose that the funding card identifier is sent as part of the complete payment information when performing a payment transaction. Gomez describes a "static payment card identifying number"—also referred to as an "EPIC" number—stored on the electronic device. EX1007, 2:25-39; *see also id.*, 1:63-64, 13:45-14:2, 22:49-51, 6:10-12, 18:57-59. The EPIC number "identifies the payment card, but does not represent a live account." *Id.*, 5:13-18. Gomez uses this static payment card identifying number in combination with an authentication cryptogram when performing a payment transaction. *Id.*, 7:9-8:51. Multiple reasons would have led a POSITA to apply Gomez's suggested use

of a static payment card identifying number in combination with an authentication cryptogram with Law before the Critical Date of the '520 patent.

128. The addition of the tokenized static number with an authentication cryptogram would have improved transaction security by preventing fraudulent use of a substituted or incorrect account number. By requiring both a tokenized static number and authentication cryptogram as part of the complete payment information, an additional layer of security would be realized to prevent unauthorized actors from exploiting any compromised portion of the payment information. Additionally, a payment processing authority would more easily identify the user's actual account number for processing a transaction with the presence of the user's tokenized static account number in the payment information because that tokenized static account number is linked to the user's actual account. EX1032, [0082]; EX1033, [0052]; EX1007, 5:13-18.

129. Further, a POSITA would have seen the addition of Gomez-like payment information (i.e., a static number and cryptogram used together) as a useful technique to improve security in a manner that would still be compatible with existing merchant payment infrastructure, particularly since that payment information would be capable of transmission in ordinary account name fields, security code fields, or both. EX1007, 2:4-13. 2:40-44, 7:52-57; EX1032, [0075] ("additional infrastructure . . . is not required"); EX1033, [0046]. Further, the fact

that Gomez is directed to a smart payment card while Law is directed to a mobile device does not teach away from the proposed combination. Indeed, Gomez's payment card is not a traditional credit card but instead contains a processor that functions to compute dynamic payment information based on seed values and/or temporal signals, like Law. EX1007, 1:58-2:1, 2:14-17, 2:21-25, 5:43-47, 7:17-27, 8:42-9:11, 13:63-14:2. Therefore, a POSITA would have implemented Gomez's payment information generation technique with a smartphone, as in Law.

130. Additionally, a POSITA would have recognized the benefits of hashing functions in payment transactions. Law discloses an algorithm and hashing functions used in generating the payment information. EX1032, [0146]-[0155]; EX1033, [0113]-[0122]. Law specifically states that SHA256 and HMAC are known cryptographic hash functions that are used in discretionary data generation. *Id.* Gomez discloses use of a cryptographic hash function to generate a message digest, from which the authentication cryptogram is ultimately derived for a payment transaction. EX1007, 8:42-43. The hash function is "a deterministic procedure that takes an arbitrary block of data, known as a 'message,' and returns a fixed-size string, known as a hash value or 'message digest[]'." *Id.*, 8:42- 48; *see also id.*, 9:58-10:3, 21:55-59. The message input to the hash function provides a transaction unit, and the digest produced by the hash function provides a cryptographic hash. Alternatively, the cryptogram as an encoded version of the digest provides a

cryptographic hash. *Id.* A POSITA would have understood, and it would have been obvious, that the discretionary data/message digest would be stored in a memory of the device for at least some time to allow processing to form the cryptogram. EX1032, [0095], [0155]; EX1033, [0065], [0122]; EX1007, 11:7-9; [10.f]. The cryptogram itself would also be processed and stored on the device for at least some time to permit its inclusion in the payment message(s) transmitted from the device to a terminal in a transaction. *Id.* A POSITA would have recognized that the cryptographic hashing functions described in Gomez would be beneficially applied to Law as a useful technique to improve security in payment transactions.

131. Moreover, a POSITA would have recognized that Law and Gomez each disclose communicating payment information via NFC communication, and a POSITA would have recognized that integrating Gomez's payment card functionality into a mobile device such as a smartphone would have reduced the number of devices that a user needs to carry while also improving the user experience due to the improved user interfaces and processing power of smartphone devices of the time. EX1032, [0088]; EX1033, [0058]; EX1007, [14:3-7]. Among other considerations, use of a multi-functional payment device in lieu of a card was known to be desirable to increase the convenience of retail and other payment transactions to users. By the Critical Date of the '520 patent, consumers commonly carried smartphones and similar devices on their person while shopping or otherwise

moving about in public. *Id.* Also, by the Critical Date, predictable benefits stemming from the use of such multi-functional wireless devices in contactless payment transactions were widely recognized. *Id.*

132. Additionally, given that the use of dynamic payment information in electronic transaction systems had been known for many years before the Critical Date of the '520 patent, the combination amounts to a predictable use of a known technique for improving transaction security (i.e., Gomez's payment information) to improve a similar system as taught in Law in a similar way, and would have achieved predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (a supposed invention that "simply arranges old elements with each performing the same function it had been known to perform" is obvious).

133. In the combination described above, the teachings of Law in view of Gomez would have rendered obvious claims 10-13, and the combination would have provided each element of these claims for the reasons described in detail below.

2. Claim 10

[10.pre]: A method of storing and generating payment information in an electronic device, the method comprising:

134. Whether or not the preamble is limiting, Law discloses an electronic device capable of storing and generating payment information. For example, Law discloses "facilitating a payment transaction at a merchant location using a virtual

card on a mobile device.” EX1032, [0002]; EX1033, [0001]. Law explains that “contactless payment is well suited for a mobile device. For example, some mobile devices have a near-field communication (NFC) system that allows data to be transferred wirelessly” with another contactless-enabled device “by touching them together or keeping them into close proximity.” EX1032, [0061]; *see also id.*, [0062] (“An NFC-enabled mobile device can be equipped with a ‘software payment card’ (e.g. a software implementation of a contactless payment card) application running inside the mobile device. The software payment card uses the compatible contactless communication capabilities of the device to interact with contactless-enabled POS terminal to facilitate payment transactions.”); EX1033, [0033]-[0034].

[10.a]: accepting a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information;

135. Law discloses a device in which issuer provided payment information is entered at a touch screen display. For example, Law describes that the “mobile device’s display 616 can be a touch-screen type display.” EX1032, [0092]; EX1033, [0062]. Law further discloses “cardholder 101 registers one or many funding cards and their mobile device with a virtual card issuer 401” and the “cardholder’s mobile device includes a payment application that can interact with the virtual card issuer 401.” EX1032, [0081]; EX1033, [0051]. Law further describes the process of registering a funding card with a virtual card issuer. EX1032, [0082] (“for each

funding card the user wishes to register, the user enters in (e.g. types in) card details into the mobile device (e.g. card details include the name printed on the funding card, the PAN printed on the funding card, the expiry date printed on the funding card, and the static security code printed on the funding card). The mobile device sends this data, plus a user provided PIN and the mobile device ID to the payment gateway server.”), [0142]; EX1033, [0052], [0109]. Figure 10 of Law illustrates these steps:

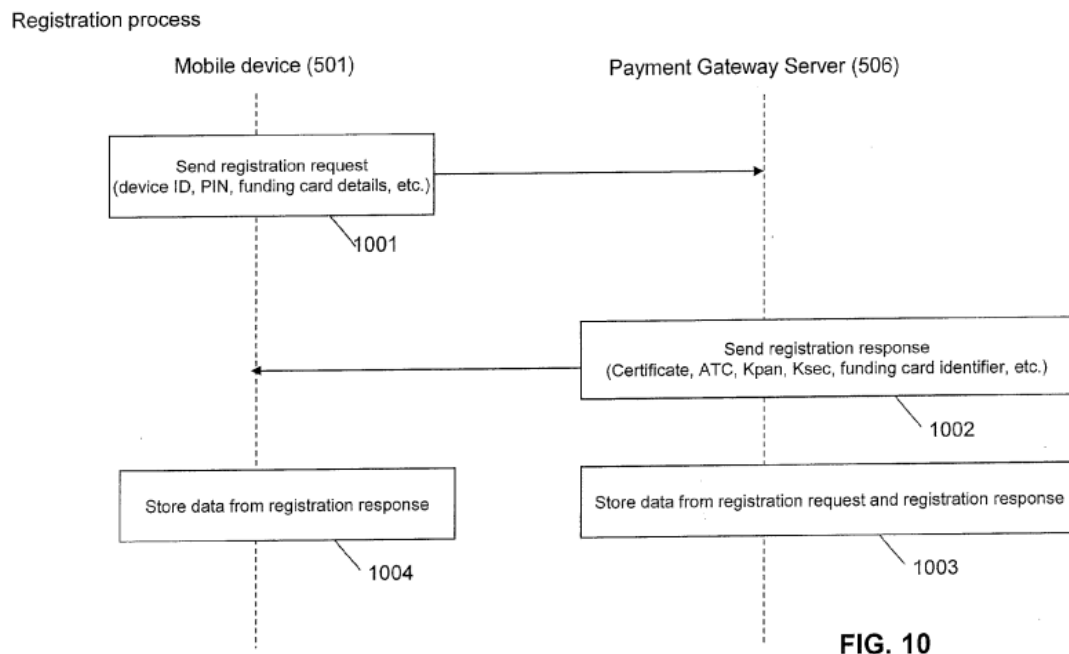


FIG. 10

EX1032, FIG. 10; EX1033, FIG. 10. Law’s disclosure of user input of a PAN would constitute at least [10.a]’s “issued payment information.” Further, Law’s disclosure of user input of an expiry date and/or static security code would constitute at least [10.a]’s “an issuer provided payment information.”

136. Gomez additionally describes inputting issuer provided payment information on a payment device. For example, Gomez teaches that “[a]n EPIC account may be established online to link one or more actual payment card accounts with the EPIC account.” EX1007, 20:2-3; *generally id.*, 20:1-28. Through this process, the user “enter[s] all credit cards information” for cards that are to be linked to the EPIC account. EX1007, 20:12-13. This setup allows an EPIC authentication server later to look up the “actual payment card account number” and “account name” linked to the EPIC account number while processing a transaction. EX1007, 18:20-25, 18:54-59, 20:30-53. A POSITA thus would have understood that the information entered by the user to link issued payment cards to his/her EPIC account would include, for each card, at least the “actual payment card account number” (i.e., “issued payment information”) and other credit card details such as expiration date and issuer-provided card security code (i.e., “an issuer provided payment information”).

[10.b]: wherein the electronic device comprises device-specific and user-specific information; and,

137. Law discloses that the memory of the device comprises both device-specific and user-specific information. For example, Law describes that during the funding card registration process, the mobile device sends card details as well as “a user provided PIN and the mobile device ID to the payment gateway server.” EX1032, [0082]; *see also id.*, [0092], [0099]; EX1033, [0052], [0062], [0069].

Information such as a mobile device ID and a user's PIN constitute device-specific and user-specific information, respectively. EX1032, [0165]; EX1033, [0132]. In response to the information sent, "the payment gateway server computes a funding card identifier which identifies the given funding card. The payment gateway server stores the funding card identifier in association with the funding card details, mobile device ID and PIN, and it sends the funding card identifier to the mobile device for storage. In an example embodiment, the funding card identifier is a value that is different from the PAN, expiry date or static security code of the funding card." *Id.*; *see also id.*, [0142]-[0143]; EX1033, [0109]-[0110]. Thus, the memory of the device stores the funding card identifier (i.e., device-specific information). *Id.* Law also discloses that the device stores key values for use in generation of the dynamic data used in the payment transaction. EX1032, [0142] (describing a "Kpan" and "Ksec"), [00146]; EX1033, [0109], [0113].

138. Additionally, the payment device according to Gomez stores in memory a "seed value," a "customer key," and a "reference credential." The "seed value," which the device uses to generate an authentication cryptogram, "is unique for each payment card, and corresponds to the payment card identifying number." EX1007, 7:27-34. Further, "the seed value may include certain non-random customer specific information, such as a unique customer key." *Id.*, 7:34- 41. Gomez further describes how the device can store "reference credentials" against which

user-entered credentials are compared for authentication. *Id.*, 9:30-39. The reference credentials limit use of the device to a specific user and provide another example of “user-specific information” stored in memory of the electronic payment device. EX1007, 10:34-36 (describing memory for storage of information on the device), 10:43-46, 11:7-9.

[10.c]: wherein the issuer provided payment information is communicated wirelessly; and,

139. As described above (*supra* [10.b]), Law describes that the issuer provided payment information is communicated wirelessly by the device which includes payment information that the user inputs to the device (e.g., funding card details that the user links to a funding card identifier (EX1032, [0082]; EX1033, [0052])) and an issuer-provided payment card account number and account name. Specifically, Law discloses that payment gateway server 506 is in communication with the mobile device 501 through a wireless network (EX1032, [0089]) and the “mobile device 501 uses a communication system 613 to interact with a wireless network 612” (*id.*, [0092]) as part of the funding card registration process. *See also* EX1033, [0059]-[0062]. Law also describes communication user provided payment information using NFC, which is wireless. EX1032, Abstract; EX1033 [0002].

140. Gomez further describes an “online” account portal that allows a user to enter and submit information about his/her EPIC account using a mobile phone through a “browser interface” or a “native application” (iPhone, Android,

Blackberry, Windows Phone, Windows Mobile, webOS, etc.).” EX1007, 20:2, 20:43-59. The online account portal specifically allows the user to enter and submit information about each of the live/actual payment cards that he/she desires to link (or has linked) to his/her EPIC account (e.g., an account name/number for a live/actual payment card during account setup, or a user’s selection of a particular live/actual payment card previously linked to the EPIC account that the user desires to use in a given transaction). EX1007, 20:1-21:3. In this context, a POSITA would have understood that information that the user enters and submits through a native application or browser interface of the payment device for online account setup and configuration—i.e., information constituting and rendering obvious “issuer provided payment information”—would be communicated wirelessly to an EPIC server. Further, Gomez describes communicating payment card information via NFC, which is wireless. EX1007, 7:49-54. Gomez also describes communicating an account name field via NFC. *Id.*, 14:3-11.²

² I understand from counsel that Patent Owner has identified a Wi-Fi or cellular network communication as [10.c]’s wireless communication. I have been asked to assume that interpretation applies to this limitation. If that interpretation applies, the Law-Gomez disclosure of issuer provided payment information communicated wirelessly aligns with Patent Owner’s interpretation of limitation [10.c].

[10.d]: receiving wirelessly a static device account number payment information for storage on the electronic device;

141. Law and Gomez disclose wirelessly receiving a static device account number for storage on the electronic device.

142. As discussed above (*supra* [10.c]), Law discloses wireless communication between a payment device and payment gateway server. Law further describes the process of receiving a static device account number payment information (i.e., a funding card identifier) for storage on the electronic device. For “each funding card the user wishes to register, the user enters in (e.g. types in) card details into the mobile device (e.g. card details include the name printed on the funding card, the PAN printed on the funding card, the expiry date printed on the funding card, and the static security code printed on the funding card). The mobile device sends this data, plus a user provided PIN and the mobile device ID to the payment gateway server.” EX1032, [0082]; EX1033, [0052]. Law explains that “[f]or each funding card, the payment gateway server computes a funding card identifier which identifies the given funding card.” *Id.* The payment gateway server “stores the funding card identifier in association with the funding card details, mobile device ID and PIN, and it sends the funding card identifier to the mobile device for storage.” *Id.* Law further discloses that “the funding card identifier is a value that is different from the PAN, expiry date or static security code of the funding

card” and “is a random value so that, if intercepted by an adversary, would not be able to recognize any funding card details.” *Id.* Law explains how the mobile device uses a communication system to interact with a wireless network during the registration process. EX1032, [0092]; EX1033, [0062]. Figure 10 of Law illustrates the process of receiving a funding card identifier (i.e. a static device account number payment information) for storage on the device:

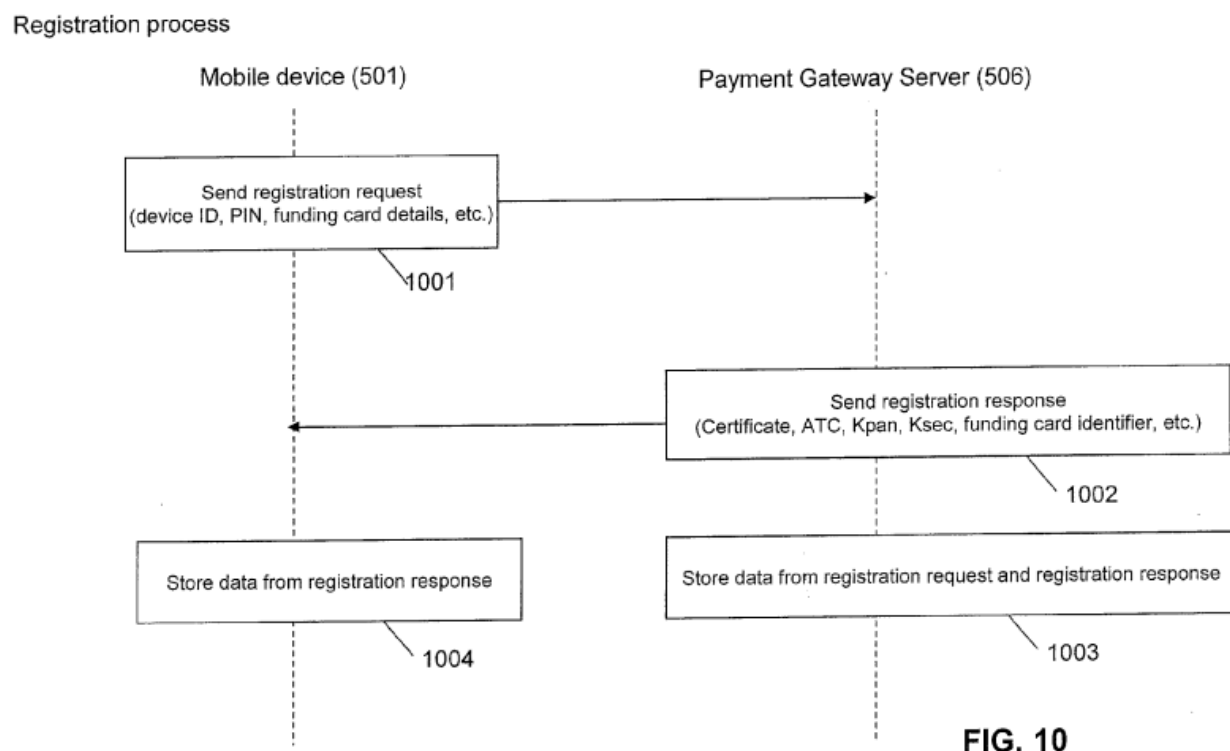


FIG. 10

EX1032, FIG. 10; EX1033, FIG 10. Law also describes communicating user provided payment information using NFC, which is wireless. EX1032 Abstract; EX1033 [0002].

143. Like Law, Gomez describes receiving a static device account number payment information for storage on the electronic device via reception of the static

payment card identifying number. Further, Gomez describes communicating payment card information via NFC, which is wireless. EX1007 7:49-54. Gomez details that the static payment card identifying number—also referred to as an “EPIC” number—“identifies the payment card” and is stored on the device. EX1007, 2:25-27; *see also id.*, 5:13-15 (“In an exemplary embodiment, an EPIC payment card uses a fully static payment card number”), 1:63-64, 13:45-14:2, 22:49-51, 6:10-12, 18:57-59. The EPIC number “identifies the payment card, but does not represent a live account.” *Id.*, 5:13-18; *see also id.*, 13:49-56 (“A fully static (16-digit) account number”). Thus, Gomez’s EPIC number, or static payment card identifying number, is a device-specific number identifying the payment card itself.³

[10.e]: at least a portion of the payment information is a limited-use number for limited use by the device, in place of a issuer provided payment information; and,

144. Law and Gomez disclose that at least a portion of the payment information is a limited-use number used in place of issuer provided payment information. For example, as described above (*supra* [10.c]-[10.d]) Law discloses that during the funding card registration process, the device receives a funding card

³ I understand from counsel that Patent Owner has identified the reception of a tokenized account number over a wireless connection as meeting [10.d]. I have been asked to assume that interpretation applies to this limitation. If that interpretation applies, the Law-Gomez disclosure of wirelessly receiving a static device account number payment information for storage on the electronic device aligns with Patent Owner’s interpretation of limitation [10.d].

identifier which is a value that is different from the issued PAN, expiry date or static security code of the funding card and is random so that, if intercepted by an adversary, actual funding card details would not be recognized. EX1032, [0082]; EX1033, [0052]. As part of this registration process, the device also receives “a certificate, an Application Transaction Counter (ATC), a key value (called Kpan) for generating a PAN, [and] a secure element key value (called Ksec).” EX1032, [0142]; *see also id.* (“The certificate is a client certificate for the mobile device 501 and, in an example embodiment, it is configured to according to the RSA algorithm and has a 2048 bit length. The ATC is a counter that is initially set to a random value between “0” or “1000” and increments with each transaction. The initialized ATC value is a random value to prevent adversaries from predicting the ATC values. Copies of the ATC are stored and synchronise on both the payment gateway server and the mobile device. In an example embodiment, the ATC is a 10 digit value. In an example embodiment, the Kpan is 128 bits long, and the Ksec is 128 bits long.”); EX1033, [0109]. In creating payment information, Law describes the process with reference to Figure 11.

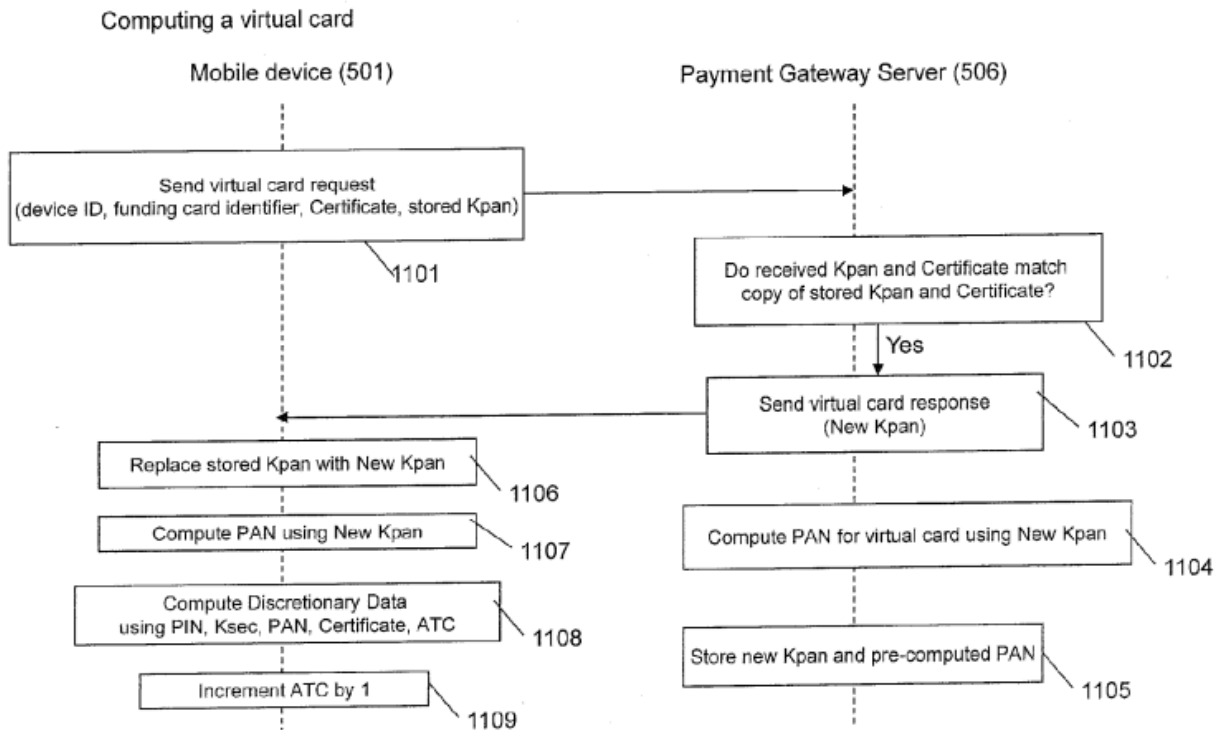


FIG. 11

EX1032, FIG. 11; EX1033, FIG. 11. Law explains that the mobile device 501 sends a virtual card request to the payment gateway server 506 (block 1101) which includes the device ID, the funding card identifier, the certificate and the stored Kpan. EX1032, [0144]; EX1033, [0111]. If the received Kpan and certificate match the Kpan and certificate stored on the payment gateway server, a virtual card response is sent back to the mobile device that includes a new Kpan (block 1103). EX1032, [0145]; EX1033, [0112]. The newly received Kpan is used to compute a different PAN (i.e. limited-use payment information) from the previous transaction for the virtual card. The mobile device then computes discretionary data using the PIN, the Ksec, the PAN, the Certificate, and the ATC (block 1108). EX1032, [0147];

see also id., [0149]-[0155] (describing details of algorithms creating dynamic payment information); EX1033, [0114], [0116]-[0122]. Law explains that discretionary data is dynamic data used in the transaction. EX1032, [0131]; EX1033, [0100]. “The ATC and the PAN keep changing with each transaction, which causes the discretionary data to be dynamic data.” EX1032, [0147]; EX1033, [0114]. A POSITA would recognize that Law’s funding card identifier (i.e., a static device account number payment information) is a limited-use number for limited use by the device in place of a issuer provided payment information.⁴ *Supra* [10.d]. A POSITA would also recognize that values such as Law’s ATC, Kpan, and one-time use discretionary data are limited-use numbers for limited-use by the device, and used in place of issuer provided payment information during the payment transaction process.

145. Additionally, Gomez discloses that the EPIC number (i.e., at least a portion of the payment information) is limited to use by a single device, and thus renders obvious a “limited-use number for limited use by the device.” EX1007,

⁴ I understand from counsel that Patent Owner has identified, among other things, a DPAN (or static number) as meeting [10.e]. I have been asked to assume that interpretation applies to this limitation. If that interpretation applies, the Law-Gomez combination discloses this limitation. I also understand that Patent Owner has identified “a issuer provided payment information” as a “PAN or associated expiration date or CVV.” Applying that interpretation, the Law-Gomez combination discloses that limited-use numbers for limited-use by the device are used in place of at least a PAN (i.e., an actual credit card number). EX1032, [0082]; EX1033, [0052].

2:25-27 (“the static payment card identifying number identifies the payment card”), 7:27-29 (“seed value is unique for each payment card, and corresponds to the payment card identifying number”). Gomez also describes how the EPIC number is used in place of a live/actual card number of an issued payment card linked to the EPIC account (i.e., “a issuer provided payment information”). EX1007, 2:19-20; *see also id.*, 6:29-30, 18:57-59 (“determines a first payment card account number (and corresponding actual account name) which is linked to the EPIC account”), 18:20-25, 2:25-39. Gomez also teaches an “authentication cryptogram” generated uniquely for each transaction, which is paired with the EPIC number and communicated in place of conventional payment information including the live/actual issuer-provided account number, and the account name and/or security code. EX1007, 1:58-2:13, 5:25-60; *generally id.*, 14:36-17:13. This also aligns with Patent Owner’s interpretation of the limitation. I understand from counsel that Patent Owner has identified a cryptogram, among other values, as [10.e]’s “limited-use number” (in addition to [10.f]’s “one-time limited use number”). Thus, Gomez’s disclosure of the EPIC number (i.e., “a static device account number payment information”) and an authentication cryptogram (i.e., “a dynamically-generated one-time limited-use number”) and the use of those values together align with Patent Owner’s interpretation of the limitation. *Id.* Applying that interpretation, the limited-use information generated by the combination of Law-

Gomez would also provide the recited limited-use number for limited use by the device in place of a issuer provided payment information. *Supra* XI.A.1.

[10.f]: dynamically generating a one-time limited-use number based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information; and

146. Law and Gomez disclose a one-time limited-use number is dynamically generated based on at least one of a set of the claimed information. *Supra* XI.A.1. For example, and as discussed above (*supra* [10.e]), Law discloses the creation of a dynamic one-time limited-use number. Specifically, Law explains that dynamic data can be generated based on the “PIN, the Ksec, the PAN, the Certificate, and the ATC.” EX1032, [0147]; *see also id.* (“The ATC and the PAN keep changing with each transaction, which causes the discretionary data to be dynamic data.”); EX1033, [0114]. Law describes the algorithm used to create the dynamic data (EX1032, [0149]-[0154]) and explains that the dynamic data is based on cryptographic number generation. EX1032, [0155] (“Truncation is performed by encoding the SHA results in decimal, then taking the left most digits. It can be appreciated that SHA256 is a known cryptographic hash function, and HMAC is a hash based message authentication code involving a cryptographic hash function in combination with a secret cryptographic key. The secret cryptographic key of the HMAC function is the

concatenated values of Ksec and PIN. The message M is the concatenated values of PAN, Certificate ID and ATC. The Certificate ID is from the Certificate.”); EX1033, [0122]. Thus, Law discloses a PIN (e.g., user-identifying information/user secrets), a mobile device ID (e.g., device information), a Kpan and Ksec (e.g., device secrets), an ATC (e.g., sequence count), and a funding card identifier (e.g., account information), among other values recited in [10.f].

147. Further, according to Gomez, the authentication cryptogram is generated from a “seed value” and a “temporal signal.” EX1007, 5:25-47, 7:17-48. The “seed value” is “unique for each payment card,” and provides combinations of bit values that render obvious “device secrets.” EX1007, 7:27-34; *see also id.*, 12:30-34, 16:31-34, 16:64-17:13. The “seed value” further includes user-identifying information and/or user secrets in the form of “non-random customer specific information, such as a unique customer key.” *Id.*, 7:34-41. Gomez also describes that “a temporal signal value may reflect the date/time of the attempted use [of the card],” and hence the authentication cryptogram can be generated based on time information as recited in [10.f]. *Id.*, 7:19-20. The temporal signal can also include a sequence count. *Id.*, 7:24-26 (“a temporal signal value may reflect the sequence value (or sequential number) of the attempted use”), 8:36-38, 10:66-11:6. Thus, a POSITA would have recognized that the Law-Gomez combination discloses

dynamic generation of a one-time limited-use number based on at least one of the set of values recited in [10.f].

[10.g]: using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.

148. Law and Gomez disclose use of a static device account number and a dynamically generated one-time limited-use number together in place of issuer provided payment information for making a payment transaction. The Law-Gomez combination renders obvious use of a static device account number and a dynamically generated one-time limited-use number together in place of issuer provided payment information for making a payment transaction. *Supra* XI.A.1. As taught in Gomez, the payment device of the Law-Gomez combination renders obvious use of the EPIC number, or static payment card identifying number (i.e., the static device account number) and authentication cryptogram (i.e., the dynamically generated one-time limited-use number) in making a payment transaction. *Id.* The card communicates the payment card identifying number, the authentication cryptogram, and other account information to the payment processing system in place of a live/actual issuer-provided account number for a payment card linked to the customer's EPIC account. EX1007, 2:25-35 ("the static payment card identifying number identifies the payment card, but does not represent a live

account”), 5:20-24, 2:29-39, 7:49-65, 8:16-24, FIGS. 3-4. The cryptogram is also communicated in place of the account holder’s name and/or security code associated with an issuer-provided account. *Id.*, 2:4-13, 5:19-24, 5:29- 32, 2:50-54 (“communicating the authentication cryptogram in a payment card account name field to the payment processing system.”). Gomez shows in FIG. 2, for example, how the EPIC number or card ID and cryptogram are transmitted (444) by the device (442) in place of an account number and name (404) that would otherwise be used in a traditional transaction like that illustrated in FIG. 1. EX1007, FIGS. 1-2.

149. It would have been obvious, and a POSITA would have been motivated, to modify Law in view of Gomez such that complete payment information is formed with a static number and a dynamically-generated number used together when making a payment, as taught by Gomez. *Supra* XI.A.1. The payment information in the resulting combination would be formed, for instance, by combining a static payment card identifying number stored on the mobile device (and received wirelessly on the device after wireless transmission of user provided payment information as taught in Law) with a cryptogram that hashes the combined data and encodes the output of the hash function in a manner suitable for transmission in a contactless connection between the mobile device and payment processing authority (as taught in both Law and Gomez). *See supra* [10.c]-[10.d]; EX1007, 9:12-64. A POSITA would have sought to use a dynamically changing temporal signal in

calculation of the cryptogram (along with a cryptographic technique such as hashing) to ensure that the cryptogram produced in each transaction would vary from prior cryptograms in an unpredictable manner, thereby frustrating the ability of illicit actors to exploit a static device account number and dynamically-generated number from prior transactions to later consummate a fraudulent transaction. *See* EX1007, 1:58-63, 2:21-25, 5:43-47, 9:12-64, 13:63-14:2.

150. The application of Gomez's payment credential techniques to the combination as described above further would have been obvious as a predictable use of known techniques that would have achieved predictable results. *KSR*, 550 U.S. at 417. Indeed, the function and use of Gomez's dynamic number/cryptograms are highly similar to what is disclosed in Law. Law and Gomez each describe contactless transactions from which the user's device submits dynamic limited-use information specifically generated to facilitate validation or authorization of a requested transaction. *See, e.g.*, EX1032, [0156]-[0166]; EX1033, [0123]-[0133]; EX1007, 17:23-18:42. The obviousness of the combination is also underscored by Law, which expressly treats the specific manner of verifying transaction requests with a payment cryptogram as something that would have been well within the capabilities and knowledge of a POSITA. EX1032, [0156]-[0166]; EX1033, [0123]-[0133]. Accordingly, a POSITA would have expected a high likelihood of success implementing the combination with Gomez. *Supra* XI.A.1.

3. Claim 11

[11]: The method of claim 10, wherein the electronic device is configured to accept the user input by at least one of a means comprising: a touch sensor array; a touch screen; a keypad; buttons; device motion; an accelerometer; a biometric input; a proximity contact sensor; optical sensors; an NFC unit; a wireless interface; a wired connection; a USB connection; an RF antenna; an inductor assembly.

151. The Law-Gomez combination discloses that the electronic device is configured to accept the user input by at least a touch sensor array/touch screen, keypad, buttons, and biometric input.

152. Law discloses a touch sensor array that allows a user to input information. EX1032, [0092] (“The mobile device’s display 616 can be a touch-screen type display or another type of display.”), [0100] (“A graphical user interface (GUI) on the menu is able to receive an input from the user to initiate a payment with a virtual card with the payment application[.]”); EX1033, [0062], [0070]. A POSITA would have understood that Law’s touch-screen display includes an array of touch sensors to provide location-dependent detection of user inputs contacting the touch screen. As discussed in ¶¶ 55-57 in connection with EX1041, a POSITA would have understood that touchscreens contain touch-sensor. *Supra* ¶¶ 55-57. Law also discloses a near-field communication (NFC) unit within a mobile device. *See* EX1032 [0088] (“The user 101 also own an NFC-enabled mobile device 501, which includes a payment application. The mobile device 501 is configured to

interact, via NFC, with a merchant POS terminal device 502.”); EX1033 [0058]. Law further discloses that the payment device includes a display. EX1032 [0092], [0100]; EX1033 [0062], [0070].

153. The Law-Gomez combination also renders obvious that the user input comprises at least an input sequence or a gesture by biometric input. For example, Gomez discloses that “[a] fingerprint reader 106 serves as a user credential input device[.]” EX1007, 11:30-31. Further, Gomez describes a “snap” action to “activate the card,” i.e., an unlock operation via snap membranes (i.e., touch sensor array). EX1007, 12:45-48; *see also id.*, 11:39-41 (describing “snap” action as activating the card by briskly snapping the card with a finger).

4. Claim 12

[12]: The method of claim 10, wherein the device-specific information comprises at least one of a set including: device identifiers; device secrets; devices keys; device usage sequence counters; and device account numbers.

154. The Law-Gomez combination discloses that the device-specific information comprises at least device identifiers, device secrets/keys, sequence counters, and device account numbers. *See supra* [10.b]-[10.e]. For example, as part of the funding card identifier provisioning, Law discloses a mobile device ID (“device identifier”). EX1032, [0082], [0158]; EX1033, [0052], [0124]. Law further discloses that the payment gateway server sends a registration response to

the mobile device which includes “include a certificate, an Application Transaction Counter (ATC), a key value (called Kpan) for generating a PAN, a secure element key value (called Ksec), and a funding card identifier that identifies each registered funding card(s).” EX1032, [0142], *see also id.* (“The ATC is a counter that is initially set to a random value between ‘0’ or ‘1000’ and increments with each transaction. The initialized ATC value is a random value to prevent adversaries from predicting the ATC values.”); EX1033, [0109]. Law further discloses that the mobile device increments the ATC by 1 for each transaction. EX1032, [0148]; EX1033, [0115]. Incrementing by 1 generates a sequential parameter. During a transaction, the mobile device computes discretionary data “using the PIN, the Ksec, the PAN, the Certificate, and the ATC (block 1108). The ATC and the PAN keep changing with each transaction, which causes the discretionary data to be dynamic data.” EX1032, [0147]; *see also id.*, [0154]-[0155] (describing the algorithm and values (such as the ATC) used to create the dynamic payment information); EX1033, [0114], [0121]-[0122]. The payment gateway server’s provisioning of data to the mobile device encompasses device-specific information. As explained above, the ATC (“device usage sequence counter”) is initialized to a random value during the device's registration process and is specific to the device, and then stored on both the mobile device and the payment gateway server and kept synchronized. EX1032, [0142], [0158], [0163]-[0164]; EX1033, [0109], [0125], [0130]-[0131]. This

information is then used along with other device-specific information to compute dynamic data for the transaction. *Id.* Further, Law discloses that the payment gateway server provisions a Kpan (“device key”) in response to receiving the mobile device ID. EX1032, [0142]; EX1033, [0109].

155. Gomez also discloses, and the combination provides, a sequence counter (e.g., a sequential instance circuit) configured to generate a sequential parameter that, in turn, is combined with a seed value to generate a message and ultimately an authentication cryptogram when the processor initiates a transaction—each of which renders obvious a limited-duration credit card number. In particular, the temporal signal can indicate a “sequence value (or sequential number) of the attempted use.” EX1007, 7:17-20. “In certain embodiments the temporal signal value may correspond to a unique number which is determined for each sequential attempted use of the card. For example, temporal signal value may increment for each attempted use, or may use an incrementing pointer to reference a table entry stored within the payment card memory.” EX1007, 8:36-41. A “sequential instance circuit” within a “temporal value circuit” of the device generates the sequential parameter when the user attempts to initiate a transaction. *Id.*, 10:64-11:6, FIG. 7 (348). The seed value includes a secret such as a unique customer key or other non-random customer specific information, and is device-specific (i.e., specific to the EPIC card). EX1007, 7:27-28 (“This seed value is unique for each payment

card[.]”), 10:64-11:6 (describing the “sequential instance circuit”), 7:17-20, FIG. 7 (348); *see also id.*, 7:26-47.

5. Claim 13

[13]: The method of claim 10, wherein the user-specific information comprises at least one of a set comprising: an email address; a username; a password; a PIN; a passcode; gestures; user information; bank accounts; payment information; device account numbers; merchant accounts; online accounts; currency amount; currency type; cryptocurrency address; cryptocurrency keys; private/public keys; signature information; and user secrets.

156. The Law-Gomez combination discloses that the user-specific information comprises at least password/PIN/passcode, user information, payment information, device account numbers, private/public keys, and user secrets. *See supra* [10.b]-[10.f].

B. Ground 1B: Claims 14-17 of the '520 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Law in view of Gomez and Spodak

1. Claim 14

[14]: The method of claim 10, further comprising rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name.

157. As an initial matter, I understand that the additional features recited in claim 14 constitute printed matter and are entitled to no patentable weight. *In re DiStefano*, 808 F. 3d 845, 848-851 (Fed. Cir. 2015). Indeed, these features have no structural or functional relationship to the underlying display or other recited elements.

158. The Law-Gomez combination discloses rendering on the display of the electronic device the payment method types stored in the electronic device, wherein the rendering comprising rendering with at least images and alphanumeric characters. For example, Law discloses that multiple funding cards can be added to a payment application on a mobile device. EX1032, [0083] (“It can be appreciated that a single payment application is required on the mobile device, which can manage multiple funding cards. If multiple funding cards are registered, each of the associated funding card identifiers are stored on the mobile device, within the single payment application.”); EX1033, [0053]. Law further discloses that when a user wishes to make a payment, “the user selects the funding card” on the touch-screen display. EX1032, [0084]; *see also id.*, [0100] (“A graphical user interface (GUI) on the menu is able to receive an input from the user to initiate a payment with a virtual card with the payment application (block 705).”); EX1033, [0054], [0070]. “The mobile device 501 then displays the funding cards that have been pre-registered by the user (block 706). A user input is provided to select one of the funding cards

(block 707).” EX1032, [0101]; EX1033, [0071]. Law discloses that an identifier for the payment network associated with the funding card is also stored in the payment application. *Id.*

159. Additionally, Gomez describes how a user can “scroll through available card accounts sequentially displayed on the card, and select[ing] one of the accounts.” EX1007, 20:37-42; *see also id.*, 20:30- 37 (“manually select the actual credit card”). By displaying available card accounts linked to the EPIC account, along with information about the EPIC account itself, the payment device renders on the display the payment method types stored in the electronic device. The displayed accounts can represent cards for different payment methods (e.g., credit or debit cards) and cards from different payment networks (e.g., VISA, MasterCard, Discover, AMEX, etc.). EX1007, 2:19-39; *see also id.*, 11:19-27, 12:64-67. To the extent that Law and Gomez do not expressly disclose all of the recited features of claim 14, it would have been obvious in view of Spodak for the displayed card accounts in the combination to be rendered with images, alphanumeric characters, and iconography including at least one of the set recited in claim 14.

160. Spodak is directed to a “universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.” EX1009, [0002]. The universal card can include a display which can show, among other things, an account number, an expiration date,

a card issuer logo, or any combination of these types of information. *Id.*, [0068] (“The front of the universal card 800 can also have a display 803 which could be used at various times to display an account number, an expiration date, a card issuer logo, any other information, or any combination of these types of information.”), FIG. 8A. Given that the Law-Gomez combination describes displaying payment details on the screen of the device, it would have been obvious to render virtual cards including the features recited in claim 14 on the display of the device in the resulting combination, as taught in Spodak, to provide an intuitive and convenient user interface by which the user could more readily associate different payment card accounts and their payment method types with visual depictions of cards for those accounts. EX1009, [0068].

2. Claim 15

[15]: The method of claim 14, further comprising accepting a user selection of a payment method type for use in a transaction responsive to a user selection from a list of payment method images rendered the display and using a touch screen interface for the user selection.

161. The Law-Gomez-Spodak combination renders obvious accepting a user selection of a payment method type for use in a transaction responsive to a user selection from a list of payment method images rendered on the display with use of a touch-screen interface. As discussed above, Law discloses use of a touch-screen interface (*supra* [10.a], [11], [14]) to select a payment card in a payment application

for use in a payment transaction. *See supra* [10.a], [11], [14]. Spodak discloses that payment methods can be rendered with logos or images. *See supra* [14].

3. Claim 16

[16]: The method of claim 15, wherein the user selection is a default payment method to be used in transactions.

162. The Law-Gomez-Spodak combination renders obvious that a user selection can be a default payment method for use in transactions. Based on Gomez, a POSITA would have found it obvious for a user to select a default payment card to use in transactions with the electronic payment device: “After entering all credit cards information, the customer may establish the default credit usage selection process.” EX1007, 20:12-13; *see also id.*, 20:63- 21:3 (“[T]he current selection may remain active for subsequent purchases until changed by the customer, or the EPIC system may default back to the pre-established credit card selection order defined in the EPIC account.”).

4. Claim 17

[17]: The method of claim 15, wherein the issuer provided payment information is selected from at least one of a set comprising: account number; card number; device account number; expiration date; card security codes; card validation values; card identification numbers; cardholder name; payment method type; merchant account; online account; an account type; a direction of transaction; the payment issuing authority; the amount of currency; the unit of currency; a funds type; cryptocurrency address; cryptocurrency key; cryptocurrency network; and card-type information.

163. The Law-Gomez-Spodak combination renders obvious that the issuer provided payment information is selected from at least one of the set recited in claim 17. For example, Law discloses that the issuer provided payment information sent to a payment gateway server during registration is the user's actual credit card number. EX1032, [0082] (“[F]or each funding card the user wishes to register, the user enters in (e.g. types in) card details into the mobile device (e.g. card details include the name printed on the funding card, the PAN printed on the funding card, the expiry date printed on the funding card, and the static security code printed on the funding card). The mobile device sends this data, plus a user provided PIN and the mobile device ID to the payment gateway server. For each funding card, the payment gateway server computes a funding card identifier which identifies the given funding card.”); EX1033, [0052]; *supra* [10.a]-[10.e].

C. Ground 2A: Claims 18-24 of the '520 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gill in view of Smith, Kay, and Gomez

1. Motivation to Combine Gill, Smith, Kay, and Gomez

164. Gill describes techniques for using a mobile device in a contactless transaction at an ATM. *Supra* X.D. When a user presents the mobile device to a contactless reader (e.g., one having an NFC interface) at the ATM, the mobile device in Gill wirelessly conveys transaction information to the ATM for a requested transaction. EX1034, 5:11-20, 13:43-51, 14:31-37, FIG. 7. Gill notes that “typical content to be transferred ... includes data identifying [a] financial account” for the transaction, such as “account number, name, expiration date, debit/credit, etc.” *Id.*, 5:13-18, 13:41-46, FIG. 6. The ATM and a backend payment infrastructure then processes the information conveyed from the mobile device to complete the transaction. *Id.* Notwithstanding these disclosures, Gill is not explicit in describing the specific information conveyed by the mobile device in a transaction request, or how such information might be secured and deployed to identify a desired payment account. Considering these gaps, it would have been obvious to a POSITA to consider references with additional implementation details and modify Gill in view of Smith such that the mobile device in Gill would be adapted to convey to the ATM at least “payment credentials” for a requested transaction, as credit card, debit card and ATM transactions typically use a payment credential, such as the mobile cloud

account number (MCA) and a payment cryptogram as taught in Smith. *Id.* The payment credentials in the resulting Gill-Smith system would further include information such as “a mobile personal identification number (PIN)” as taught in Smith. EX1035, [0068]. Applying Smith’s proposed use of payment credentials—including an MCA and payment cryptogram—in a system of the resulting combination would have been obvious to a POSITA by the Critical Date of the ’520 patent. As an initial matter, Gill and Smith each describe mobile devices and systems that operate in highly similar contexts. *Id.* Indeed, both Gill and Smith describe mobile devices adapted for contactless transactions, and the mobile devices described in the references are each configured with a virtual wallet to hold a collection of payment vehicles, cards, or accounts for use in a given transaction. EX1034, 10:34-53, FIG. 5; EX1035, [0041], [0075], FIG. 2. Gill further focuses on ATM transactions, and explains that an ATM transaction ordinarily involves (among other things) “debit” transactions—i.e., among the same types of transactions for which Smith’s device was specifically intended to support. EX1034, 2:1-2 (“initiate a debit account transaction”), 4:62-63 (“with ATM transactions, the transaction is generally a debit account transaction”); EX1035 [0029] (“Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.”), [0031] (“debit cards”). A POSITA thus would have understood Smith’s payment credentials

and expected them to be operable in ATM transactions like those discussed in Gill.

165. Moreover, a POSITA would have sought to use payment credentials like Smith's in the combination with Gill (and Kay and Gomez, as described below) to realize predictable security improvements. For example, since the MCA is merely a token for the real card account number (RCA), per Smith, the mobile device can store the MCA without needing to store the RCA, thereby mitigating the risk of the RCA being leaked, hacked, or otherwise compromised from the mobile device itself, or even any transaction involving the mobile device. *See* EX1035, [0034] ("As a result, the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud."); *see also id.* ("A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA). The RCA may correspond to a payment account issued to the user by an issuer 112. The MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.").

166. Conducting contactless transactions with the MCA rather than the RCA would also improve security by preventing unauthorized actors from exploiting the MCA in fraudulent transactions. Because the MCA must be paired with a valid cryptogram for each transaction, a stolen MCA would be insufficient by itself to

conduct a fraudulent transaction without a new, validly generated cryptogram. EX1035, [0070] (“In step 608, the service provider 110 may receive the MCA and additional payment credentials if applicable and may verify (e.g., validate) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art.”), [0040] (“The use of the MCA may enable the user of the mobile device 102 to more securely conduct a contactless payment transaction without using an RCA.”).

167. Additionally, cryptograms in payment devices were common long before the '520 patent. A payment cryptogram like Smith's provides additional security by enabling a transaction processor to verify that the payment credentials submitted in a transaction originated from an authorized device and/or user. For example, Smith teaches that the cryptogram is generated based on device secrets securely stored on the mobile device (referred to as “mobile cloud account data”)—thereby ensuring that unauthorized actors who lack such secrets cannot fraudulently generate a valid cryptogram. EX1035, [0007], [0067]. A POSITA likewise would have sought to require submission of a valid payment cryptogram in ATM transactions of the Gill-Smith-Kay combination to further improve security and reduce the likelihood of fraudulent transactions. The security enhancements stemming from use of both an MCA and a cryptogram in contactless ATM transactions (e.g., credit/debit transactions at an ATM) would have furthered Gill's

objectives of providing for secure transactions with an ATM. *See* EX1034, 1:34-36 (“The absence of contactless functionality with ATMs in the marketplace is largely due to security issues ...”), 4:35-55.

168. Integrating Smith’s suggested use of payment credentials, including at least an MCA and payment cryptogram, in ATM transactions like Gill’s would have amounted to an obvious application of known techniques to improve a similar system in substantially the same way as described in Smith, and would have achieved merely predictable results (e.g., more secure transactions). *KSR*, 550 U.S. at 417. As noted, Gill and Smith each describe mobile devices for contactless transactions (both including credit and debit transactions), and the system in the resulting combination would utilize such payment credentials in substantially the same way taught by Smith. EX1035, [0029]. For each of these reasons, the combination would have been obvious, and a POSITA would have expected a high likelihood of success in pursuing its implementation.

169. Next, it would have been obvious to a POSITA to apply in the combination Kay’s suggestion for a graphical user interface (GUI) on a mobile device, which would allow a user to select a particular type of transaction from a list of available types. Gill discloses that a customer can “input[] instructions to [an] ATM 200 to execute [a] desired transaction.” EX1034, 14:31-36. “The desired transaction may be any type of ATM transaction such as, for example, withdrawing

funds, depositing funds, transferring funds, balance checks, ordering products such as checks, and the like.” *Id.*; *see also id.*, 4:1-3, 5:14-16, 9:15-25 (disclosing a “credit card” as another payment vehicle for an ATM transaction in lieu of a “debit card”). Gill also indicates that the user can input instructions for an ATM transaction (including selecting the desired type of transaction) at the mobile device rather than the ATM, and the user’s instructions are then communicated from the mobile device to the ATM via NFC or another short-range wireless connection. *Id.*, FIG. 7 (depicting instructions input at box 720 through the external apparatus (mobile device) 120), 17:56-62. The mobile device can also include a “graphical user interface (GUI) that allows the user to perform various transactional processes” and that “allow[s] the user to set certain payment preferences or mobile wallet preferences.” *Id.*, 10:42-46; *see also id.*, 13:9-17, FIG. 5.

170. Nonetheless, Gill does not expressly depict the GUI and lacks detail as to how the user would specifically interact with the GUI to input instructions or select a particular type of ATM transaction. Kay demonstrates, however, that such GUIs adapted to receive user instructions for ATM transactions on a mobile device were known well before the ’520 patent. Kay, like Gill, discloses a method of conducting ATM transactions using a mobile device. EX1036, [0038]-[0052], FIGS. 3, 4A-4F. The mobile device includes a mobile banking and wallet application that “allow[s] a user to wirelessly conduct transactions (e.g., payments,

account transfers) using one or more accounts of the customer without a credit card or debit card present” *Id.*, [0039]. The application includes a user interface that allows a user to “choose a category of instructions or transactions.” *Id.* As shown in FIG. 4B (reproduced below), the user interface “present[s] options for ‘withdraw’ 415 and ‘deposit’ 420.” *Id.*, [0040]. “The customer can select withdraw 415 to withdraw cash from the financial transaction terminal,” or select deposit 420 to deposit funds into an account. *Id.* The GUI also allows a user to enter a PIN or other credentials for authentication, and to input an amount for the transaction such as a withdrawal amount as shown in FIG. 4D:

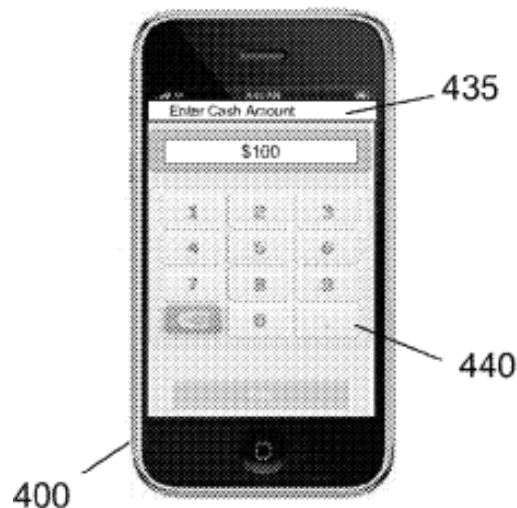


FIG. 4D

EX1036, FIG. 4D; *see also id.*, [0043].

171. Multiple reasons would have motivated a POSITA to implement a GUI like Kay's in the mobile device of the Gill-Smith-Kay combination, in particular a GUI adapted to receive user input for an ATM transaction including a user's selection of a desired transaction type (e.g., withdrawing, depositing, or transferring funds) and an indication of a desired amount for the transaction. To start, such a GUI would have facilitated the user's ability to interact with a mobile device to carry out ATM transactions in the manner described in Gill and Smith. As noted above, Gill's original solution already contemplated that the mobile device would include a GUI for the user to input instructions for ATM transactions. EX1034, 10:42-46, 13:9-17, 14:31-36, FIGS. 5, 7. Kay's GUI provides concrete design elements for a GUI in a similar context, which would allow a user to enter instructions for aspects of the desired transaction (e.g., the transaction amount and type) in a logical and intuitive layout on a small screen of a mobile device (e.g., by guiding the user through a series of interface screens for different stages of the transaction and providing selectable elements in a list of available transaction types). *Id.*; *see also* EX1034, 10:42-46, 13:9-17, 14:31-36, FIGS. 5, 7. By providing a list of selectable transaction types and allowing the user to progress through different interface screens, the user could conveniently enter instructions on the mobile device without needing to separately enter instructions through the ATM. Additionally, integrating

a GUI like Kay's into the resulting combination would have involved no more than a predictable use of a known GUI as taught in Kay to improve similar devices in substantially the same way, and would have achieved merely predictable results (e.g., more secure transactions). *KSR*, 550 U.S. at 417. Kay's GUI is specifically designed for ATM transactions, and would naturally support ATM transactions in the combination as well. Hence, a POSITA would have expected a high likelihood of success combining the teachings of Kay with those of Gill and Smith in the manner described above.

172. Although Smith discloses that the payment cryptogram can be a dynamic number, can take the form of an authorization request cryptogram or a dynamic card validation code, and can be generated based on at least a portion of the mobile cloud account data securely stored on the mobile device, Smith does not expressly disclose many details as to how the payment cryptogram would be made to change across transactions or how the cryptogram would be calculated. Nonetheless, the use of dynamic cryptograms in electronic transaction systems had been known for many years before the Critical Date of the '520 Patent. A POSITA would have known many ways in which a cryptogram like Smith's could be generated so as to provide a unique value for each transaction, and to permit a service provider or issuer to use the cryptogram in authenticating and authorizing transaction requests.

173. Gomez provides one such solution that involves computing a cryptogram based on a “temporal signal” that changes from transaction to transaction. *See, e.g.*, EX1007, 1:64-2:1 (“The authentication cryptogram is generated based upon a seed value stored within the payment card, and further based upon a temporal signal which changes for each attempted use of the payment card[] ...”), 7:17-27 (“a temporal signal is generated which corresponds to the instance of attempted use”; “a temporal signal value may reflect the date/time of the attempted use”; “a temporal signal value may reflect the sequence value (or sequential number) of the attempted use”). In Gomez, the temporal signal is combined with other data stored on the device (e.g., a seed value and static payment card identifying number) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. *Id.*, 8:11-51. The cryptogram is then formed by encoding the output of the hash function. *Id.*, 2:14-17, 8:52-9:11.

174. Because the temporal signal changes with each attempted use, the output of the hash function and the ultimately encoded cryptogram changes with each transaction, even if the seed value remains constant. Gomez explains that “[t]he encoding of the authentication cryptogram renders it extremely difficult for an unauthorized party, without knowledge of the seed value corresponding to the payment card, to generate a new authentication cryptogram in attempt to authorize a future fraudulent transaction.” *Id.*, 5:43-47; *see also id.*, 2:21-25 (“fraudulent use

would not be possible because any attempted transaction would not be approved without an appropriate authentication cryptogram generated uniquely for such transaction”), 1:58-63, 13:63-14:2.

175. It would have been obvious, and a POSITA would have been motivated, to further modify the Gill-Smith-Kay combination in view of Gomez such that the payment cryptogram would be generated using a temporal signal and cryptographic methods like those described in Gomez. The cryptogram in the resulting combination with Gomez could be formed, for instance, by combining at least a portion of the mobile cloud account data stored on the mobile device (as taught in Smith) with a temporal signal (as taught in Gomez), hashing the combined data, and encoding the output of the hash function in a manner suitable for transmission in a contactless connection between the mobile device and the ATM. *Id.* A POSITA would have sought to use a dynamically changing temporal signal in calculation of the cryptogram (along with a cryptographic technique such as hashing) to ensure that the cryptogram produced in each transaction would vary from prior cryptograms in an unpredictable manner, thereby frustrating the ability of illicit actors to exploit an MCA and cryptograms from prior transactions to later consummate a fraudulent transaction. *See* EX1007, 1:58- 63, 2:21-25, 5:43-47, 13:63-14:2.

176. The application of Gomez’s cryptogram techniques to the combination as described above further would have been obvious as a predictable use of known

techniques that would have achieved no more than predictable results. *KSR*, 550 U.S. at 417. Indeed, the function and use of Gomez’s cryptograms are highly similar to Smith’s. Smith and Gomez each describe contactless transactions from which the user’s device submits a token account number (e.g., an MCA in Smith or an EPIC number (static payment card identifying number) in Gomez) paired with a cryptogram that is specifically generated to facilitate validation or authorization of a requested transaction. *See, e.g.*, EX1035, [0070]-[0071]; EX1007, 18:20-25, 18:54-59. The obviousness of the combination is also underscored by Smith, which expressly treats the specific manner of verifying transaction requests with a payment cryptogram as something that would have been well within the capabilities and knowledge of a POSITA. EX1035, [0070] (“service provider 110 ... may verify (e.g., validate) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art”). Accordingly, a POSITA would have expected a high likelihood of success implementing the combination with Gomez.

177. In the combination described above, the teachings of Gill in view of Smith, Kay, and Gomez would have rendered obvious claims 18-24, and the combination would have provided each element of these claims for the reasons described in detail below.

2. Claim 18

[18.pre]: A method of facilitating and authorizing an automated teller machine (ATM) transaction involving an electronic device, wherein an electronic device transacts wirelessly with an ATM, the method comprising:

178. Whether or not the preamble is a limitation, the Gill-Smith-Kay-Gomez combination renders obvious the recited method. For example, Gill discloses “methods ... for receiving a contactless transmission from an external apparatus to an ATM.” EX1034, 4:28-34; *see also id.*, Abstract. The external apparatus can be a mobile device (electronic device) having a contactless transmission interface that allows the mobile device to transact wirelessly with the ATM. *Id.*, 5:13-18 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received ...”), 3:56-63 (“[T]he term ‘tap’ or ‘tapping’ may refer to bringing an external apparatus close to or within the proximity of an ATM contactless interface so that information can be communicated wirelessly between the external apparatus and the ATM using short range wireless transmission technology, such [as] near-field communication (NFC) technology, radio-frequency (RF) technology, or the like.”), 9:63-10:4 (“A ‘mobile device’ 500 may be any mobile communication device, such as a cellular telecommunications device (i.e., a cell phone or mobile phone), personal digital assistant (PDA), ... or the like.”), FIG. 5. Gill describes a range of possible transactions that can be performed with a mobile device and ATM,

including withdrawals, deposits, and fund transfers. *Id.*, 14:32-36.

179. Gill further describes techniques for authorizing an ATM transaction, e.g., by requiring that the user enter a valid PIN or otherwise be authenticated before initiating or otherwise carrying out a transaction. EX1034, 5:11-20 (“the ATM is configured to ... require further security authorization in order to access the desired financial account at the ATM” and “[g]enerally speaking, the further security authorization will require at least the input of the proper PIN associated with the account”), 7:29-46 (“require users to identify and/or authenticate themselves ... before the ATM 200 will initiate, perform, complete, and/or facilitate a transaction”), 13:23-31 (“memory 520 may include such data as user authentication information to gain access to the mobile wallet application 521, user authentication information for each payment vehicle that is stored by or accessible via the mobile wallet application 521, user authentication information to access the secure module 581 of the mobile wallet chip 580, etc.”), 13:47-51, 14:9-30, FIGS. 6 (614), 7 (715).

[18.a]: providing, by the electronic device, at least one of account information; identification; and authorization, for the ATM transaction; and,

180. Gill-Smith-Kay-Gomez renders obvious providing, by the mobile (electronic) device, account information, identification, and authorization for the

ATM transaction.⁵

181. As to “account information,” Gill’s mobile device provides such information to the ATM terminal via a contactless/wireless connection when a user “taps” the mobile device at the ATM. EX1034, 5:11-20 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received (i.e. account information, for example, account number name, expiration date, debit/credit, etc.) and require further security authorization in order to access the desired financial account at the ATM.”), 13:41-46 (“typical content to be transferred from the external apparatus 120 includes data identifying the financial account associated with the external apparatus”), FIGS. 6-7. Gill also discloses that the mobile device transmits account information as “payment vehicle data.” *Id.*, 12:29-32 (“the antenna and other hardware or software that transmit payment vehicle data from the secure module 581 of the mobile device 500 may be integrated into the secure module 581”), 11:7-16 (“payment vehicle data 571 for each payment vehicle that is stored in the secure module 581 may include the payment vehicle type, the payment vehicle number, the name associated with the payment vehicle, the expiration date of the payment vehicle, the security code associated with the payment vehicle, ... etc.”).

⁵ While the combination addresses all three recited items (i.e., account information, identification, and authorization), it is my understanding that only one is required to satisfy the claim element.

182. In the combination, and based on Smith, the mobile device provides account information via a contactless/wireless connection including a mobile cloud account number (MCA) and a payment cryptogram. EX1035, [0067] (“The term ‘tapping’ may refer to the transmission of payment credentials via near field communication from the mobile device 102 to the contactless terminal 104 due to the close proximity of the mobile device 102 to the terminal 104. The payment credentials may include a payment cryptogram The contactless terminal 104 may forward the payment credentials, including the MCA and payment cryptogram, to the acquirer 106[] ...”), [0034] (“A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA). The RCA may correspond to a payment account issued to the user by an issuer 112.”), FIG. 6.

183. As to “identification” and “authorization,” the payment vehicle data provided by the mobile device includes a “security code associated with the payment vehicle.” EX1034, 11:9-14. A POSITA would have understood that the security code in a payment vehicle is used to verify the identity of a device or user and to authorize a transaction. Further, in the combination, the information transmitted from the mobile device identifies the requested financial account for a transaction. *Id.* For example, according to Smith, the mobile device conveys the MCA (and a corresponding cryptogram) to identify the account associated with a requested

transaction. The MCA functions to identify the requested account, e.g., it is linked to a real card account number (RCA) by the service provider and the RCA “correspond[s] to a payment account issued to the user by an issuer 112.” EX1035, [0034], [0067]. The MCA and cryptogram are packaged as payment credentials in an “authorization request” and used by a service provider and/or issuer to validate the request or deny authorization for a transaction. EX1035, [0070]-[0072], FIG. 6; *infra*, [18.g].

184. Gill-Smith-Kay-Gomez also renders obvious identification and authorization in a transaction in which a user authenticates himself/herself by presenting valid credential(s). EX1034, 5:15-18 (“require further security authorization in order to access the desired financial account at the ATM”; “the further security authorization will require at least the input of the proper PIN associated with the account”), 7:29-46 (“require users to identify and/or authenticate themselves to the ATM 200 before the ATM 200 will initiate, perform, complete, and/or facilitate a transaction”), 13:47-51, 14:9-30 (“the customer may input authentication information on his external apparatus 120”), FIGS. 6-7; EX1035, [0068] (“credentials may include a mobile personal identification number (PIN), [0069]- [0071].

[18.b]: wherein the electronic device comprises a user interface comprising: displays; touch sensors; and buttons; and,

185. Gill-Smith-Kay-Gomez renders obvious a mobile device (electronic device) comprising a user interface that includes displays, touch sensors, and buttons.

186. For example, Gill teaches that “the mobile device 500 may have a user interface that includes user output devices 536 and/or user input devices 540.” EX1034, 12:33-44, FIG. 5. “The user output devices 536 may include a display 530 (e.g., a liquid crystal display (LCD) or the like)” *Id.* “The user input devices 540, which may allow the mobile device 500 to receive data from a user 110, may include any of a number of devices allowing the mobile device 500 to receive data from a user, such as a keypad, keyboard, touch-screen, touchpad, microphone, mouse, joystick, other pointer device, button, soft key, and/or other input device(s).” EX1034, 12:33-44. A POSITA would have understood that a touch-screen and touchpad would include touch sensors to permit positional detection of a user’s contact with the touch-screen or touchpad, respectively. A keypad and keyboard would each include mechanical buttons, while a graphical user interface would include virtual or soft buttons such as the buttons 415, 420 and buttons 440 like those depicted in the GUIs disclosed in Kay (and applied to the Gill-Smith-Kay-Gomez combination). EX1036, FIGS. 4B, 4D. A POSITA would have known of mobile

devices as of the Critical Date of the '520 patent whose user interfaces commonly included such physical display elements as touch sensors and buttons.

187. Gill-Smith-Kay-Gomez also provides multiple “displays” at least to the same extent as the specification of the '520 patent itself, which refers to just a single display 250/450. *See* EX1001, FIGS. 2A-2B, 4A-4B. Even if [18.b] is interpreted to require multiple physical displays, a POSITA would have known that mobile devices like Gill’s and Smith’s can include multiple displays, and it would have been obvious and beneficial to provide multiple displays in the mobile device of the Gill-Smith-Kay-Gomez combination to expand options available for displaying information to a user. A POSITA would have appreciated that the provision of multiple displays would allow for different sets of information to be presented to the user simultaneously or at different times thereby expanding viewing options for the user (e.g., a first set of information could be displayed on a primary display located at a first part of the device and additional information could be displayed on a secondary display at a second part of the device). *Id.*

188. To the extent the term “displays” encompasses virtual display elements on a physical display, the combination also provides such features. Kay, for example, discloses a series of display screens that each depict multiple display elements allowing a user to input instructions for an ATM transaction, such as displays of elements 415, 420 for selecting a desired transaction type, displays of

elements 430 for inputting a PIN, and displays of elements 440 for inputting a transaction amount. EX1036, FIGS. 4A-4C.

[18.c]: recording a user selection from the user interface of the electronic device of a user selected account from which the electronic device is operable to wirelessly convey with an ATM; and,

189. Gill-Smith-Kay-Gomez renders obvious recording a user selection from the user interface of the mobile device (electronic device) of a user-selected account from which the device is operable to wirelessly convey with an ATM. For example, Gill discloses that “the GUI for the mobile wallet application 521 may allow the user 110 to enter input to select a payment vehicle” for a transaction. EX1034, 13:9-17; *see also id.*, 4:1-6 (“the term ‘payment vehicle’ may refer to an electronic payment vehicle, such as an ‘electronic credit or debit card’” or other “account identifying information stored electronically in a mobile device”). The mobile device is operable to convey data corresponding to the selected payment vehicle (and thus the selected account) to an ATM. *Id.*, 5:13- 16 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received (i.e. account information, for example[] ...)”), 6:42-49 (“The contactless interface 300 is configured to contactlessly and/or wirelessly send and/or receive information over relatively short ranges.”), 13:44-46 (“typical content to be transferred from the external apparatus 120 includes data identifying the financial account associated with the external apparatus”).

190. In the combination, Smith also discloses that the user can select a particular account from a GUI to cause the mobile device to wirelessly convey payment credentials corresponding to the selected account (including an MCA and payment cryptogram). EX1035, [0067]-[0068], [0075] (“The wallet 202 may store the mobile cloud account 704 and related data (e.g., MCA, post issuance scripts, etc.) for selection by the user 302 for use in a contactless payment transaction.”), FIGS. 6-7.

191. A POSITA further would have understood and/or it would have been obvious for the mobile device to record the user’s selection. This is evident, for example, from the fact that the mobile device properly acts on the user’s selection by conveying information to the ATM for the correct account in accordance with the user’s selection. EX1035, [0067]-[0068], [0075]; EX1034, 5:13-16, 13:9-17.

[18.d]: recording a user selection from the user interface of the electronic device of a user selected account operation, wherein said user selected account operation is selected from a list of funds transfer operations; and,

192. Based on Gill, it would have been obvious for the device to present a GUI that allows the user to enter transaction instructions “indicating what type of financial transaction the authenticated user wants to conduct at the contactless ATM.” EX1034, 18:19-22. For example, the user can select among transaction types that include “withdrawing funds, depositing funds, transferring funds,

balanc[ing] checks, ... and the like.” *Id.*, 14:31-37; *see also id.*, 19:12-19 (“[R]eceive financial transaction instructions from an authenticated user associated with the external apparatus via the connection between the contactless ATM and the communication sticker affixed to the external apparatus, wherein financial transactions include withdrawing, depositing, or transferring funds and ordering financial institution products”). Figure 7 shows the user inputting transaction instructions at the mobile device (external apparatus 120):

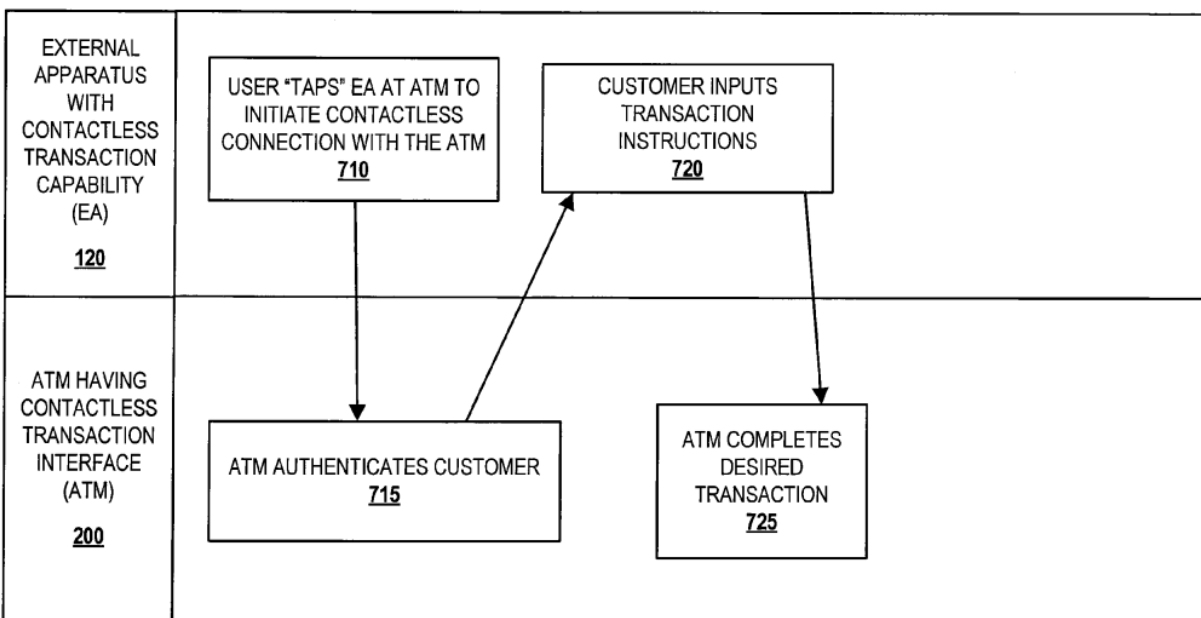
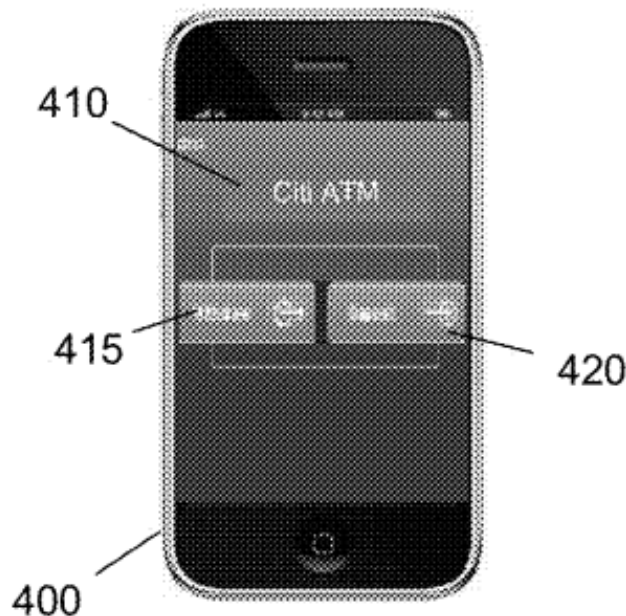


FIG. 7

EX1034, FIG. 7 (720); *see also id.*, 12:33-34, 13:9-17 (describing mobile device GUI).

193. Based on Kay, it would have been obvious for the user to select from the GUI a desired ATM funds transfer operation from a list that includes, for example, depositing and withdrawing funds from an account.



EX1036, FIG. 4B (illustrating withdraw 415 and deposit 420); *see also id.*, [0040] (“As shown in FIG. 4B, a mobile device 400 has received a request to conduct a transaction at a financial transaction terminal, such as an ATM ..., and is presenting on the display of the mobile device 400 a user interface ... presenting options for ‘withdraw’ 415 and ‘deposit’ 420. The customer can select withdraw 415 to withdraw cash from the financial transaction terminal.”); *generally id.*, [0038]-[0044], FIGS. 3-4.

194. Kay's teachings in this regard would have been obvious to apply to the combination with Gill, Smith, and Gomez for the reasons described above. In the combination, the GUI would predictably allow the user to select from a list of funds transfer operations such as "withdrawing funds, depositing funds, transferring funds, ... and the like." EX1034, 14:31-37. A POSITA would have understood and/or it would have been obvious that the mobile device records the user's election of the user's indicated operation. This is evident, for example, from the fact that the mobile device properly acts on the user's selection by proceeding to carry out the indicated operation. *Id.*; EX1034, FIG. 7; EX1036, [0040]-[0041].

[18.e]: wherein user input information from the user interface includes at least one of a set comprising: identification, account, amount of currency, operation and authorizing information; and,

195. Gill-Smith-Kay-Gomez renders obvious receiving user input information from the user interface that includes at least one from the set recited in [18.e].

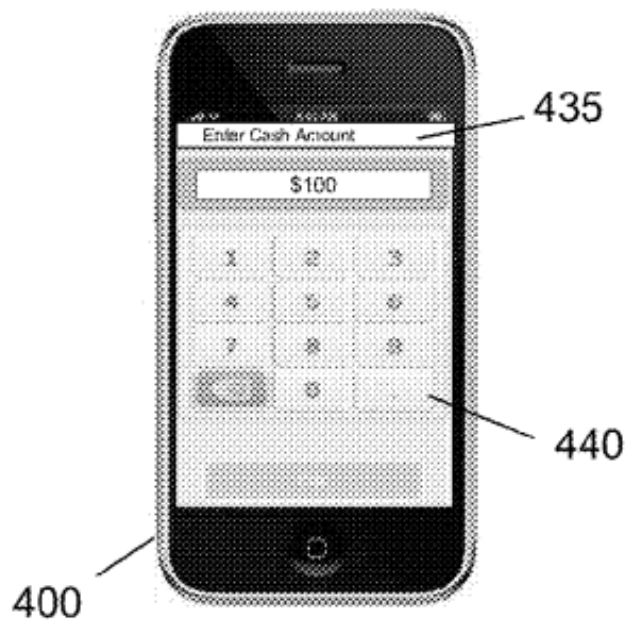
196. For example, Gill describes how the user can input identification and/or authorizing information to authenticate himself/herself for a transaction. EX1034, 14:15-21 ("the customer may input authentication information on his external apparatus 120 and such transfer such data to the ATM 200 upon establishing the contactless connection"), 13:23-31 ("memory 520 may include such data as user authentication information to gain access to the mobile wallet application 521, user

authentication information for each payment vehicle that is stored by or accessible via the mobile wallet application 521, user authentication information to access the secure module 581 of the mobile wallet chip 580, etc.”); *see also id.*, EX1036, [0041] and FIG. 4C (user-entered pin).

197. Gill further describes user inputs from the user interface regarding account information. EX1034, 13:14-15 (“The GUI for the mobile wallet application 521 may allow the user 110 to enter input to select a payment vehicle”); *supra*, [18.a].

198. Gill also describes user inputs received at the mobile device directed to operations of the device. EX1034, FIG. 7 (715-720) (depicting the user inputting instructions to the external apparatus 120 to execute the desired transaction); *see also id.*, 14:31-37.

199. In the combination, Kay also discloses the mobile device receiving user input information from a user interface indicating an “amount of currency” for a transaction. EX1036, [0043] (“In 340, the customer enters the amount of cash to withdraw and confirms the transaction. As shown in FIG. 4D, a mobile device 400 has a user interface that prompts the customer to ‘Enter Cash Amount’ 435 using a keypad 440 on a touchscreen of the mobile device 400 ...”).



EX1036, FIG. 4D (illustrating amount of currency entered on device); *see also* EX1034, 12:33-34, 13:9-17 (describing mobile device GUI).

[18.f]: wherein the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC; and,

200. Gill-Smith-Kay-Gomez renders obvious that the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC. Gill discloses that interactions between the mobile device and the ATM occur wirelessly via near-field communications (NFC). EX1034, 3:56-67 (“the term ‘tap’ or ‘tapping’ may refer to bringing an external apparatus close to or within the proximity of an ATM contactless interface so that information can be communicated wirelessly between the external apparatus

and the ATM using short range wireless transmission technology, such near-field communication (NFC) technology”), 14:15-21 (“the customer may input authentication information on his external apparatus 120 and such transfer such data to the ATM 200 upon establishing the contactless connection”), 5:11-18 (“the ATM is configured to process the data received ...”), 13:41-46 (“typical content to be transferred from the external apparatus 120 includes data identifying the financial account associated with the external apparatus”). For example, as shown in FIG. 7, “the customer taps the external apparatus 120 at the ATM 200 to initiate a contactless connection with the ATM,” and proceeds to exchange wirelessly the identification, selection, information and authorizing operations as described above with respect to [18.a] and [18.c]-[18.e]. EX1034, 13:51-14:37; *see also id.*, 13:32-51, FIG. 6.

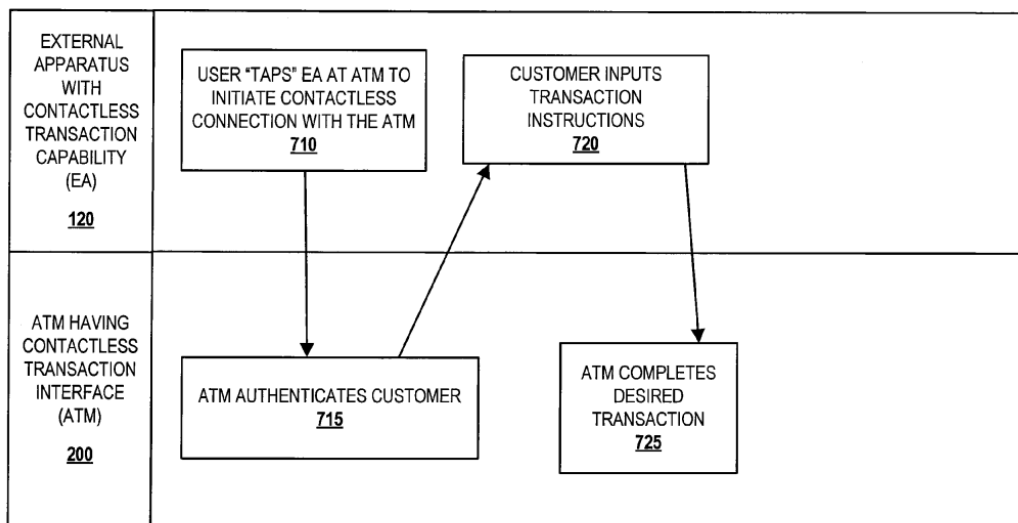


FIG. 7

EX1034, FIG. 7 (communication between external apparatus 120 and ATM 200).

201. Smith also discloses, and the combination provides for, the exchange of payment credentials (including an MCA and payment cryptogram) wirelessly between the mobile device and a terminal. *Supra*, [18.a]. The payment credentials are useful to identify and authorize the device for a transaction, and they correspond to an account indicated by a user's selection. EX1035, [0067] ("The term 'tapping' may refer to the transmission of payment credentials via near field communication from the mobile device 102 to the contactless terminal 104 due to the close proximity of the mobile device 102 to the terminal 104. The payment credentials may include a payment cryptogram The contactless terminal 104 may forward the payment credentials, including the MCA and payment cryptogram, to the acquirer 106[] ..."), [0034] ("A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA). The RCA may correspond to a payment account issued to the user by an issuer 112."); *see also id*, [0045], [0058]-[0059] (describing user's selection of a payment account for a transaction), FIG. 6; *supra*, [18.a].

[18.g]: wherein the ATM is configured for performing the user selected account operation using the identification and authorizing information; and,

202. Gill-Smith-Kay-Gomez renders obvious configuring the ATM to perform the user-selected account operation using identification and authorization information received wirelessly from the mobile device. *Supra*, [18.a], [18.c]-[18.f].

For example, Gill teaches that the ATM authenticates the customer based on credentials (e.g., a PIN) received wirelessly from the mobile device. EX1034, 14:17-20 (“the customer may input authentication information on his external apparatus 120 and such transfer such data to the ATM 200 upon establishing the contactless connection”), 13:47-48 (“ATM 200 authenticates the user”), FIG. 6 (614), FIG. 7 (715). Once the ATM receives further transaction instructions including the user-selected account operation and identification and authorizing information, Gill discloses that the ATM is configured to “execute the desired transaction.” *Id.*, 14:31-37, FIG. 7 (720); *see also id.*, 5:11-20, 7:29-46 (“ATM 200 will initiate, perform, complete, and/or facilitate a transaction”).

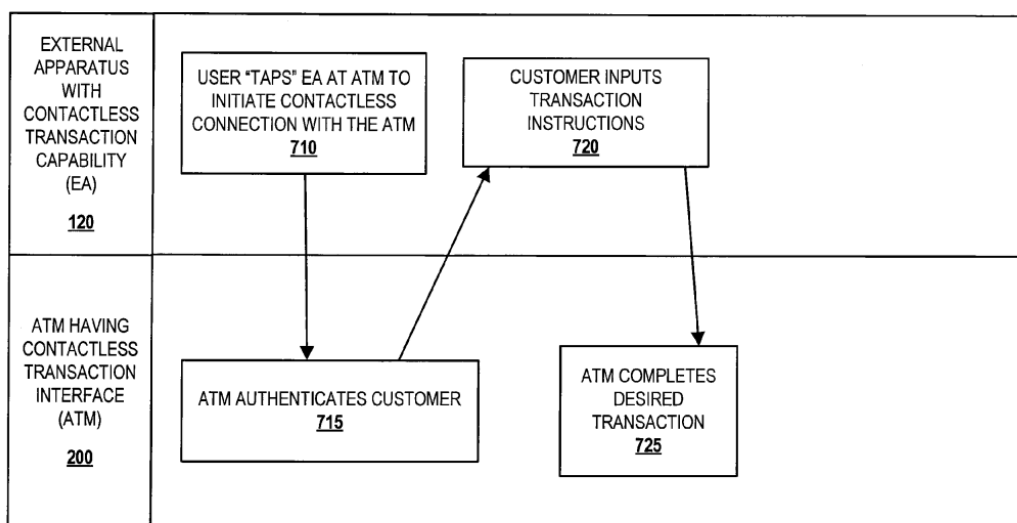


FIG. 7

EX1034, FIG. 7 (steps 720 and 725).

[18.h]: wherein the identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions; and,

203. Gill-Smith-Kay-Gomez renders obvious exchanging wirelessly with an ATM transaction data including account, identification, and authorizing information, as discussed above. *Supra* [18.a], [18.b]-[18.f].

204. Based on Smith, it would have been obvious for the wireless exchange to further involve transmission of a mobile card account number (MCA) and a payment cryptogram from a mobile device to a terminal. EX1035, [0067] (“In step 602, the user 302 may ‘tap’ the contactless terminal 104 using the mobile device 102 with payment credentials loaded into the mobile cardlet in the secure storage 210. The term ‘tapping’ may refer to the transmission of payment credentials via near field communication from the mobile device 102 to the contactless terminal 104 due to the close proximity of the mobile device 102 to the terminal 104, which sometimes may result in the mobile device 102 physically tapping the terminal 104. The payment credentials may include a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code[] ... The contactless terminal 104 may forward the payment credentials, including the MCA and payment cryptogram ...”), FIG. 6; *see also id.*, [0051] (“MCAs for use in conducting contactless payment transactions”).

205. The MCA is a statically generated limited-use number portion of the payment credentials provisioned to the mobile device, and is linked by a service provider to a real card account number (RCA) for an actual account of the user. EX1035, [0040] (“The use of the MCA may enable the user of the mobile device 102 to more securely conduct a contactless payment transaction without using an RCA.”), [0034] (“The RCA may correspond to a payment account issued to the user by an issuer 112. The MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.”). The MCA remains unchanged and static across transactions initiated by the mobile device, but has a limited period of use defined by an expiration date assigned to the MCA. *Id.*, [0086] (“the generated MCA may include an expiration date”).

206. Further, according to Smith, the payment cryptogram can be a “dynamic card validation code” or an “authorization request cryptogram,” either of which a POSITA would have understood and found obvious to be a dynamically-generated limited-use number portion of the payment credentials. EX1035, [0103], [0067], [0096]-[0097], [0063]. Smith specifically explains that the payment cryptogram is “generated” for each transaction—in contrast to the MCA which is read from memory of the device. EX1035, [0067]. The significance of the

cryptogram having a dynamic, limited use would have been apparent to a POSITA, as it was commonly understood that updating the cryptogram on a frequent basis (e.g., with each transaction) protects against the risk of payment credentials (including the MCA and cryptogram) from a prior transaction being reused by an illicit actor to conduct a fraudulent transaction with the same credentials. Instead, Smith explains that the service provider can identify and authorize a transaction request by verifying the cryptogram using known techniques. EX1035, [0070] (“the service provider 110 may receive the MCA and additional payment credentials if applicable and may verify (e.g., validate) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art”), [0067] (cryptogram generated based on secret “mobile cloud account data stored in the secure element 210” of the mobile device). The service provider’s verification of the MCA and associated cryptogram identifies that the transaction request was initiated from an authorized user’s device, and can be used to validate the request or deny authorization for the transaction. *Id.*, [0070] (“If the verification of the credentials fails, then, in step 610, the payment network 108 may receive an indication from the service provider 110 to deny the authorization”), [0071]-[0072]. It would have been obvious to apply Smith’s suggested use of statically and dynamically generated limited-use number portions including an MCA and cryptogram in the resulting combination for the reasons

discussed above in the combination overview. *Supra* § XI.C.1.

207. Moreover, Gomez discloses that the payment cryptogram is dynamically generated based on a temporal signal and constitutes “dynamically generated limited-use number portions” that change from transaction to transaction. EX1007, 1:64-2:1 (“The authentication cryptogram is generated based upon ... a temporal signal which changes for each attempted use of the payment card[] ...”), 7:17-27 (“a temporal signal is generated which corresponds to the instance of attempted use”; “a temporal signal value may reflect the date/time of the attempted use”; “a temporal signal value may reflect the sequence value (or sequential number) of the attempted use”), 2:21-25 (“fraudulent use would not be possible because any attempted transaction would not be approved without an appropriate authentication cryptogram generated uniquely for such transaction”). Gomez further discloses that the temporal signal value is combined with other data stored on the device (e.g., a seed value and static payment card identifying number) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. *Id.*, 8:11-51. The cryptogram is then formed by encoding the output of the hash function. *Id.*, 2:14-17, 8:52-9:11. Gomez explains that “[t]he encoding of the authentication cryptogram renders it extremely difficult for an unauthorized party, without knowledge of the seed value corresponding to the payment card, to generate a new authentication cryptogram in attempt to authorize a future fraudulent transaction.”

EX1007, 5:43-47; *see also id.*, 2:21-25 (“fraudulent use would not be possible because any attempted transaction would not be approved without an appropriate authentication cryptogram generated uniquely for such transaction”), 1:58-63, 13:63-14:2. It would have been obvious to apply Gomez’s suggested use of statically and dynamically generated number portions including a static payment card identifying number and authentication cryptogram in the resulting combination for the reasons discussed above in the combination overview. *Supra* XI.C.1. The cryptogram in the resulting combination with Gomez could be formed by combining at least a portion of the mobile cloud account data stored on the mobile device (as taught in Smith) with a temporal signal (as taught in Gomez), hashing the combined data, and encoding the output of the hash function in a manner suitable for transmission in a contactless connection between the mobile device and the ATM. *Id.* A POSITA would have sought to use a dynamically changing temporal signal in calculation of the cryptogram (along with a cryptographic technique such as hashing) to ensure that the cryptogram produced in each transaction would vary from prior cryptograms in an unpredictable manner, thereby frustrating the ability of illicit actors to exploit an MCA and cryptograms from prior transactions to later consummate a fraudulent transaction. *See* EX1007, 1:58- 63, 2:21-25, 5:43-47, 13:63-14:2. The application of Gomez’s cryptogram techniques to the combination as described above further would have been obvious as a predictable use of known

techniques that would have achieved no more than predictable results. *KSR*, 550 U.S. at 417. Accordingly, a POSITA would have expected a high likelihood of success implementing the combination with Gomez.

[18.i]: wherein said static and dynamic information is combined to perform the user selected ATM operation.

208. Smith discloses, and the combination renders obvious, that the MCA and payment cryptogram, i.e., said static and dynamic information, is combined into “payment credentials” to form an authorization request for performance of a user-selected operation. EX1035, [0067] (“the payment credentials, including the MCA and payment cryptogram”; “‘tapping’ may refer to the transmission of payment credentials via near field communication from the mobile device 102”), FIG. 6 (602); *see also id.*, [0059] (“the user 302 may (e.g., via the display UI 204), select an MCA for use in funding a contactless payment transaction”).⁶ In the combination as described above (*supra* IX.C.1), the MCA and cryptogram are combined into payment credentials to perform a user-selected ATM operation such as a deposit, withdrawal, or funds transfer operation like those described in Gill, Smith, Kay, and

⁶ Smith alternately refers to the MCA and payment cryptogram being combined to form “transaction data.” EX1035, [0011] (“The receiving device is configured to receive transaction data related to a financial transaction, wherein the transaction data includes at least an MCA and a payment cryptogram.”), [0096] (“In step 1104, a receiving device may receive transaction data related to a financial transaction, wherein the transaction data may include at least an MCA and a payment cryptogram.”).

Gomez. EX1034, 14:34-37; EX1035, [0029] (“Transactions that may be performed via a payment network include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.”), [0031] (“Payment cards may include ... debit cards”); *supra*, [18.g].

3. Claim 19

[19]: A method of claim 18, wherein the identification and authorizing information is generated from at least one of a set identification and data comprising: ATM accounts; user identification; biometric user identification; device-identifiers; email address; username; transactional information; merchant identifiers; facility location; user accounts; cryptocurrency address; cryptocurrency keys; merchant accounts; online accounts; bank accounts; device account numbers; payment numbers; card issuing authority; and payment-issuer; and wherein further the data includes at least one of time; duration; passwords; passcodes; device position; device motion; device-specifics; secrets; keys; a currency; currency amounts; cryptocurrency amount; transaction limits; transaction records; usage duration; and usage sequence counts.

209. Gill describes how identification and authorization information is generated from “account information” and/or “payment vehicle data” that includes an account name (e.g., user identification or username), an account number (e.g., payment numbers, ATM accounts, bank account), and an expiration date (e.g., transaction information). EX1034, 5:11-20 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received (i.e. account

information, for example, account number, name, expiration date, debit/credit, etc.)”), 12:29-32 (“that transmit payment vehicle data from the secure module 581 of the mobile device 500”), 11:7-16 (“payment vehicle data 571 for each payment vehicle that is stored in the secure module 581 may include the payment vehicle type, the payment vehicle number, the name associated with the payment vehicle, the expiration date of the payment vehicle, the security code associated with the payment vehicle, whether the payment vehicle is a credit or debit payment vehicle, gift card payment vehicle, etc”). Gill further describes identification and authorization information is generated from credentials (e.g., secrets, passwords, or passcodes) such as a user’s PIN. *Id.*, 5:18-20 (“the further security authorization will require at least the input of the proper PIN associated with the account”), 7:34-40 (“authenticate an ATM user based at least partially on an ATM debit card, smart card, token ..., username, password, PIN, biometric information, and/or one or more other credentials”), 14:13-20.

210. Smith further discloses, and the combination provides, that the mobile device generates transaction data or payment credentials for identification and authorization from an MCA and a payment cryptogram. *Supra* [18.h]-[18.i]; EX1035, [0067]. The MCA points to a real card account and constitutes a device account number, payment number, and/or device identifier. *Id.* The cryptogram is generated based on secret mobile cloud account data stored on the mobile device,

including secrets and a key. EX1035, [0067] (“The payment credentials may include a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code, generated based on at least a portion of the mobile cloud account data stored in the secure element 210.”), [0086] (“The mobile cloud account data 802 may include at least the issuer public key certificate, the ICC public key certificate, and the MCA. In some embodiments, the generated MCA may include an expiration date, which may be further included in the mobile cloud account data 802. In one embodiment, the mobile cloud account data 802 may further include static track data and initialization vectors”).

211. Gomez further discloses, and the combination provides, that the mobile device generates transaction data or payment credentials for identification and authorization from a static payment card identifying number and authentication cryptogram. Gomez discloses that a temporal signal value is combined with other data stored on the device (e.g., a seed value and static payment card identifying number) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. EX1007, 8:11-51.

4. Claim 20

[20]: A method of claim 18, wherein user entered identification and authorizing information is recorded through the user interface of the electronic device from at least one of set including: a plurality of button-press actions; a swipe gesture received at a touch sensor of the electronic device; a key press sequence received at the touch sensor; a passcode sequence received at the buttons; a plurality of swipe gestures received at a touch sensor of the electronic device; a key press PIN sequence received at the touch sensor; a passcode sequence received at the touch sensor; an accelerometer sensor indicating a user motion of the electronic device; an action and sequence of motions of the electronic device as performed by a user; an action of the user to move the electronic device into a specific orientation; a biometric sensor confirming the electronic device is in a grip of the user; and a biometric sensor confirming the electronic device has remained in the possession of the user from activation to transaction.

212. Based on Gill, the mobile device records user-entered identification and authorization information through a user interface, including entry of a “username, password, PIN, biometric information, and/or one or more other credentials.” EX1034, 7:32-38; *see also id.*, 5:18-20 (“require at least the input of the proper PIN associated with the account”), 13:47-51, 14:9-30. Gill further discloses that “[t]he user input devices 540” of the mobile device can include a “touchscreen” and “keypad.” *Id.*, 12:33-44. A POSITA would have understood and/or it would have been obvious that the user’s entry of a PIN, passcode, or like credentials would include at least one of “a plurality of button-press actions,” “a key press sequence

received at the touch sensor,” “a passcode sequence received at the buttons,” “a key press PIN sequence received at the touch sensor,” or “a passcode sequence received at the touch sensor.” EX1036, FIG. 4C and [0042] (discussing one example of a user interface on a mobile phone adapted to receive a user’s entry of a PIN to authorize an ATM transaction).

5. Claim 21

[21]: A method of claim 18, wherein the identification and authorizing information is recorded responsive to the user inputting information using input methods provided by the ATM to record at least one of a PIN number; a passcode; a password; a biometric identification; and user known secrets.

213. Gill discloses, and the combination renders obvious, identification and authorization information recorded responsive to the user inputting information using input methods provided by the ATM to record a PIN number, a password, a biometric identification, and user known secrets. EX1034, 7:32-38 (“ATM 200 is configured (and/or the ATM application 244 is executable) to authenticate an ATM user based at least partially on an ATM debit card, smart card, token (e.g., USB token, etc.), username, password, PIN, biometric information, and/or one or more other credentials that the user presents to the ATM 200.”), 14:9-13 (“Block 715 represents the ATM 200 authenticating the customer. Authentication may be by any typical means as understood by those skilled in the art, but generally requires the

customer to enter a PIN associated with the account the customer wishes to authenticate himself to the ATM 200.”).

6. Claim 22

[22]: The method of claim 18, wherein the limited-use number dynamically generated in the device is based on cryptographically combining data selected from the group consisting of an ATM information, the locality of an ATM reader facility, information regarding the facility performing the transaction, bank information, a time of day, a date, a transaction amount, a count of past transactions, a sequence count, a historical record of transactions, a merchant account, a user's location, an online address, a device-internal secret, a device unique identifier, a payment authority key, a payment issuer authority secret, a method and direction of payment, deposit, transfer and receipt, a cryptocurrency server, a cryptocurrency type, a cryptocurrency private key, a cryptocurrency public key, a cryptocurrency address, a touch gesture, a biometrically sensed user information, a user's private information, a user key, a user email, password, passcode, a PIN, a user secret, and a user input.

214. Smith discloses, and the combination renders obvious, that the payment cryptogram (i.e., the limited-use number dynamically generated in the device) is generated using cryptographic techniques based on at least portions of the mobile cloud account data securely stored on the mobile device. EX1035, [0067] (“a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code, generated based on at least a portion of the mobile cloud account data stored in the secure element 210”). The mobile cloud account data comprises

device-internal secrets such as the ICC public key certificate and ICC public key certificate. *Id.*, [0086] (“The mobile cloud account data 802 may include at least the issuer public key certificate, the ICC public key certificate, and the MCA.”). In the combination, Gomez further teaches that the cryptogram can be generated based on a temporal signal including a date and a time of day, or a sequence count or count of past transactions. EX1007, 7:17-27 (“a temporal signal is generated which corresponds to the instance of attempted use”; “a temporal signal value may reflect the date/time of the attempted use”; “a temporal signal value may reflect the sequence value (or sequential number) of the attempted use”), 8:36-41, 10:58-11:6. As discussed in the overview of the Gill-Smith-Kay-Gomez combination (§ IX.C.4), it would have been obvious to combine the temporal signal with additional information such as the mobile cloud account data or other information like Gomez’s seed value, which includes device internal secrets, device unique identifiers, and/or a user secret. EX1007, 7:27-39 (“This seed value is unique for each payment card, and corresponds to the payment card identifying number. ... [I]n certain embodiments, the seed value may include certain non-random customer specific information, such as a unique customer key, either alone or in addition to a pseudo-random bit string.”).

7. Claim 23

[23]: The method of claim of 18, wherein the payment information comprises combining a plurality of static portions, and a plurality of dynamically generated limited-use portions, and wherein the static portion is a token account number with a limited-duration expiration date, to be used in place of issuer provided information.

215. The mobile device of the Gill-Smith-Kay-Gomez combination generates and transmits payment information that includes a mobile card account number (MCA) and a payment cryptogram as taught in Smith. *Supra* [18.h]-[18.i]. Further, and as described above, and the combination renders obvious, the Gill-Smith-Kay-Gomez combination discloses that the duration of the cryptogram would be limited by generating it based on both a temporal signal that changes with each transaction and secret(s) stored on the device such as a seed value (as taught in Gomez) or mobile cloud account data (as taught in Smith). *Supra* § IX.C.1.

216. In this context, the Gill-Smith-Kay-Gomez combination provides the additional features recited in [23]. For example, Smith discloses that the MCA is formed by combining a first set of digits that are different from the corresponding RCA and a second set of digits taken directly from the corresponding RCA. EX1035, [0095] (“In one embodiment the MCA may include at least a portion of the RCA. In a further embodiment, the portion of the RCA may include at least the last four digits of the RCA.”), [0091]. Both portions of the MCA are static, as the

corresponding digits from the RCA are fixed and the remaining digits likewise unchanged for the lifetime of the MCA. *Id.*, [0086]. The MCA is a token account number with a limited-duration expiration date for use in place of the RCA (i.e., issuer-provided information). *Id.* (“the generated MCA may include an expiration date”), [0034] (“The MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.”), [0040] (“The use of the MCA may enable the user of the mobile device 102 to more securely conduct a contactless payment transaction without using an RCA.”).

217. Moreover, Gomez teaches, and the combination renders obvious, that the cryptogram can be generated by combining a “date” and a “time” (i.e., a plurality of dynamically-generated limited use portions) to form a temporal signal used in calculating the cryptogram. EX1007, 7:17-24 (“At step 256 a temporal signal value is generated which corresponds to the instance of attempted use. In some embodiments such a temporal signal value may reflect the date/time of the attempted use. The date and time may be determined by a real-time clock device included within the payment card[] ...”), 7:41-48. As another example, Gomez describes techniques for encoding the cryptogram into a sequence of characters (e.g., 32 characters). *See generally id.*, 14:36-17:13. With this encoding, each character

represents a different portion of the message digest, and the characters (i.e., a plurality of dynamically generated limited-use portions) are combined to form the complete cryptogram. *Id.*, 15:43-51 (describing a radix-64 numbering system in which each character of the cryptogram represents 6 bits of the message digest), 15:61-65 (describing a radix-32 numbering system in which each character of the cryptogram represents 5 digits of the message digest). It would have been obvious to encode the cryptogram with higher-order characters rather than mere binary digits in order to convey more information in fewer characters, as taught by Gomez. EX1007, 14:37-63, 15:17-60. Fewer numbers of higher-order characters would thus be needed to achieve the same level of security from the cryptogram as a greater number of lower-order characters, thereby permitting more secure cryptograms to be transmitted from the mobile device in fewer numbers of characters (e.g., in a fixed-length field with a limited number of characters). *Id.*; *see also id.*, 15:57-58 (“Such a code could be useful in a NFC environment”).

8. Claim 24⁷

[24]: The method of claim of 18, wherein the amount of currency information can be a unit of value from at least one of a set of comprising: a cash amount, an amount of a debit account, an amount of credit, a maximum spending amount, a merchant account, a bank account amount, a unit of cryptocurrency, an online account funds, an payment issuer unit of funds, and a merchant account points.

218. As discussed with respect to [18.e], Kay discloses, and the combination renders obvious, a mobile device that receives user input information from a user interface indicating an “amount of currency” for a transaction. EX1036, [0043] (“In 340, the customer enters the amount of cash to withdraw and confirms the transaction. Figure 4D, for example, shows a mobile device 400 with a user interface that prompts the customer to ‘Enter Cash Amount’ 435 using a keypad 440 on a touchscreen of the mobile device 400 ...”).

XII. JURAT

219. In signing this Declaration, I understand 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 acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear remotely for

⁷ The additional features recited in this claim are not limiting as they do not define further limitations of the recited method; they are nonetheless obvious.

cross-examination within the United States during the time allotted for cross-examination.

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

Dated: September 1, 2025 By: 
Michael I. Shamos, Ph.D.