

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARDWARE INC.,

Patent Owner

Case No. IPR2025-001146
U.S. Patent No. 10,339,520

DECLARATION OF DR. CLIFFORD NEUMAN

I.	INTRODUCTION.....	14
A.	EDUCATIONAL BACKGROUND AND PROFESSIONAL EXPERIENCE	14
II.	MATERIALS CONSIDERED	17
III.	OVERVIEW AND LEGAL STANDARDS	18
A.	PERSON OF ORDINARY SKILL IN THE ART	19
B.	OBVIOUSNESS	19
C.	CLAIM CONSTRUCTION	24
D.	PRINTED SUBJECT MATTER.....	25
IV.	LEVEL OF A PERSON OF ORDINARY SKILL.....	25
V.	OVERVIEW OF THE '520 PATENT.....	26
A.	SUMMARY OF THE '520 PATENT.....	26
B.	FIELD OF ENDEAVOR.....	28
C.	PROBLEM PURPORTEDLY SOLVED BY THE INVENTORS OF THE '520 PATENT	29
D.	FILE HISTORY OF THE '520 PATENT	30
VI.	BACKGROUND OF TECHNOLOGY	31
A.	THE EVOLUTION OF PAYMENT CARDS	32
1.	<i>Magnetic Stripe Cards.....</i>	<i>32</i>
2.	<i>Smart/Chip Cards</i>	<i>35</i>
3.	<i>Europay, MasterCard, and Visa (EMV) Standard.....</i>	<i>36</i>
B.	CONTACTLESS PAYMENTS.....	36
1.	<i>Near Field Communications.....</i>	<i>36</i>
a)	Active Mode	38
b)	Passive Mode.....	40
2.	<i>Contactless EMV Payment Cards.....</i>	<i>41</i>
a)	Mobile Devices and Mobile Wallets	42
b)	Card Emulation Mode	45
3.	<i>Contactless ATMs</i>	<i>47</i>

C.	PAYMENT CREDENTIAL SECURITY FEATURES	52
1.	<i>Alternatives to a Payment Account Number (PAN).....</i>	52
2.	<i>Alternatives to Static Card Verification Values</i>	55
VII.	SUMMARY OF THE PRIOR ART REFERENCES	58
A.	GILL.....	58
1.	<i>Gill is Analogous Art.....</i>	61
B.	SMITH	62
1.	<i>Smith is Analogous</i>	64
C.	KAY	65
1.	<i>Kay is Analogous Art.....</i>	66
D.	GOMEZ.....	66
1.	<i>Gomez is Analogous Art</i>	70
VIII.	SUMMARY OF UNPATENTABILITY	71
IX.	OPINIONS REGARDING GROUND 1: CLAIMS 18-21 AND 24 ARE OBVIOUS OVER <i>GILL, SMITH, AND KAY</i>.....	71
A.	CLAIM 18	71
1.	<i>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:</i>	72
2.	<i>18(a): providing, by the electronic device, at least one of account information; identification; and authorization, for the ATM transaction; and, ...</i>	73
a)	Gill's Teachings	74
b)	Smith's Teachings	76
c)	Motivation to Combine	77
3.	<i>18(b): wherein the electronic device comprises a user interface comprising: displays; touch sensors; and buttons; and, ...</i>	85

4.	<i>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, ...</i>	<i>88</i>
	a) Gill's Teachings	88
	b) Smith's Teachings	89
5.	<i>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, ...</i>	<i>90</i>
	a) Gill's Teachings	90
	b) Kay's Teachings	92
	c) Motivation to Combine	94
6.	<i>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, ...</i>	<i>96</i>
	a) Gill's Teachings	96
	b) Kay's Teachings	98
	c) Motivation to Combine	99
7.	<i>18(f): wherein the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC; and, ...</i>	<i>101</i>
8.	<i>18(g): wherein the ATM is configured for performing the user selected account operation using the identification and authorizing information; and, ...</i>	<i>103</i>
9.	<i>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, ...</i>	<i>106</i>
10.	<i>18(i): wherein said static and dynamic information is combined to perform the user selected ATM operation.</i>	<i>109</i>

B.	CLAIM 19	111
1.	<i>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;</i>	<i>111</i>
	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.	111
C.	CLAIM 20	114
1.	<i>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.</i>	<i>114</i>

D.	CLAIM 21	116
1.	<i>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.....</i>	<i>116</i>
E.	CLAIM 24	116
1.	<i>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.....</i>	<i>116</i>
X.	OPINIONS REGARDING GROUND 2: CLAIMS 18-24 ARE OBVIOUS OVER GILL, SMITH, KAY, AND GOMEZ.....	118
A.	CLAIM 18	118
1.	<i>Gomez's Teachings.....</i>	<i>119</i>
2.	<i>Motivation to Combine</i>	<i>120</i>
B.	CLAIMS 19-21, 24	124
C.	CLAIM 22:	124
1.	<i>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,</i>	

	<i>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.</i>	<i>124</i>
D.	CLAIM 23:	126
1.	23. <i>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.....</i>	<i>126</i>
XI.	CONCLUSION.....	130

CLAIM LISTING

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:

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

18(b): wherein the electronic device comprises a user interface comprising: displays; touch sensors; and buttons; and,

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,

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,

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,

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

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

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,

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

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-specifcs; secrets; keys; a currency; currency amounts; cryptocurrency amount; transaction limits; transaction records; usage duration; and usage sequence counts.

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.

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.

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.

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.

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.

I, Dr. Clifford Neuman, declare the following:

I. INTRODUCTION

1. I have been retained by counsel for Petitioners as a technical expert in the above-captioned case. Specifically, I have been asked to render certain opinions regarding the IPR petition with respect to U.S. Patent No. 10,339,520 (the “’520 Patent”). I understand that the Challenged Claims are 18-24, and my opinions herein are limited to those claims.

A. Educational Background and Professional Experience

2. My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Appendix A. The following is a brief summary of my relevant qualifications and professional experience. I received a Ph. D. in Computer Science in 1992 and an M.S. in Computer Science in 1988 from the University of Washington, and an S.B. (Bachelor’s) in Computer Science and Engineering in 1985 from the Massachusetts Institute of Technology.

3. Since receiving my doctorate, I have devoted my career to the field of distributed computer systems development and research with a significant portion of my experience in the area of electronic commerce and internet payments. I have studied, taught, practiced, and researched in the field of computer science for over forty years.

4. I am currently an Associate Professor of Computer Science Practice in the Department of Computer Science at the University of Southern California (USC), where I have taught since 1992. I am also the Director of the Center for Computer Systems Security, an affiliated Scientist at USC's Information Sciences Institute, and I direct the Computer Security Curricula within the Data Science Program at USC. I teach and have taught numerous courses at USC, including advanced courses in computer science for upper-level undergraduates and graduate students, on topics such as distributed systems and computer and network security.

5. As part of my research at USC, I have worked in a number of areas, including research in distributed computer systems with emphasis on scalability and computer security, especially in the areas of authentication, authorization, policy, electronic commerce, and protection of cyber-physical systems and critical infrastructure such as the power grid. I have worked on the design and development of scalable information, security, and computing infrastructure for the Internet. I am also the principal designer of the Kerberos system, an encryption-based authentication system used among other things as the primary authentication method for most versions of Microsoft's Windows and for many other enterprise computer systems. I have also developed systems that used Kerberos as a base for more comprehensive computer security services supporting authorization, audit, and electronic payments.

6. In addition to my academic experience, I have many years of practical experience designing computer security systems. For example, from 1985-1986, I worked on Project Athena at MIT, to produce a campus-wide distributed computing environment. I also served as Chief Scientist at CyberSafe Corporation from 1992-2001. I have designed systems for network payment which build upon security infrastructure to provide a secure means to pay for services provided over the Internet. For example, I designed the NetCheque and NetCash systems, which are suitable for micropayments (payments on the order of pennies where the cost of clearing a credit card payment would be prohibitive). In 2000 and 2001, I was on the advisory board for NetResearch Inc, d/b/a BayBuilder, which was a company developing online auction platforms.

7. As part of my research on improving authentication and the security of electronic commerce in the late 1990s, I was involved with the integration of smart cards and PCMCIA cryptographic processors into security services used by end-point computing devices such as personal computers. Also in the late 1990's I worked with the Financial Services Technology Consortium on their electronic check project.

8. I have authored or co-authored over 50 academic publications in the fields of computer science and engineering. In addition, I have been a referee or editor for the following academic journals: ACM Transaction on Information and

Systems Security and International Journal of Electronic Commerce. My curriculum vitae includes a list of publications on which I am a named author. I am also a member of the IEEE, Association for Computer Machinery (ACM), and the Internet Society (ISOC), among others. I have also served as program and/or general chair of the following conferences: The Internet Society Symposium on Network and Distributed System Security and the ACM Conference on Computer and Communications Security.

II. MATERIALS CONSIDERED

9. I have relied upon my education, knowledge, and experience with payment systems, including mobile payment systems, as well as the other materials discussed in this declaration in forming my opinions.

10. In developing my opinions, I have considered the following materials:

Exhibit	Description
1001	U.S. Patent No. 10,339,520 (the “’520 Patent”)
1002	File History of the ’520 Patent (“the ’520 File History”)
1004	U.S. Patent No. 9,098,846 (“Gill”)
1005	U.S. Pub. No. 2013/0232083 (“Smith”)
1006	U.S. Pub. No. 2013/0124410 (“Kay”)
1007	U.S. Patent No. 9,600,808 (“Gomez”)

11. I have considered these materials from the viewpoint of a POSITA as of the priority date of the ’520 Patent. For the purposes of this declaration, I have been asked to assume that the earliest priority date of the ’520 Patent is March 15,

2013. I note that my opinions provided in this Declaration are made from the perspective of a POSITA as of this priority date of the '520 Patent unless expressly stated otherwise. To the extent that I use any verb tense in this Declaration that is present tense (e.g., “a POSITA would understand” instead of “a POSITA would have understood”), such verb tense should be understood to be my opinion as of the '520 Patent's priority date (again, unless expressly stated otherwise). I merely use the present verb tense for ease of reading.

III. OVERVIEW AND LEGAL STANDARDS

12. In formulating my opinions, I have been instructed to apply certain legal standards. I am not a lawyer. I do not offer any testimony regarding what the law is. Instead, the following sections summarize the law as I have been instructed to apply it in formulating and rendering my opinions found later in this declaration. I understand that, in an *inter partes* review (“IPR”) proceeding, patent claims may be deemed unpatentable if it is shown that they are anticipated or rendered obvious in view of the prior art. I understand that prior art in an IPR review is limited to patents or printed publications that predate the priority date of the patent at issue. I understand that questions of claim clarity (definiteness) and enablement cannot be considered as a ground for considering the patentability of a claim in these proceedings.

A. Person of Ordinary Skill in the Art

13. I understand that the '520 Patent, the record of the proceedings at the Patent Office (which I understand is called the "File History" or "Prosecution History"), and the teachings of the prior art are evaluated from the perspective of a person of ordinary skill in the art ("POSITA"). I understand that the factors considered in determining the ordinary level of skill in the art may include: (i) the levels of education of the inventor; (ii) the types of problems encountered in the art; (iii) prior art solutions to those problems; (iv) the rapidity with which innovations are made; (v) the sophistication of the technology; and (vi) the educational level of persons working in the field.

14. I understand that a person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors above. The hypothetical person is presumed to have the same level of skill as the typical practitioner of the art and is presumed to have knowledge of all prior art in the relevant field. I understand that the inventor's actual knowledge or lack of knowledge of prior art reference is irrelevant to the obviousness determination.

B. Obviousness

15. I understand that a claim may be invalid under 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been "obvious" to a

POSITA in view of a single or combination of prior art references at the time the claimed invention was made. I further understand that a POSITA is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent-in-suit and all analogous prior art. I understand that obviousness in an IPR review proceeding is evaluated using a preponderance of the evidence standard, which means that the claims must be more likely obvious than nonobvious.

16. I also understand that an obviousness determination includes the consideration of various factors including: (1) the scope and content of the prior art, (2) the differences between the prior art and the claim at issue, and (3) the level of ordinary skill in the pertinent art. I understand that secondary considerations of non-obviousness such as commercial success, long-felt but unresolved needs, failure of others, and so forth may be assessed as well. I have been informed that an obviousness analysis must focus on the state of the art at the time of the invention to avoid impermissibly using hindsight to invalidate a patent.

17. In considering whether certain prior art renders a particular patent claim obvious, I have been informed that I can consider the scope and content of the prior art, including the fact that a POSITA would regularly look to the disclosures in patents, trade publications, journal articles, conference papers, industry standards, product literature and documentation, texts describing competitive technologies,

requests for comment published by standard setting organizations, and materials from industry conferences, as examples.

18. I have been informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be “analogous art” to the claimed invention. A reference is analogous art if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). For a reference to be “reasonably pertinent” to the problem, it must logically have commended itself to an inventor’s attention in considering the problem. In determining whether a reference is reasonably pertinent, one should consider the problem faced by the inventor, as reflected either explicitly or implicitly, in the specification. I believe that the documents I considered in forming my opinions in this IPR are well within the range of documents a POSITA would have consulted to address the type of problems described in the Challenged Claims.

19. I have been informed that to establish that a claimed invention was obvious based on a combination of prior art elements, an articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I have been informed that the prior art, either as a single reference or a combination of multiple items of prior art, renders a patent claim obvious when there was an

apparent reason for a POSITA, at the time of the invention, to combine or modify the prior art. Rationales for combining or modifying the prior art include, but are not limited to, any of the following: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

20. I have also been informed that where there is a motivation to combine, claims may be rejected as obvious provided a POSITA would have had a reasonable expectation of success regarding the proposed combination. I have also been informed that common sense may be considered. Common sense teaches that familiar items may have obvious uses beyond their primary purposes. I have been informed that if the combination was obvious to try (regardless of whether it was

actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than non-obvious innovation.

21. I have been informed that the existence of an explicit teaching, suggestion, or motivation to combine known elements of the prior art is a sufficient, but not a necessary, condition to a finding of obviousness. In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose described in the patent-in-suit controls. I have been further informed that the obviousness analysis may consider the effects of demands known to the technological community or present in the marketplace and the background knowledge possessed by a POSITA. These issues may be considered to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent.

22. I have been informed that it is improper to combine references where the references teach away from their combination. A reference may be said to teach away when a POSITA, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the patent applicant. I have also been informed that a reference does not teach away if it merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into the invention claimed.

23. I am informed that even if a case of obviousness is established, the final determination of obviousness must also consider “secondary considerations” if presented. Secondary considerations include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unsatisfied need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) lack of independent simultaneous invention within a comparatively short space of time; and (h) teaching away from the invention in the prior art.

24. I have been further informed that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be based on prior art features. The establishment of a nexus is a question of fact. While I understand that Patent Owner here has not offered any secondary considerations at this time, I will supplement my opinions should Patent Owner raise secondary considerations during the course of this proceeding.

C. Claim Construction

25. I understand that the claim terms in an IPR proceeding are construed according to their plain and ordinary meaning as understood in light of the claim language, the patent’s description, and the prosecution history viewed from the

perspective of a POSITA. I further understand that where a patent defines claim language, the definition of the patent controls, even if there are other definitions that might be understood by those working in the art. I have applied these principles when interpreting the Challenged Claims and in rendering the opinions provided in this declaration.

26. I understand that Petitioner does not assert that any claim terms require express construction for purposes of this IPR.

D. Printed Subject Matter

27. I have been informed and understand that limitations that are directed to the presence or absence of printed matter are not entitled to patentable weight if the printed matter has no functional or structural relationship to the associated physical substrate.

IV. LEVEL OF A PERSON OF ORDINARY SKILL

28. Based on my review and analysis of the '520 Patent, the cited prior art, and the ordinary skill factors described in this section, a POSITA in the field of the '520 Patent at the time of the earliest possible priority date (March 15, 2013) would have been knowledgeable regarding the field of payment processing and digital authentication. In my experience in this field, most workers of ordinary skill in the art as of the earliest possible priority date of March 15, 2013 would have had at least a bachelor's degree in computer science, computer engineering, electrical

engineering or the equivalent, and one or two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technology such as NFC. Additional industry experience or technical training may offset less formal education, while advanced degrees or additional formal education may offset lesser levels of industry experience. When I refer to the understanding of a POSITA, I am referring to the understanding of such a person as of March 15, 2013.

29. As of March 15, 2013, I had more than ordinary skill in the art. I am, however, familiar with the skills and knowledge possessed by those I would have considered to be of ordinary skill in the art as of that date.

30. My opinions provided in this declaration would not change in view of minor modifications to this level of ordinary skill.

V. OVERVIEW OF THE '520 PATENT

A. Summary of the '520 Patent

31. The '520 Patent generally describes emulating a standard credit card with a device “capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe ... for the purpose of emulating a standard credit card” for use in financial transactions. *'520 Patent (EX1001)*, Abstract; 2:14-24. The '520 Patent also describes “allow[ing] user control of said device for the purpose of authorizing or controlling use of said device in the application of credit,

debit and cash transactions.” *'520 Patent (EX1001)*, 2:20-24. The invention also describes “generating a limited-duration credit card number when performing a transaction.” *'520 Patent (EX1001)*, 2:24-29. This limited-duration number “is limited in scope to a predetermined number of authorized transactions.” *'520 Patent (EX1001)*, 2:26-29. The electronic device is capable of using near field communications (“NFC”) to conduct a transaction using the limited-duration number. *'520 Patent (EX1001)*, 2:32-62.

32. “The credit card device comprises a realtime clock that is able to produce a cryptographically protected timestamp for each interaction.” *'520 Patent (EX1001)*, 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.” *'520 Patent (EX1001)*, 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.” *'520 Patent (EX1001)*, 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.” *'520*

Patent (EX1001), 10:18-23. In some cases, the disclosed credit card device is used to conduct transactions with an automated teller machine (ATM). *'520 Patent (EX1001)*, 11:16-26, 12:44-53, 14:59-60.

B. Field of Endeavor

33. I have been informed that the field of endeavor of the claimed invention can be determined by reference to explanations of the invention's subject matter in the patent application, including the embodiments, function, and structure of the claimed invention.

34. The '520 Patent expressly defines the field of invention, and notes that embodiments "generally relate to electronic or smart credit card devices and, more specifically, to more secure, smart credit card devices." *'520 Patent (EX1001)*, 1:25-29. Given this express definition provided by the '520 Patent itself, and its inventor, it is my opinion that a POSITA would understand the field of endeavor for the '520 Patent to include at least electronic or smart payment devices.

35. The '520 Patent criticizes existing systems due to being "susceptible to theft and/or compromise." *'520 Patent (EX1001)*, 1:63-2:4. Therefore, in my opinion, a POSITA would understand that the problem the inventor of the '520 Patent was attempting to solve the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

C. Problem Purportedly Solved by the Inventors of the '520 Patent

36. I have been informed that a prior art reference is “reasonably pertinent” if a POSITA would have consulted it and applied its teachings when faced with the problem that the inventor was trying to solve. As such, I have been asked to analyze the '520 Patent and determine the problem that the inventors were trying to solve.

37. The '520 Patent notes that a concern with “credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise” and therefore they “have security limitations.” *'520 Patent (EX1001)*, 1:63-67. The '520 Patent also noted that “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.” *'520 Patent (EX1001)*, 1:67-2:4. To solve these problems, the “Summary of the Invention” describes “multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe” for the “purpose of emulating a standard credit card.” *'520 Patent (EX1001)*, 2:14-18. The “Summary of the Invention” further describes a method of performing a transaction that includes “generating a limited duration credit card number.” *'520 Patent (EX1001)*, 2:24-27. Thus, a POSITA would understand that the '520 Patent is directed to

solving the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

D. File History of the '520 Patent

38. I have reviewed the prosecution history for the '520 Patent. Notably, there were no substantive rejections based on prior art at any point during the review of the application that issued as the '520 Patent. *See generally '520 File History (EX1002)*. The only rejection that was made was based on statutory double patenting. *'520 File History (EX1002)*, 69. The applicant responded to the rejection by amending independent claim 1 and adding new claims 10-24. *'520 File History (EX1002)*, 107-121. No further rejections were issued and a Notice of Allowance then issued. In the Notice of Allowance, the examiner noted that available prior art reference, Sebastian et al. (US 2013/0297509) taught a mobile payment using a dynamic code. *'520 File History (EX1002)*, Notice of Allowability. However, the Examiner noted none of the prior art teaches the limitations required by the claims of the application that issued as the '520 Patent. *'520 File History (EX1002)*, Notice of Allowability. A corrected Notice of Allowance was later filed indicating an Examiner's Amendment provided an amendment to claim 2 and 3 indicating the detected proximity was "between the electronic device and a second electronic device." *'520 File History (EX1002)*, Corrected Notice of Allowance. Other minor amendments were made to claims 4 and 8 for clarity. *'520 File History (EX1002)*.

The Examiner's reasons for allowance remained the same as the original reason for allowance. Nothing in the file history indicates the art set forth in the petition was located or analyzed by the Examiner.

VI. BACKGROUND OF TECHNOLOGY

39. I was asked to briefly summarize the background of the prior art from the standpoint of a person having ordinary skill in the art prior to March 15, 2013. As explained below, a POSITA would have understood that the payment system features described in the '520 Patent (including, for example, limited-use payment information, transaction sequence counts, device account numbers, and secrets) had long been a feature of payment systems that were developed by leading payment processors (including Mastercard and Visa) years before the earliest filing date of the '520 Patent.

40. As described below, all of the hardware components and functionalities encompassed by the Challenged Claims were well-known to a POSITA in the industry prior to the invention of the '520 patent.

41. The evolution of electronic payment systems can be traced back several decades, marked by key technological milestones that have transformed how financial transactions are processed. Early developments in this field centered on introducing magnetic stripe technology for payment card transactions. Before the late 1960s, credit card transactions primarily consisted of "a tiny printing press to

record raised letters and numbers from a card onto a form made of pressure-sensitive paper with carbon copies.” *IBM (EX1020)*, 1. However, this process was “insecure, slow, and prone to errors” therefore a need for magnetic stripe cards arose. *IBM (EX1020)*, 1.

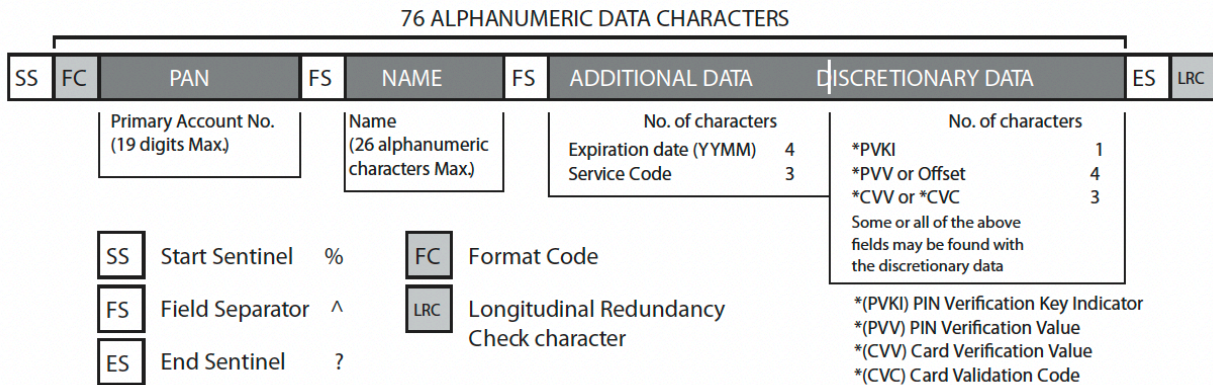
A. The Evolution of Payment Cards

1. Magnetic Stripe Cards

42. In the 1960s, “[t]he process of attaching a magnetic stripe to a plastic card was invented by IBM [.]” *Coskun (EX1021)*, 59. “A magnetic stripe card is one that contains a digital storage space where the data are loaded during the manufacturing phase. The stripe is made up of tiny magnetic particles in a resin. It is traditionally a read-only item. It is read by physical contact by swiping the card past a device with a magnetic reading head.” *Coskun (EX1021)*, 6.

43. Data encoded on the back of the magnetic stripe is called track data such as what is defined in ISO/IEC 7813, 7810, and 7811. *MagTek (EX1022)*, 1. For example, track 1 data includes the following:

Card Data Format - Track 1

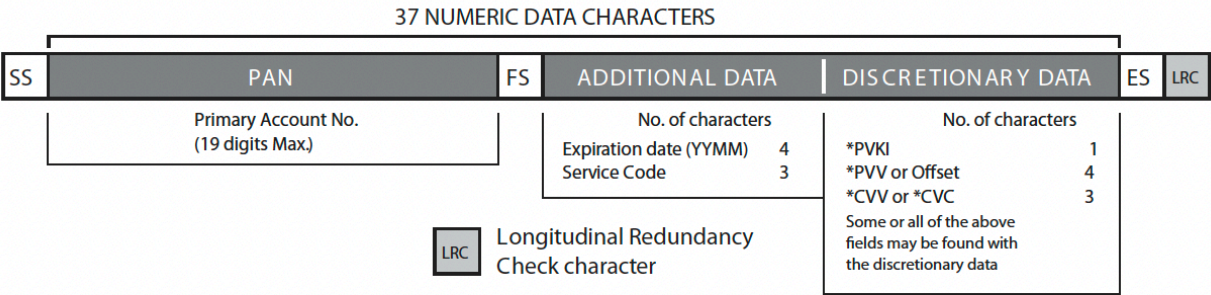


MagTek (EX1022), 1. On a card's track:

“there is a Discretionary Data (DD) segment that allows for the issuer to include some relevant information to use in the transaction authorization process. The typical DD segment includes the static CVV (VISA) or CVC (MASTERCARD) values, which are allotted three characters. Replacing the three character CVV or CVC data with a three digit dynamic code (dCVV in Visa, Inc. terms, or CVC3 in MasterCard, Inc. terms), including the dCVV of CVC3 indicator character (e.g., a status flag indicating that dynamic data is present), and including a four character Application Transaction Counter value allows the card issuer to use a set of data unique to each transaction to authorize a transaction.”

Bona (EX1009), [0102]. Track 2 data includes the following data:

Card Data Format - Track 2



Magtek (EX1022), 1.

44. The mag stripe “approach that IBM had helped develop was adopted as a US standard in 1969 and as an international standard two years later, enabling mag stripe cards to be used anywhere in the world.” *IBM (EX1020), 1*. The global standardization of magnetic stripe cards paved the way for global adoption.

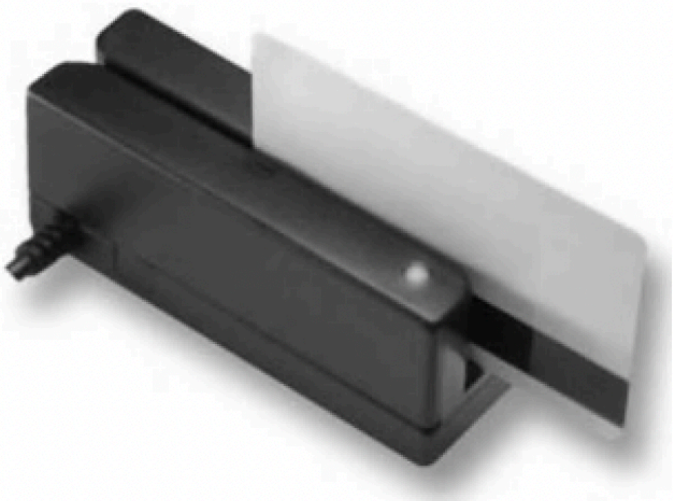


Figure 2.15 Magnetic stripe card.

Coskun (EX1021), Figure 2.15.

45. “In recent years, chip-enabled cards that encrypt cardholder data have begun to replace mag stripe cards, which carry static data directly in the magnetic stripe. However, demand for magnetic stripe cards remains strong because of their low cost, reliability and the huge, global installed base of card readers. And even though the job performed by magnetic stripes can now be done with chip cards and mobile phones, the global financial and transaction systems that thrive today are a legacy of the unassuming magnetic stripe.” *IBM (EX1020)*, 2.

2. *Smart/Chip Cards*

46. Smart cards were well known in the art all the way back to the “1970s.” *Coskun (EX1021)*, 60. “The first mass use of the cards was for telephone payments in the 1980s. In the meantime, microprocessor smart cards were developed and microchips were integrated into debit cards in the 1990s. Smart card based electronic purse systems which store values on a card and do not need network connectivity, began to be used in Europe in the mid 1990s.” *Coskun (EX1021)*, 60.

47. One major improvement “in smart card technology occurred in the 1990s; smart card based SIMs were introduced and started to be used in GSM based mobile phone environments in Europe. The use of smart cards increased with the ubiquity of mobile phones in Europe. In 1993, the international payment brands Europay, MasterCard, and Visa (EMV) collaborated to develop new specifications

for smart cards in order to use them in payments both as a debit and a credit card.”
Coskun (EX1021), 60.

3. *Europay, MasterCard, and Visa (EMV) Standard*

48. The EMV standard established a global framework for secure, chip-based payment card transactions. It introduced dynamic data generation, such as cryptograms to prevent replay attacks and authenticate transactions securely. *EMV (EX1023)*, 71-74 (“generation of the combined dynamic signature and Application Cryptogram”); 74-77 (“Dynamic Signature Verification”); 87-91 “generation of the Application Cryptograms (TC, ARQC, or AAC) generated by the ICC and the Authorisation Response Cryptogram (ARPC) generated by the issuer and verified by the ICC.”) The EMV standard defined clear steps in the transaction process, including cardholder verification (e.g., PIN or signature). *See EMV (EX1023)*, 81-86. The EMV standard laid the foundation for modern secure payments, including contactless and mobile EMV solutions.

B. Contactless Payments

1. *Near Field Communications*

49. Near Field Communication (NFC) “enables communication between an NFC enabled mobile phone at one end, and another NFC-enabled mobile phone, an NFC reader, or an NFC tag at the other end.” *Coskun (EX1021)*, 1. In terms of

distance, “NFC is restricted to within very close proximity.” *Coskun (EX1021)*, 1. This proximity is often “within 4 cm[.]” *Coskun (EX1021)*, 32.

50. Around 2006-2007, several companies began testing contactless NFC payments. For example, in April 2006, Visa conducted “the world’s first mobile Visa payWave payment pilot” involving about “2000 merchants and 200 participants.” *Coskun (EX1021)*, 341-342. As another example, HSBC partnered with MasterCard and “tested the use of NFC enabled mobile handsets in payment.” *Coskun (EX1021)*,. This “payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36000 merchants accepted the MasterCard PayPass payment option at that time.” *Coskun (EX1021)*, 342.

51. NFC has been used to facilitate contactless transactions in payment cards and mobile devices, enabling consumers to make payments simply by tapping their cards. *Smart (EX1026)*, 7. NFC “technology is defined by the NFC Forum founded by Nokia, Philips, and Sony which allow communication based on RFID technology and ISO/IEC 14443 infrastructures.” *Coskun (EX1021)*, 71.

52. For communication “between two NFC interfaces, the individual NFC interface can take on different functions, i.e. that of an NFC initiator (master device) or an NFC target (slave device). Communication is always started by the NFC initiator. In addition, NFC communication distinguishes between two different operational modes, the active and the passive mode.” *Finkenzeller (EX1024)*, 57.

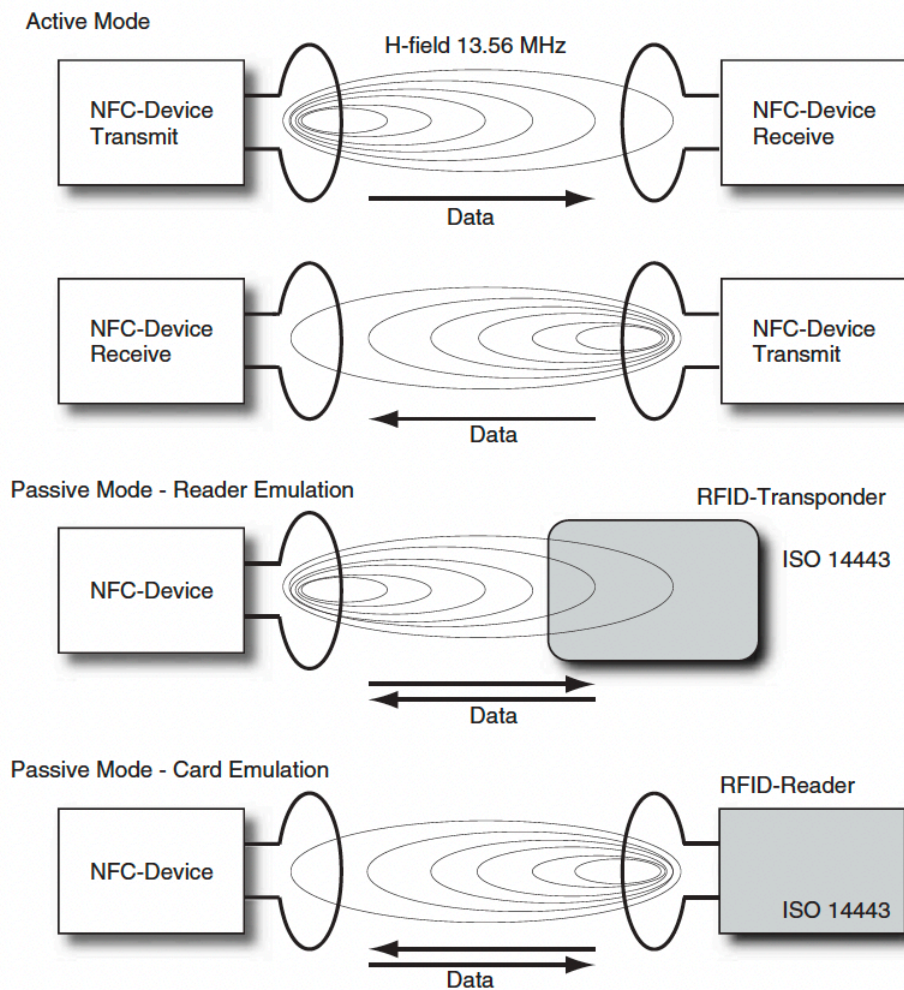


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzeller (EX1024), 58.

a) Active Mode

53. An NFC device, for example a mobile phone or payment card, can send information via NFC to another NFC interface. For example, “to transmit data between two NFC interfaces in active mode, at first one of the NFC interfaces activates its transmitter and thus works as the NFC initiator. The high-frequency

current that flows in the antenna induces an alternating magnetic field H which spreads around the antenna loop. Part of the induced magnetic field moves through the antenna loop of the other NFC interface which is located close by. Then a voltage U is induced in the antenna loop and can be detected by the receiver of the other NFC interface. If the NFC interface receives signals and the corresponding commands of an NFC initiator, this NFC interface automatically adopts the roll of an NFC target.” *Finkenzeller (EX1024)*, 57.

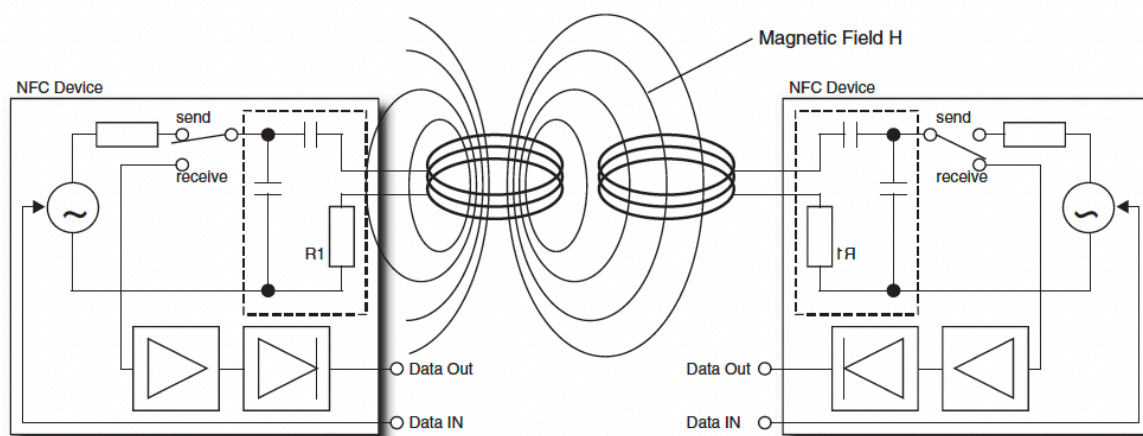


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (EX1024), 58.

54. A mobile device or card is also able to receive an NFC request. For example, “[t]he transmission direction is reversed in order to send data from the NFC target to the NFC initiator. This means that the NFC target activates the transmitter and the NFC initiator switches to receiving mode. Both NFC interfaces

alternately induce magnetic fields where data is transmitted from transmitter to receiver only.” *Finkenzeller (EX1024)*, 59.

b) Passive Mode

55. In passive mode “the NFC initiator induces a magnetic alternating field for transmitting data to the NFC target. The field’s amplitude is modulated in line with the pulse of the data to be transmitted (ASK modulation). However, after having transmitted a data block, the field is not interrupted, but continues to be emitted in an unmodulated way. The NFC target now is able to transmit data to the NFC initiator by generating a *load modulation*. The load modulation method is also known from RFID systems.” *Finkenzeller (EX1024)*, 59.

56. The NFC interface “that is the target is also able to establish, in addition to other NFC interfaces, the communication to compatible passive transponders (e.g. according to ISO/IEC 14443) that the NFC target supplies with power and that, via load modulation, can transmit data to the NFC interface. This option enables electronic devices equipped with NFC interfaces, such as NFC mobile phones, to read and write on different transponders such as smart labels or e-tickets. As the NFC interface in this case behaves similar to an RFID reader, this option is also called ‘reader mode’ or ‘*reader-emulation mode*’.” *Finkenzeller (EX1024)*, 59.

57. If an NFC interface “is located close to a compatible RFID reader (e.g. according to ISO/IEC 14443), the NFC reader is also able to communicate with a reader. Here, the NFC interface adopts the roll of an NFC target and can transmit data to the reader using load modulation. This option enables RFID readers to exchange data with an electronic device with NFC interface, such as NFC mobile phones. From the reader’s perspective, the electronic device behaves like a contactless smart card; this option is also called ‘card mode’ or ‘*card-emulation mode*’.” *Finkenzeller (EX1024)*, 59.

2. Contactless EMV Payment Cards

58. “From a contactless smart card technology perspective, the major progress was the agreement of Visa and MasterCard in 2004–2006 to implement contactless payment and ticketing applications such as mass transit and highway tolls in the USA. With the introduction of contactless smart cards such as the MIFARE proximity smart card by Philips, contactless smart card applications started to have a considerable market share in Europe and the US.” *Coskun (EX1021)*, 60. As an example, in 2006, Mastercard “worked with the Ohio Turnpike Commission to bring a consumer trail of *PayPass* payments” using “payment cards for self-service toll transactions.” *PayPass (EX1025)*, 1.

59. As of 2012, the typical contactless payment card working in the US were not EMV-compliant but instead utilized a NFC-enabled chip that transmitted

the magnetic stripe data (MSD) included on the associated payment card along with a dynamic value or cryptogram to facilitate transactions. *Smart (EX1026)*, 6.

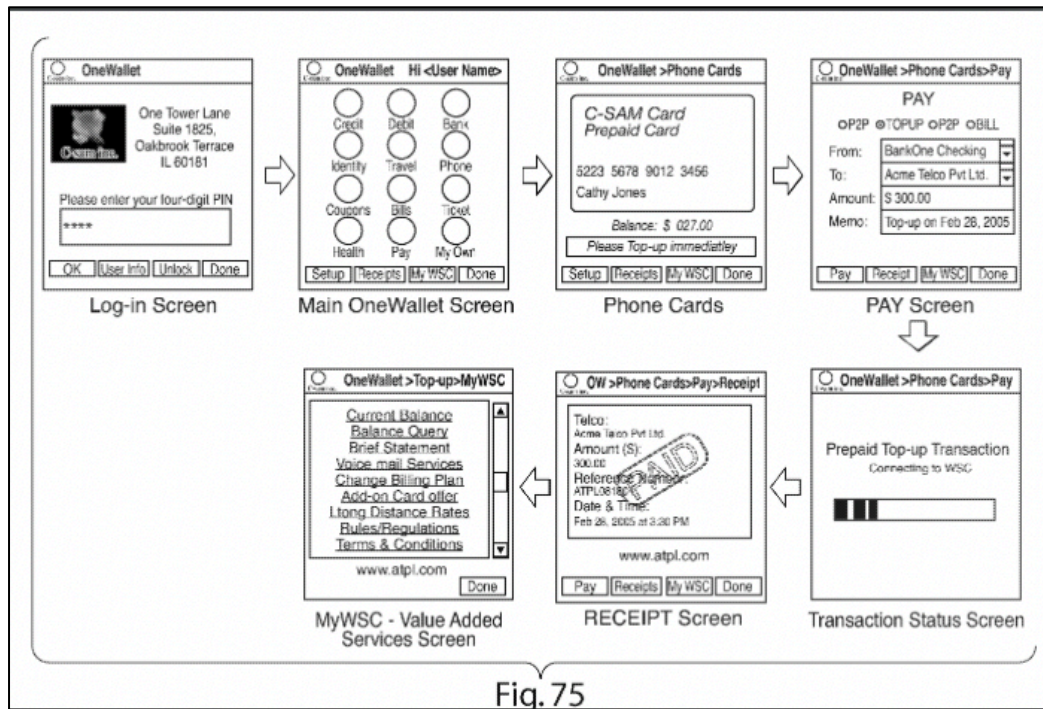
a) Mobile Devices and Mobile Wallets

60. Mobile devices performing contactless payments were well known before the '520 Patent.

61. Around 2006-2008, several companies began testing mobile contactless NFC payments. As an example, HSBC partnered with MasterCard to test “the use of NFC enabled mobile handsets in payment.” *Coskun (EX1021)*, 342. This “payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36000 merchants accepted the MasterCard PayPass payment option at that time.” *Coskun (EX1021)*, 342. In 2008, the ING Bank also tested the “viability of NFC technology in mobile payment systems for low value purchases in Romania” using “MasterCard (PayPass).” *Coskun (EX1021)*, 344.

62. A mobile phone can perform these contactless payments via the use of a mobile wallet. A mobile or electronic wallet is similar to “a person’s leather, physical wallet[.]” *Pitroda (EX1027)*, [0025]. An “electronic wallet contains one or more identification cards, credit cards, or the like. The electronic wallet is an electronic collection of one or more of these types of physical materials that can be

reviewed, viewed and used electronically to achieve similar results to the physical analogs.” *Pitroda (EX1027)*, [0025].



Pitroda (EX1027), Fig. 75. A user can “view and manage mobile payment cards and other applications...through the mobile wallet graphical user interface.” *Smart (EX1026)*, 11.

63. A number of trials relating to mobile wallets were run prior to the '520 Patent filing. For example, in 2007, a Q2 Wallet trial was run. The Q2 Wallet “eliminates the need for users to carry Oyster smart cards in their wallets. Users can pay for their travel expenses through the Oyster application by simply touching their mobile phones to the Oyster NFC readers at London underground tube stations, on buses, and on trams.” *Coskun (EX1021)*, 35. See also *Coskun*, 346. Nokia 6131, one

of the first NFC enabled phones, was the pilot test phone for the Q2 Wallet. *Coskun (EX1021)*, 346. (“About 500 O2 mobile network subscribers participated in the pilot and they were equipped with Nokia 6131 NFC enabled mobile phones.”)



Figure 9.8 O2 Wallet [1]. Photographed by Juha Sarkkinen, The City of Oulu, Smart Touch Project.

Coskun (EX1021), 347.

64. As another example, “Yapi Kredi Bank and the MNO Turkcell collaborated in the NFC enabled mobile-wallet service. The service launched commercially in 2011 [7].” Turkcell’s mobile wallet software is preloaded and “supports more than one bank-issued application.” *Coskun (EX1021)*, 345.

65. By 2012 the use of mobile phones with mobile wallets was well known. For example, MasterCard PayPass Wallet was released. *PayPass (EX1025)*, 1. (“integrate PayPass Wallet into its mobile application.”). MasterCard also released

a list of 42 “Approved Mobile Devices”—including phones from Google, Intel, LG, Asus, HTC, Nokia, BlackBerry, Samsung, Zony, and ZTE—all of which supported at least one mobile payment wallet. *MasterCard Mobile Partner (EX1028)*, 1.

b) Card Emulation Mode

66. A mobile phone can perform transactions via the mobile wallet using card-emulation mode. *Finkenzeller (EX1024)*, 59 (“the electronic device behaves like a contactless smart card; this option is also called ‘card mode’ or ‘*card-emulation mode*’.”); *see also Coskun (EX1021)*, 78 (“card emulation mode provides smart card capability for mobile phones.”)

67. In “card emulation mode, the RF interface is based on the ISO/IEC 14443 (Type A, Type B) standard and FeliCa.” *Coskun (EX1021)*, 96. “Either an NFC enabled mobile phone emulates an ISO 14443 smart card or a smart card chip integrated in a mobile phone is connected to the antenna of the NFC module.” *Coskun (EX1021)*, 111. A NFC application needs a Graphical User Interface (GUI) and Secure Element (SE) application. *Coskun (EX1021)*, 152. (“GUI (Graphical User Interface) application which must be present for all operating mode applications and provides both a GUI for the user and the capability to read NFC components...Secure Element (SE) application which is needed in order to provide a secure and trusted environment for applications”). The SE may be within the mobile phone or a remote-SE.

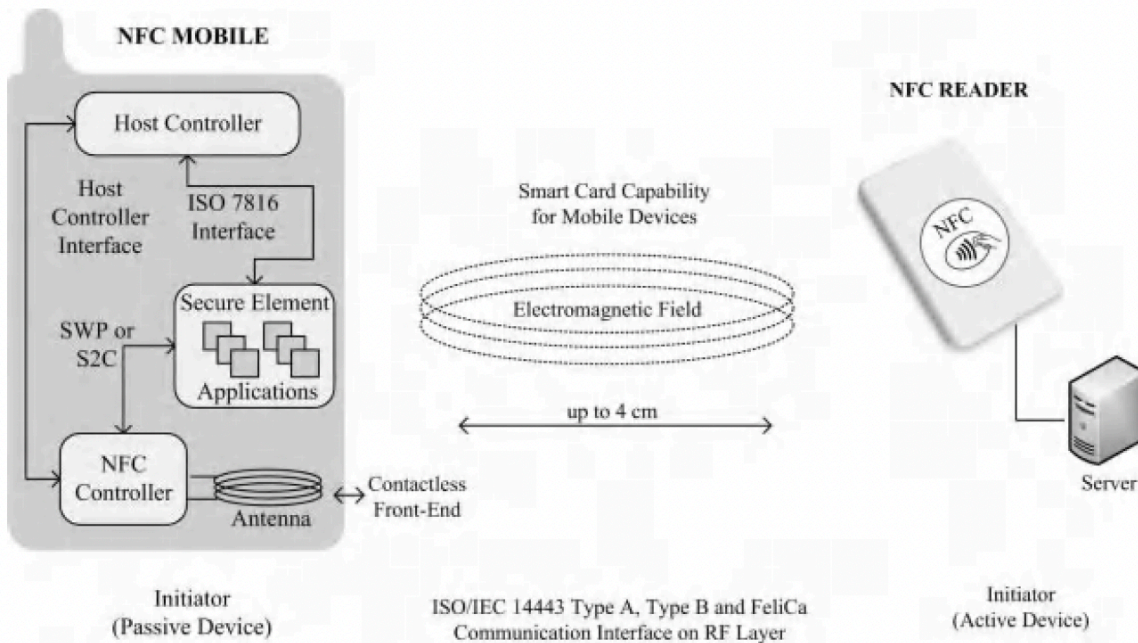


Figure 3.32 Communication architecture of card emulation operating mode.

Coskun (EX1021), Figure 3.32. It is worth noting that the above phone includes a secure element.

68. In the instance where a phone does not include a secure element, the mobile phone still needs a way to provide a secure and trusted environment for applications. Often, the mobile phone will have a remote-SE located outside of the mobile phone's hardware. As an example, "the NFC mobile device has the ability to use a SE for the transaction that is not physically located in the mobile device. This may be done by creating a data connection to a remote SE for which is used for the payment transaction. In step 757, while the phone is being placed into card emulation mode, the connection to the remote SE that will be used for emulation is attempting

to connect. As illustrated in step 758 there is a chance that the connection is already open in which case the flow in FIG. 14 will simply allow the ISO/IEC 7816-4 APDU data to pass directly through the connection to the remote SE and back 763 successfully completing the transaction 764. There is also a chance that the connection to the remote SE does not exist and needs to be created, as described subsequently in step 762.” *Yeager (EX1029)*, [0089].

3. *Contactless ATMs*

69. Smart devices for use with contactless ATMs were well known before the ’520 Patent.

70. In 1988, the National Institute of Standards and Technology issued NIST Special Publication 500-157, entitled “Smart Card Technology: New Methods for Access Control” (“*Smart Card Tech.*”) (EX1035). 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.

Smart Card Tech. (EX1035), 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.

Smart Card Tech. (EX1035), 3.

71. Fig. 5 of *Smart Card Tech.* illustrates the difference between contact-type and contactless smart cards:

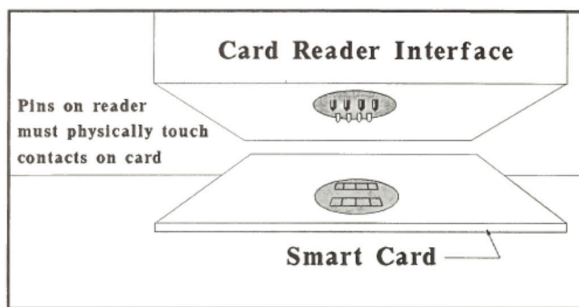


Figure 4. Contact-Type Smart Card Interface

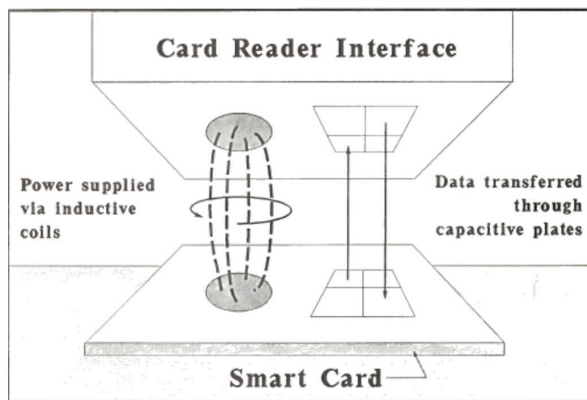
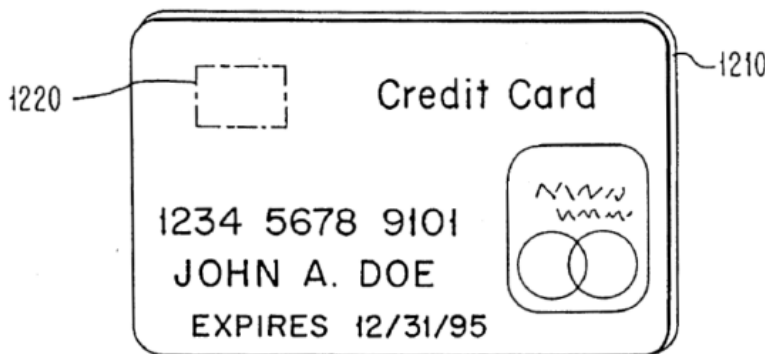


Figure 5. Non-Contact-Type Smart Card Interface

72. On September 9, 1994, Moskowitz et al., assignors to IBM, filed an application that issued as U.S. Patent 5,528,222 on June 18, 1996, entitled “Radio Frequency Circuit and Memory in Thin Flexible Package” (EX1036). It discloses a

Radio Frequency Identification (RFID) tag that could be used with an ATM or credit card:



Moskowitz (EX10036), Fig. 12; 7:20-24 (“FIG. 12 shows ISO standard credit card 1210 containing an RF tag 1220. The credit card may serve as an ATM card ...or any credit or debit card.”).

73. 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. (*EX1037*). 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.

Wenninger (EX1037), 2.

74. 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.

Wenninger (EX1037), 1.

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

76. 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” (EX1038). It discloses a card reader that could read all three of magnetic stripe cards, contact smart cards and contactless smart cards, specifically to 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).

Kenneth (EX1038), 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.

Kenneth (EX1038), 1:18-25.

77. Additionally, 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 No. 7,004,385 on February 28, 2006, entitled "Currency Dispensing ATM with RFID Card Reader" (EX1039).

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.

Douglass (EX1039), 2:31-42.

78. Additional examples of contactless transactions between a mobile device and an ATM can be found in U.S. Pub. No. 2007/0265984 (Sanantha)

(EX1040) and U.S. Pub. No. 2012/0197691 (Grigg) (EX1041). *Sanantha*, [0035]-[0036]; *Grigg*, [0108] (“The external apparatus may generally be a contactless transaction terminal such as a contactless payment terminal, an automated teller machine (ATM), or the like.”), Figs. 1, 7.

79. Thus, a POSITA was well-aware of the use of mobile devices in contactless ATM transactions prior to the ’520 Patent.

C. Payment Credential Security Features

80. With the increase in contactless payment transactions came additional opportunities for malicious individuals to gain unauthorized access to a user’s payment information. Below, I describe an exemplary group of prior art attempts to prevent fraud and protect sensitive information.

1. Alternatives to a Payment Account Number (PAN)

81. Early payment cards (e.g., magnetic stripe cards) lacked significant security protocols to protect customer’s payment account numbers (PAN). However, the integration of tokenization—replacing a PAN with a cryptographically created replacement called a token—into the payment card industry allowed for substantially more secure payment transactions. *EMVCo* (EX1030), 6, 9.

82. Using these limited-use numbers or tokens in place of the PAN was well-known long before the Critical Date. In fact, in August of 2011, PCI SSC adopted tokenization guidelines. *PCI SSC* (EX1031), 5. Tokenization replaces

“sensitive PAN values with non-sensitive token values.” *PCI SSC (EX1031)*, 5. Non-sensitive means that the number does “not require any security or protection” because “the token has no value to an attacker.” *PCI SSC (EX1031)*, 5. These limited-use tokens are either “single-use or multi-use.” *PCI SSC (EX1031)*, 5. A token can consist of numeric characters, alphabetic characters, or a combination thereof. *PCI SSC (EX1031)*, 5. Using tokens “instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment[.]” *PCI SSC (EX1031)*, 3. PCI SSC also teaches that “[o]ne of the primary goals of tokenization solution should be to replace sensitive PAN values with non-sensitive token values.” *PCI SSC (EX1031)*, 5.

83. Another alternative to the PAN is called a virtual PAN (VPAN). As an example, Kranzley teaches that each “VPAN 502 is associated with a PAN 504. That is, each VPAN 502 is associated with an actual payment account number that has been issued to a cardholders.” *Kranzley (EX1042)*, [0066]. Each VPAN is also “associated with the static card verification code 506 from the payment account.” *Kranzley (EX1042)*, [0066]. In Figure 5 “[t]he table includes entries identifying VPANs that have been issued or assigned by the payment provider 110.”

500

VPAN 502	PAN 504	STATIC CARD VERIFICATION CODE 506	COUNTER 508	VPAN EXPIRY 510
5555-5555-5555-5555	5422-4343-2324-1332	432	0	04/01/2009
5555-5457-4381-3243	5489-2382-1818-4343	312	4	04/30/2009
5555-5929-3453-1242	5982-2381-2848-1281	647	9	05/4/2009
5555-2438-3422-4629	5898-2428-5421-0938	321	0	03/28/2009

FIG. 5

Kranzley (EX1042), Fig. 5. The “VPANs processed over the payment network operated by MasterCard International Incorporated, VPANs are 16 digit numeric codes in which the first 6 digits are used to identify the VPAN as a VPAN to be routed to a payment provider 110 for processing.” *Kranzley (EX1042)*, [0065].

84. As an additional example, Grigg teaches a “mobile wallet account number” that “is a distinct number that is different from any traditional financial institution account number or any other account number associated with a payment device...[that] may be utilized for a transaction for a product.” *Grigg (EX1041)*, [0011]. Grigg teaches that the mobile wallet on the user device 204 will be assigned a “mobile wallet account number” to be used by the user device 204 in place of a traditional account number such as a credit card number (PAN). *Grigg (EX1041)*, [0006], [0047], [0051]. Grigg notes that the payment device or devices are for

example, “credit cards” or a “payment device account number (such as a traditional bank account number) [.]” *Grigg (EX1041)*, [0002], [0006]. Grigg notes that each payment device has a “different mobile wallet account number[.]” *Grigg (EX1041)*, [0011], [0003] (“[A] mobile wallet is typically associated with the individual’s mobile device[.]”). In Grigg, the financial institution application “provide[s] the user 202 via the user device 204 the assigned mobile wallet account number.” *Grigg (EX1041)*, [0053]. This mobile wallet number “may be permanently associated with the mobile wallet” *Grigg (EX1041)*, [0051]. “[A] user 202 may use his/her user device 204 as a mobile wallet” to make payments at a point-of-transaction (POT) or online. *Grigg (EX1041)*, [0043].

85. It was well known in the art that replacing a PAN with a different number increases security. For example, an article titled “Security in Mobile Payments” by Vizzarri et al. (“Vizzarri”) teaches different techniques to guarantee security in m-payment systems. Classical methods are end-to-end encryption and tokenization. With tokenization an encrypted or random value, called token, replaces the card number (PAN) or the magnetic stripe track data in an electronic transaction. The token then becomes the reference number representing the card number, so all tokens can be referenced back to the original card number.” *Vizzarri (EX1032)*, 5.

2. Alternatives to Static Card Verification Values

86. Another method to increase security in transactions comes in the form of the card verification value (CVV-Visa) or card verification code (CVC - MasterCard). The banking industry “developed a type of “password” for use with credit and debit cards. This password takes the form of an authentication code and is commonly referred to in the industry as a “card verification value” or “CVV.” *Ashfield (EX1033)*, [0002]. A CVV is “a “3-digit security code[.]” *Ashfield (EX1033)*, [0002].

87. To increase security in transactions, a one-time use dynamic CVV code may be generated. For example, this “dynamic CVV can be compared to at least a portion of a one-time password generated for the specific credit/debit card, and a transaction authorization can be sent to the merchant or vendor when the dynamic CVV matches all or a portion of the one-time password. A transaction denial can be sent when the dynamic CVV does not match.” *Ashfield (EX1033)*, [0005]. The bank “can separate the dynamic CVV from credit/debit card data, validate the credit/debit card data, and then merge the CVV with the credit/debit card data once the dynamic CVV is authenticated to produce the transaction authorization.” *Ashfield (EX1033)*, [0005].

88. Mastercard uses a CVC3 value and Visa uses a dCVV value to replace the static CVV. For example, Bona teaches “[r]eplacing the static CVV value with the dynamic dCVV or CVC3 codes (in the embodiments where the data is formatted

for VISA® and MASTERCARD® transactions, respectively) [.]” *Bona (EX1043)*, [0037]. Bona notes that “[t]hese one-time (i.e., dynamic) codes are generated by the smart card chip and are unique to each transaction.” *Bona (EX1043)*, [0037]. Dynamic data such as a CVC3 “would provide sufficient information in the payment authorization process to eliminate both ‘card present’ and ‘card not present’ fraud.” *Bona (EX1043)*, [0037]. Yeager teaches that “[e]xamples of cryptograms at the time of this filing are defined by the following card specification in table 4.” *Yeager (EX1029)*, [0162].

TABLE 4

Card specification	Cryptogram Designator or Name
MasterCard PayPass MSD	CVC3
Visa Contactless MSD	dCVV
Discover ZIP MSD	dCVV
EMV, Visa QVSDC, VISA VSDC, MasterCard MCHIP	AC, TC, AAC, ARQC

Yeager, Table 4.

89. Yeager teaches “[a] ‘cryptogram’ as used herein may be classified as ‘dynamic’ meaning that it is always changing from one interrogation (transaction) to the next[.]” *Yeager (EX1029)*, [0162].

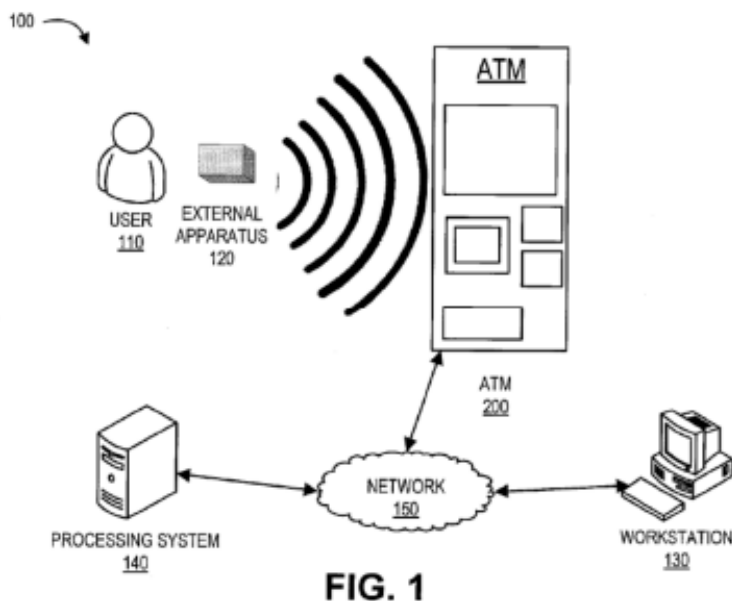
90. As described below, all of the technology claimed in the Challenged Claims predates the '520 Patent and would have been within the knowledge of a POSITA.

VII. SUMMARY OF THE PRIOR ART REFERENCES

A. Gill

91. Gill describes “[a]n 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.” *Gill (EX1004)*, Abstract, 3:51-67.

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



Gill (EX1004), Fig. 1.

93. External apparatus 120 is “operated by a user 110 who may be a customer who wants to make an ATM 200 transaction.” *Gill (EX1004)*, 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.” *Gill (EX1004)*, 5:13-18.

94. 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*:

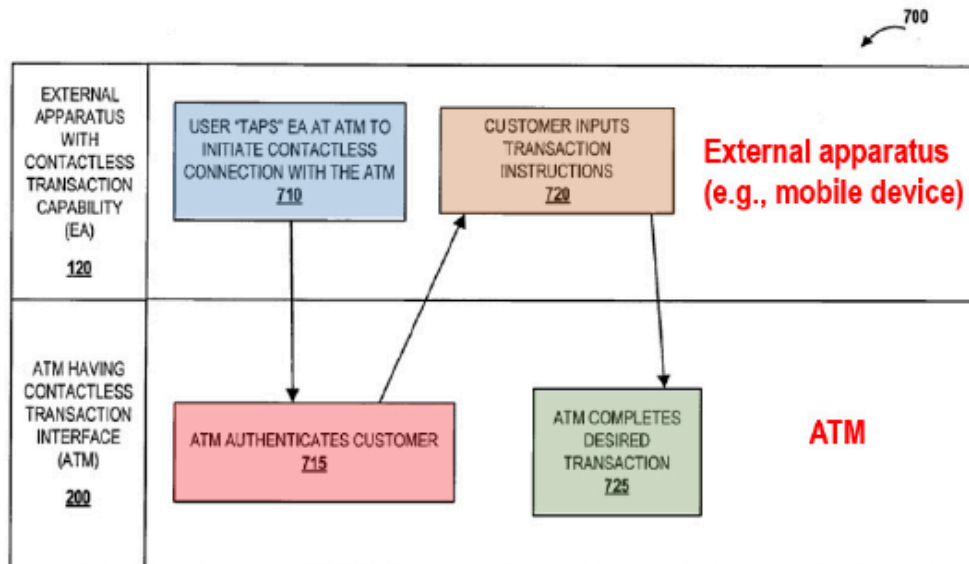


FIG. 7

Gill (EX1004), Fig. 7 (annotated).

95. As shown in Figure 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.” *Gill (EX1004)*, 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. *Gill (EX1004)*, 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.” *Gill (EX1004)*, 14:13-20. This includes requiring that the user enter a valid PIN or otherwise be authenticated before initiating or otherwise carrying out a transaction. *Gill (EX1004)*, 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, 13:47-51, 14:9-30, Figs. 6 (614), 7 (715). 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). *Gill (EX1004)*, 14:31-38, 17:56-62.

1. Gill is Analogous Art

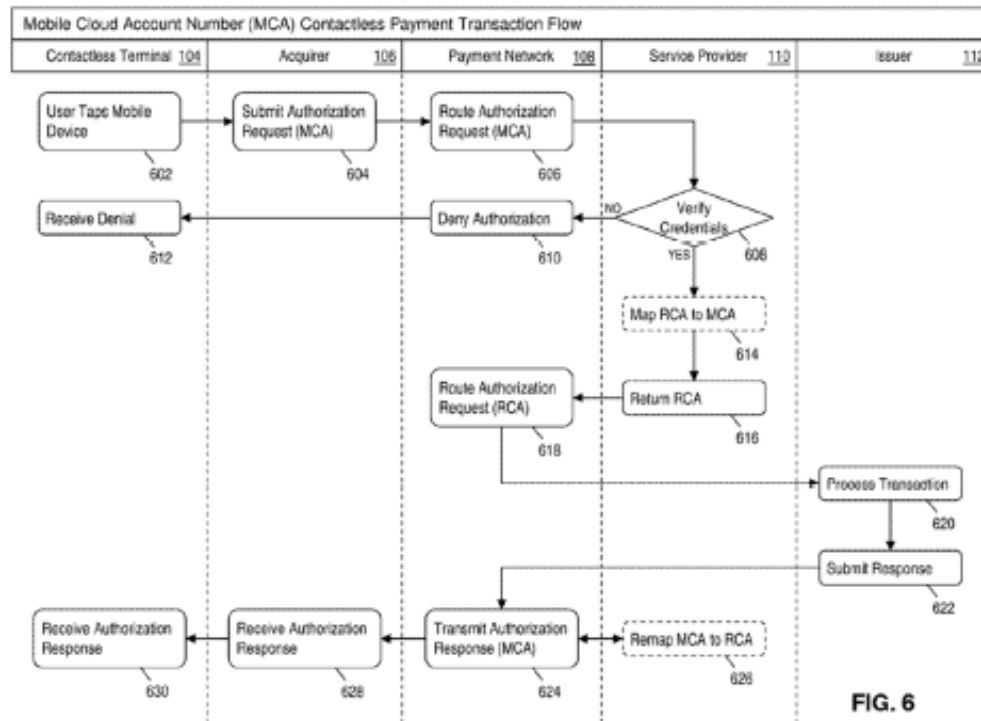
96. The '520 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications in a secure manner. '520 Patent (*EX1001*), 1:31-36, 2:49-62, 3:6-15. Similar to *Gill*, the '520 Patent describes a credit card device that securely uses a user's payment information in a financial transaction with an ATM. '520 Patent (*EX1001*), Abstract, 1:23-28, Fig. 1.

97. Additionally, a POSITA would have found *Gill* reasonably pertinent to the problem faced by the inventors of the '520 Patent because both *Gill* and the '520 Patent are directed to increasing the security of contactless payment transactions. For example, *Gill* describes a device and process for securely generating and transmitting payment credentials from a mobile device to a payment terminal (e.g., NFC point-of-sale terminal). *Gill (EX1004)*, 1:32-40, 4:35-42. Likewise, the '520 Patent describes that its invention "address security concerns of a credit card owner" for use in NFC transactions. '520 Patent (*EX1001*), 1:23-28, 1:63-2:4, 9:9-15. Accordingly, a POSITA would have considered *Gill* analogous art to the '520 Patent.

B. Smith

98. Smith describes techniques for conducting contactless payment transactions, such as through near field communications (NFC), with a mobile device. *Smith (EX1005)*, [0002], [0035], [0049], [0061], [0067].

99. 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. *Smith (EX1005)*, [0032]-[0037]; *see also* [0029]. 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).” *Smith (EX1005)*, [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.” *Smith (EX1005)*, [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.” *Smith (EX1005)*, [0034]. This tokenization process is illustrated in Figure 6:



Smith (EX1005), Fig. 6.

100. As shown in Figure 6, Smith discloses that a user initiates a contactless transaction by tapping his/her mobile device at a terminal. *Smith (EX1005)*, [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.” *Smith (EX1005)*, [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.” *Smith (EX1005)*, [0070]. Authorization for the transaction may be denied if the verification fails. *Smith (EX1005)*, [0070]. 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. *Smith (EX1005)*, [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.” *Smith (EX1005)*, [0072].

1. Smith is Analogous

101. The ’520 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications in a secure manner. *’520 Patent (EX1001)*, 1:31-36, 2:49-62, 3:6-15. Similar to *Smith*, the ’520 Patent describes a credit card device that securely uses a user’s payment information in a financial transaction. *’520 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1. .

102. Additionally, a POSITA would have found *Smith* reasonably pertinent to the problem faced by the inventors of the ’520 Patent because both *Smith* and the ’520 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. For example, *Smith* describes conducting “payment transactions is through the use of near field communication (NFC) technology to securely transmit payment

credentials from the mobile device to a contactless terminal.” *Smith (EX1005)*, [0003], [0034] (“[T]he user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.”), [0040]. Likewise, the ’520 Patent describes that its invention “address security concerns of a credit card owner” for use in NFC transactions. *’520 Patent (EX1001)*, 1:23-28, 1:63–2:4, 9:9-15. Accordingly, a POSITA would have considered Smith analogous art to the ’520 Patent.

C. Kay

103. Kay discloses techniques to “allow greater access to a banking platform via a mobile device.” *Kay (EX1006)*, Abstract, [0004]. 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. *Kay (EX1006)*, Abstract, [0004]; *see also*, [0038]-[0043], Figs. 4A-4D.

104. Kay describes techniques for conducting contactless payment transactions, such as through near field communications (NFC), with a mobile device. *Kay (EX1006)*, [0025], [0051]-[0052], Figs. 3, 4A-4E . Kay further discloses displaying a time, a passcode (PIN) and a currency amount on a mobile phone payment interface. *Kay (EX1006)*, [0040]-[0043], Figs. 4A- 4D. The user may be required to enter the PIN on the mobile device to conduct the transaction. *Kay (EX1006)*, [0041]-[0042], Fig. 4C.

1. Kay is Analogous Art

105. The '520 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications in a secure manner. '520 Patent (EX1001), 1:31-36, 2:49-62, 3:6-15. Similar to Kay, the '520 Patent describes a mobile device that securely uses a user's payment information in a financial transaction. '520 Patent (EX1001), Abstract, 1:23-28, Fig. 1.

106. Additionally, a POSITA would have found Kay reasonably pertinent to the problem faced by the inventors of the '520 Patent because both Kay and the '520 Patent describe the need for increased security in financial transactions using smart card or mobile devices. For example, Kay describes "security issues" with conducting ATM transactions. Kay (EX1006), [0003], [0050]. Likewise, the '520 Patent describes that its invention "address security concerns of a credit card owner" for use in NFC transactions. '520 Patent (EX1001), 1:23-28, 1:63-2:4, 9:9-15. Accordingly, a POSITA would have considered Kay analogous art to the '520 Patent.

D. Gomez

107. Gomez teaches "[a] payment card system uses a static payment card identifying number and generates, for each attempted transaction, an authentication cryptogram based at least upon a seed value stored within the payment card and further based upon a temporal signal value that changes for each attempted use of

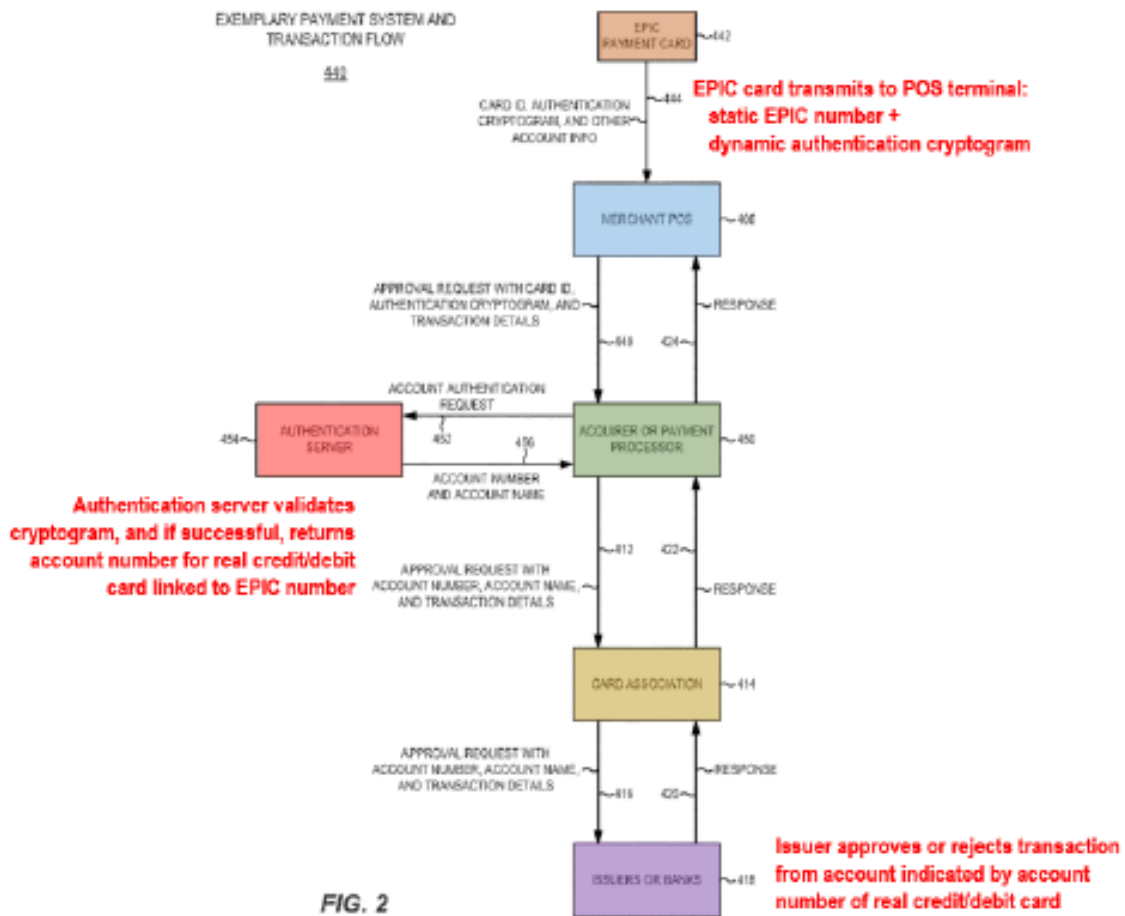
the payment card.” *Gomez (EX1007)*, Abstract. Gomez describes that its payment card can communicate the identifying number and cryptogram to the payment processing system via NFC. *Gomez (EX1007)*, 7:49-59, 8:3-23, 14:3-7, Figs. 3-4.

108. Gomez discloses “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.” *Gomez (EX1007)*, 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.” *Gomez (EX1007)*, 5:7-11, Fig. 7.

109. Customers of the system described in Gomez are issued an electronic payment card, referred to as an “EPIC” card. *Gomez (EX1007)*, 2:19-39. The EPIC card has a static payment card identifying number corresponding to the customer’s EPIC account. *Gomez (EX1007)*, 2:19-39. 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. *Gomez (EX1007)*, 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.” *Gomez (EX1007)*, 2:35-37.

110. 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. *Gomez (EX1007)*, 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. *Gomez (EX1007)*, 7:49-8:82. 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. *Gomez (EX1007)*, 18:4-42, Figs. 17-18.

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



112. 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.

Gomez (EX1007), 8:42-51.

113. 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.**

Gomez (EX1007), 7:17-26.

1. *Gomez is Analogous Art*

114. The '520 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications in a secure manner. '520 Patent (*EX1001*), 1:31-36, 2:49-62, 3:6-15. Similar to Gomez, the '520 Patent describes a credit card device that generates and uses the user's payment information for secure use in a financial transaction. '520 Patent (*EX1001*), Abstract, 1:23-28, Fig. 1.

115. Additionally, a POSITA would have found Gomez reasonably pertinent to the problem faced by the inventors of the '520 Patent because both Gomez and the '520 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized

transactions. For example, Gomez describes 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.” *Gomez (EX1007)*, 1:32-48; *see also*, 2:19-25, 4:64-5:18, 17:15-18, 21:37-40. Likewise, the ’520 Patent describes that its invention “address security concerns of a credit card owner” for use in NFC transactions. *’520 Patent (EX1001)*, 1:23-28, 1:63–2:4, 9:9-15. Accordingly, a POSITA would have considered Smith analogous art to the ’520 Patent.

VIII. SUMMARY OF UNPATENTABILITY

116. I have reproduced the Proposed Grounds of Unpatentability from the Petition for ease of reference:

Ground	Claim(s)	References
1	18-21, 24	Gill (EX1004), Smith (EX1005), and Kay (EX1006)
2	18-24	Gill, Smith, Kay, and Gomez (EX1007)

IX. OPINIONS REGARDING GROUND 1: CLAIMS 18-21 AND 24 ARE OBVIOUS OVER *GILL, SMITH, AND KAY*

A. Claim 18

117. In my opinion, the combination of Gill, Smith and Kay renders obvious as a whole claims 18-21 and 24 of the ’520 Patent.

1. 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:

118. Gill discloses “methods ... for receiving a contactless transmission from an external apparatus to an ATM.” *Gill (EX1004)*, 4:28-34; *see also*, 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. *Gill (EX1004)*, 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.”), Figs. 1, 5. As part of the transaction, Gill describes the mobile device transmitting, and the ATM receiving, the payment vehicle data, relating to the transaction, such as “account number, name, expiration date, debit/credit, etc” and a “security code.” *Gill (EX1004)*, 5:11-18, 11:7-14, 12:29-32.

Gill describes a range of possible transactions that can be performed with a mobile device and ATM, including withdrawals, deposits, and fund transfers. *Gill (EX1004)*, 14:32-36.

119. 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. *Gill (EX1004)*, 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).

120. As discussed further below, the combination of Gill-Smith-Kay teach or render obvious Claim 18 as a whole.

2. ***18(a): providing, by the electronic device, at least one of account information; identification; and authorization, for the ATM transaction; and,***

121. Gill-Smith-Kay renders obvious providing, by the mobile (electronic) device, account information, identification, and authorization for the ATM transaction.¹

a) Gill's Teachings

122. Gill teaches the mobile device provides “payment vehicle data” to the ATM terminal via a contactless/wireless connection when a user “taps” the mobile device at the ATM. *Gill (EX1004)*, 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.”), 7:64-8:2, 11:7-14, 11:34-53, 12:19-32 (“The network interface 560 may also include a mobile wallet interface 571 in order to allow a user to execute some or all of the above-described processes with respect to the mobile wallet application 521 and the secure module 581 of the mobile wallet chip 580. ... The mobile device 500 may comprise a transceiver that works in conjunction with the secure module 581 of the mobile device 500. In one embodiment, the antenna

¹ Although the claim recites three elements (i.e., account information, identification, and authorization), only one is required to satisfy this claim element.

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.”), 13:41-46, Figs. 6-7.

123. “Payment vehicle data” includes 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” ” (account information). *Gill (EX1004)*, 11:7-16; *see also*, 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”), 13:32-51. *Gill* additionally teaches that the user inputs authentication information, such as a “username, password, PIN, biometric information, and/or one or more other credentials,” to the ATM. *Gill (EX1004)*, 7:29-38; *see also* 5:15-20 (“the security authorization will require at least the input of a PIN associated with an account”), 13:47-51, 14:9-30, Figs. 6-7. Claim 20 of the ’520 Patent describes “user entered identification and authorizing information” recorded through the user interface as including “a key press PIN sequence received at the touch sensor.” *See, e.g., ’520 Patent (EX1001)*, Claim 20; *see also*, 11:27-42 (describing entry of a username and passcode to pre-authorize a user for a transaction), Claim 21 (“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”). As described above, Gill teaches the same.

b) Smith’s Teachings

124. In the combination, and based on Smith, the mobile device providing information via a contactless/wireless connection including a mobile cloud account number (MCA) (*identification* of the account) and a payment cryptogram (*authorization*) *for the ATM transaction*, in addition to other payment credentials, such as account name, expiration date, and security code. Smith teaches a mobile device providing payment credentials to a contactless terminal, such as a MCA, payment cryptogram, and online PIN. *Smith (EX1005)*, [0067]-[0068] (“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.”), [0045] (describing transmission of mobile cloud account data to contactless terminal), [0086] (describing that mobile cloud

account data may include static track data) Fig. 6; *see also* Section VII.B (describing Smith). The payment credentials are forwarded to a service provider that validates the MCA, payment cryptogram, and other credentials. *Smith (EX1005)*, [0037]-[0039], [0067], [0069]-[0070].

125. 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.” *Smith (EX1005)*, [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. *Smith (EX1005)*, [0067], [0070]-[0072], Fig. 6; *see also* Claim 18(g). Thus, the MCA is information provided by the mobile device for identification of the account to be used and the cryptogram is provided by the device for authorization of the transaction.

c) Motivation to Combine

126. As discussed above, Gill describes techniques for using a mobile device in a contactless transaction at an ATM. *Supra*, Section VII.A (describing Gill). 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. *Gill (EX1004)*, 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.,” a security code, a username and PIN. *Gill (EX1004)*, 5:13-20, 7:29-38, 11:7-13, 13:41-51, Fig. 6. A POSITA would have understood that the username and PIN in a payment vehicle is used to authenticate a user during the authorization process. The ATM and a backend payment infrastructure then processes the information conveyed from the mobile device to complete the transaction. *Gill (EX1004)*, 5:13-20, 11:7-13, 13:41-51, Fig. 6.

127. Notwithstanding these disclosures, however, Gill provides little additional detail about 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 and authorize a transaction. 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. In combination, information such as the mobile cloud account number (MCA) and a payment cryptogram (identification and authorization information), would be provided, in addition to other account information described in Gill and Smith, such as the account name, expiration date, and identification of credit or debit account (account information).

128. Including various pieces of information in payment credentials in a financial transaction was commonplace at the time as it was required to authorize and complete the transaction. For example, Yeager describes the interactions between a mobile device with NFC functionality and a POS reader (e.g. ATM), including that Track 1 and/or Track 2 equivalent data, as defined in ISO7813, is received by the reader. *Yeager (EX1029)*, [0058], [0259] (describing POS as including ATMs). As discussed in the Background of Technology, Track 1 data includes information such as account number, name, expiration date, service code, and discretionary data (e.g., PIN verification key, PIN verification value, CVV and/or CVC). *Magtek (EX1022)*, 1. Track 2 data includes similar data, but omits the name. *Magtek (EX1022)*, 1. A POSITA would have expected that such data would be transmitted to an ATM during a financial transaction.

129. Applying Smith's use of payment credentials—including an MCA and payment cryptogram—in Gill would have been obvious to a POSITA by the time of the '520 patent. As an initial matter, Gill and Smith each describe mobile devices and systems that operate in highly similar contexts by interacting with a contactless terminal to perform a transaction. *Gill (EX1004)*, 3:51-67, Figs. 1, 6; *Smith (EX1005)*, [0032]-[0038], Figs. 1, 7. 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. *Gill* (EX1004), 10:34-53, 11:3-16, 13:3-31, Fig. 5; *Smith* (EX1005), [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. *Gill* (EX1004), 2:1-2 (“initiate a debit account transaction”), 4:62-63 (“with ATM transactions, the transaction is generally a debit account transaction”); *Smith* (EX1005), [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”).² A POSITA thus would have understood Smith’s payment credentials and expected them to be operable in ATM transactions like those discussed in Gill.

130. Moreover, a POSITA would have sought to use payment credentials like Smith’s MCA and payment cryptogram in the combination with Gill (and Kay, as described below) to realize predictable security improvements. As discussed in

² Apart from debit account transactions, Gill and Smith both describe systems operable to perform transactions conducted with a credit card or credit account. *See, e.g., Gill*, Abstract, 2:4-5; *Smith* (EX1005), [0029]-[0031]

the Background of Technology (Section VI.C), the use of information in place of a PAN, such as a token or virtual, PAN was well-known prior to the '520 Patent, as described in *PCI SSC (EX1031)* (payment token), *Kranzley (EX1042)* (VPAN), and *Grigg (EX1031)* (mobile wallet account number). Using such a replacement number (Smith's MCA) in place of the primary account number (Smith's RCA) reduced the amount of cardholder data in the environment, thereby reducing the possibility of a user's account being compromised. This is because the real account number need not be stored on the mobile device, nor transmitted in a transaction, making it close to impossible to determine from the information transferred in the transaction.

131. The use of a dynamic cryptogram, such as Smith's payment cryptogram, generated by a device to authorize a payment transaction was equally well-known long before the '520 Patent. *See, e.g.,* Section VI.C.2; *see also below*, Claims 18(h) and 19.

132. Accordingly, a POSITA would have been well aware of the benefits and implementation of using an alternative account number and a dynamic cryptogram in financial transaction, as discussed below.

133. Consistent with the above knowledge of a POSITA, because Smith's MCA is merely a token for the real card account number (RCA), the mobile device can store the MCA without needing to store or send 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 Smith (EX1005)*, [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.”), [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. 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.”).

134. Conducting contactless transactions with the MCA and a cryptogram 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. *Smith (EX1005)*, [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.”).

135. Additionally, cryptograms in payment devices were common long before the '520 patent, as discussed briefly above. 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 and other data 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. *Smith (EX1005)*, [0007], [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.”), [0077], [0086], [0103]. A POSITA likewise would have been motivated 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 Gill (EX1004)*, 1:34-36 (“The absence of

contactless functionality with ATMs in the marketplace is largely due to security issues ...”), 4:35-55.

136. Integrating Smith’s suggested use of payment credentials, including 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). Indeed, Gill recognizes that ATMs have not “enjoyed the benefits of contactless transactions, while numerous point-of-sale (POS) contactless terminals have been made available.” *Gill (EX1004)*, 4:35-38. Gill continues that financial institutions “do not wish to institute contactless ATM terminals that do not utilize any security verification.” *Gill (EX1004)*, 4:51-55. Thus, a POSITA would have been motivated to combine Gill and Smith to provide more secure contactless ATM transactions. 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. *Smith (EX1005)*, [0011], [0029], [0067], [0096], Fig. 6; *Gill (EX1004)*, 14:1-37, Fig. 7. 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 to yield the predictable result of more secure payment transactions.

137. In the combination, the information provided by the mobile device to the ATM is at least information relating to an account information (e.g., account name, expiration, debit/credit), identification (e.g., MCA and username), and/or authorization (e.g., cryptogram and PIN) for a transaction at an ATM.

3. ***18(b): wherein the electronic device comprises a user interface comprising: displays; touch sensors; and buttons; and,***

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

139. Gill teaches that “the mobile device 500 may have a ***user interface*** that includes user output devices 536 and/or user input devices 540.” *Gill (EX1004)*, 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)” *Gill (EX1004)*, 12:33-44. “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).” *Gill (EX1004)*, 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. The “touch sensor array” of ’520 Patent refers to a “touchscreen panel” or “keypad.” *’520 Patent*

(EX1001), 6:31-33 (“A user input may be made via the touch sensor array 245, which may comprise a touchscreen panel, a keypad, or a combination thereof.”), 9:19-25, Figs. 2B, 4A. A keypad and keyboard would each include mechanical buttons, while a graphical user interface on a touchscreen 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 combination). *Kay* (EX1006), Figs. 4B, 4D; see Claims 18(d)-(e).

140. Mobile devices including a touchscreen and touch sensors were well known at the time. For example, U.S. Patent No. 8,462,133 to Lynch, et al. (assigned to Apple) (“Lynch”), describes a phone, such as an iPhone, having a touchscreen assembly also including buttons. *Lynch* (EX1044), 4:24-5:3, Fig. 1A. The touchscreen assembly includes a capacitive sensor (i.e., touch sensor) that “may sense the touch.” *Lynch* (EX1044), 5:39-48, 6:65-7:2, Fig. 2A. These types of devices with touch sensors were well known prior to the ’520 Patent.

141. A POSITA, therefore, would have known of mobile devices as of the ’520 patent whose user interfaces commonly included such physical display elements, including touch sensors and buttons for a touchscreen display, as taught by Kay, and been motivated to use the same consistent with Gill’s description of a GUI for user input.

142. Gill-Smith-Kay provides multiple “displays” to the same extent as the specification of the ’520 patent itself, which refers to just a single display 250/450. *See ’520 Patent (EX1001)*, Figs. 2A-2B, 4A-4B.

143. Even if Claim 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 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 to interact with a mobile wallet application (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).

144. 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.

Kay (EX1006), Figs. 4A-4; *see also* Claims 18(d)-(e).

4. ***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,***

145. Gill-Smith-Kay 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.

a) Gill's Teachings

146. 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**” (*user selection from the user interface ... of a user selected account*) for a transaction. *Gill (EX1004)*, 13:9-17; *see also*, 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”), 10:41-46. The mobile device is operable to convey data corresponding to the selected payment vehicle (*user selected account*) to an ATM over a wireless or contactless interface such as NFC (*wirelessly convey with an ATM*). *Gill (EX1004)*, 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.”), 10:47-53, 13:33-46.

b) Smith’s Teachings

147. In the combination, Smith also discloses that the user can select a particular account from a GUI to cause the mobile device wirelessly convey payment credentials corresponding to the selected account (including an MCA and payment cryptogram). *Smith (EX1005)*, [0035] (“The user may indicate, using the mobile device 102, one of the MCAs to be used to fund a financial transaction ... The mobile device may then transmit payment credentials for the indicated mobile cloud account data to a contactless point-of-sale terminal via near field transaction.”), [0045], [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. The payment credentials are conveyed wirelessly via NFC. *Smith (EX1005)*, [0035], [0049], [0059], [0061], [0067], Fig. 5.

148. A POSITA further would have understood and/or it would have been obvious for the mobile device to record the user’s selection from the user interface. This is evident, for example, from the fact that the mobile device properly acts on the user’s selection/instructions by conveying payment information from the mobile device to the ATM for the correct account in accordance with the user’s selection.

Smith (EX1005), [0035], [0049], [0059], [0061], [0067]-[0068], [0075]; *Gill (EX1004)*, 5:13-16, 13:9-17, 14:31-37. In other words, without first recording the user input, the device could not operate in accordance with the input instructions.

5. ***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,***

a) Gill's Teachings

149. 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.” *Gill (EX1004)*, 18:19-22.

150. Gill discloses that a customer can “input[] instructions to [an] ATM 200 to execute [a] desired transaction.” *Gill (EX1004)*, 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.” *Gill (EX1004)*, 14:31-36; *see also*, 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 teaches the user can select among transaction types that include “***withdrawing funds, depositing funds, transferring funds, balanc[ing] checks, ... and the like.***” *Gill (EX1004)*, 14:31-37; 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):

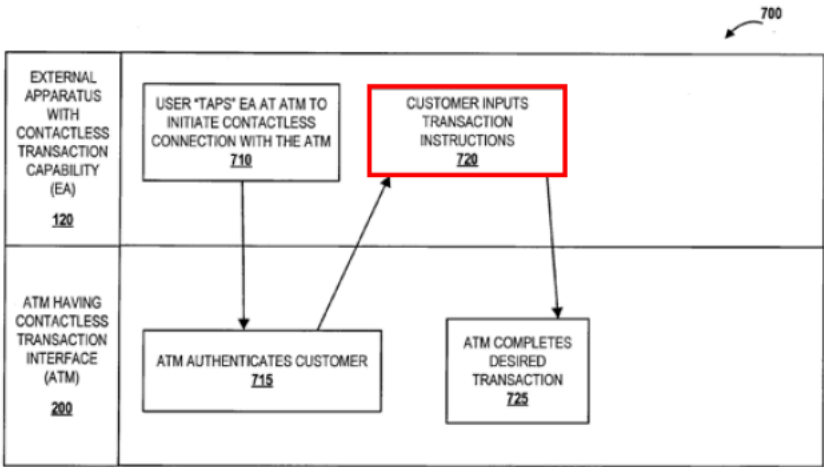


FIG. 7

Gill (EX1004), Fig. 7 (annotated); *see also*, 12:33-34, 13:9-17 (describing mobile device GUI).

151. 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. *Gill*

(EX1004), Fig. 7 (depicting instructions input at box 720 through the external apparatus (mobile device) 120), 16:58-64, 18:19-22. 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.” *Gill (EX1004)*, 10:42-46; *see also*, 13:9-17, Fig. 5.

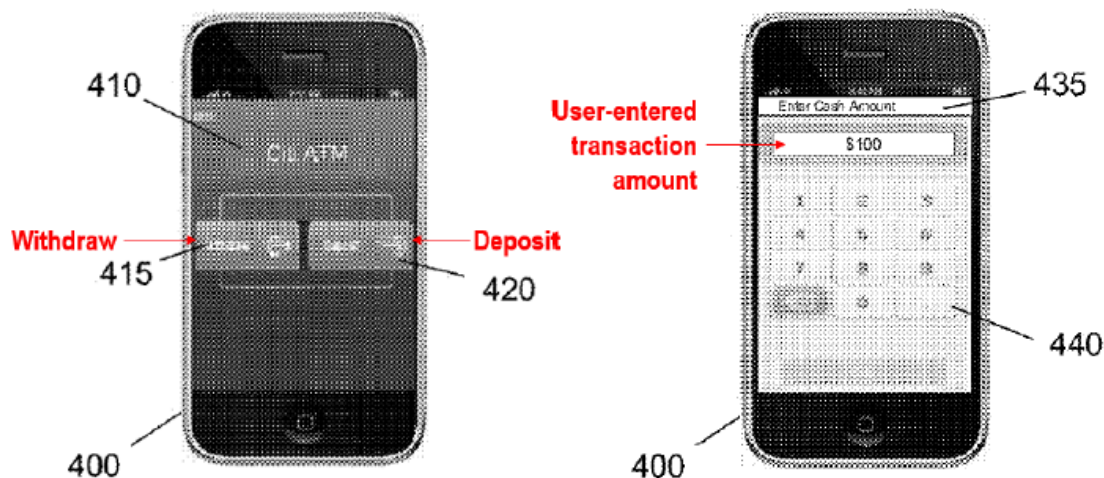
152. Nonetheless, Gill does not expressly depict the GUI and lacks detail as to how the user would specifically interact with the GUI to input instructions or select a particular type of ATM transaction.

b) Kay’s Teachings

153. 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. Kay demonstrates GUIs adapted to receive user instructions for ATM transactions on a mobile device were known well before the ’520 Patent.

154. Kay, like Gill, discloses a method of conducting ATM transactions using a mobile device including a touchscreen. *Kay (EX1006)*, [0017]-[0021], [0038]-[0052], Figs. 1, 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” *Kay (EX1006)*, [0039], [0035]. The application includes a user interface that allows a user to “choose a category of instructions or transactions.” *Kay (EX1006)*, [0040]. As shown in Figure 4B (reproduced below), the user interface “present[s] options for ‘withdraw’ 415 and ‘deposit’ 420.” *Kay (EX1006)*, [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. *Kay (EX1006)*, [0040]. 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 Figure 4D:



Kay (EX1006), Figs. 4B (left) and 4D (right) (annotated); *see also*, [0042]-[0043], Fig. 4C (depicting PIN entry).

155. Kay’s teachings in this regard would have been obvious to apply to the combination with Gill and Smith for the reasons described below. 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.” *Gill (EX1004)*, 14:31-37.

c) Motivation to Combine

156. 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, including funds transfer options. 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. *Gill (EX1004)*, 5:13-16, 13:9-17, 14:31-37, Fig. 7; *Kay (EX1006)*, [0040]-[0041]; *Smith (EX1005)*, [0067]-[0068], [0075].

157. It would have been obvious to a POSITA to apply in the combination Kay’s teaching of a graphical user interface (GUI) on a mobile device, which would allow a user to select a particular type of transaction (e.g., those described in *Gill* and *Smith*) from a list of available transaction types. 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, which already teach a GUI and touchscreen display. 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. *Gill (EX1004)*, 10:41-46, 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). *Kay (EX1006)*, [0038]-[0052], Figs. 1, 3, 4A-4F. 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. As with the preceding limitation, the device could not operate in accordance with the input instructions without first recording the user input.

158. 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 (i.e., devices with GUIs) in substantially the same way, and would have achieved merely predictable results (e.g., more secure transactions). Kay's GUI is designed for ATM transactions and would naturally

support the ATM transactions described by Gill as well. Hence, a POSITA would have expected a reasonable expectation of success combining the teachings of Kay with those of Gill and Smith in the manner described above.

6. ***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,***

159. Gill-Smith-Kay renders obvious receiving user input information from the user interface that includes at least one of a set recited in Claim 18(e).

a) Gill's Teachings

160. Gill teaches a user can input identification, account, operation and/or authorizing information in order to perform an ATM transaction. For example, Gill teaches that “the ATM 200 may require users to identify and/or authenticate themselves to the ATM[.]” *Gill (EX1004)*, 7:29-32. For example, the user may be authenticated based on a username and PIN. *Gill (EX1004)*, 7:32-38; *see also*, 14:15-21 (“the customer may input authentication information_on his external apparatus 120 and [] 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

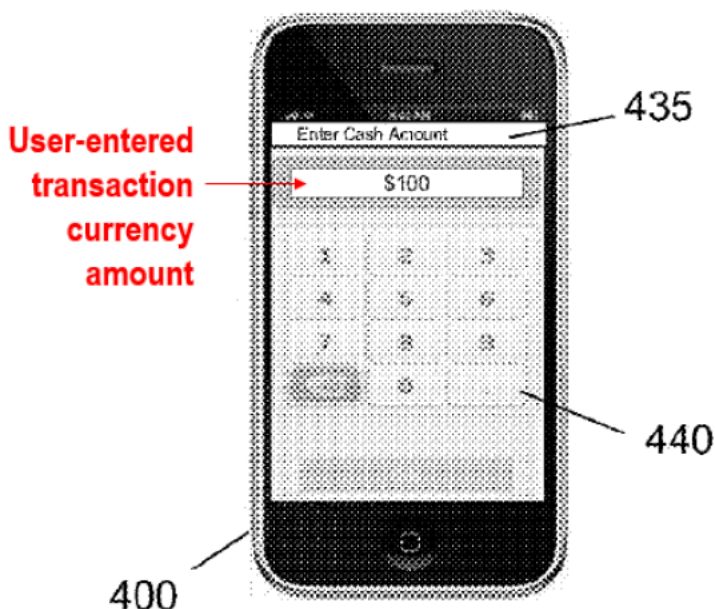
581 of the mobile wallet chip 580, etc.”), 14:9-20. Similarly, the user inputs identification and authentication information, such as a “username, password, PIN, biometric information, and/or one or more other credentials,” to the ATM. *Gill (EX1004)*, 7:29-38; *see also* 5:13-20 (“[T]he ATM is configured 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. Generally speaking, the further security authorization will require at least the input of a PIN associated with an account”), 13:47-51, 14:9-20 (“Authentication ... generally requires the customer to enter a PIN associated with the account the customer wishes to authenticate himself to the ATM 200. ... [T]he customer may input authentication information on his external apparatus 120 and such transfer such data to the ATM 200 upon establishing the contactless connection.”), Figs. 6-7. As discussed in Claim 18(a), the ’520 Patent describes that “user entered identification and authorizing information” includes “a key press PIN sequence.”

161. Gill further describes user inputs to the user interface regarding a payment vehicle (account information). *Gill (EX1004)*, 13:14-15 (“The GUI for the mobile wallet application 521 may allow the user 110 to enter ***input to select a payment vehicle***”), 12:33-35, 13:9-17; *supra*, Claim 18(a).

162. Gill also describes user inputs received at the mobile device directed to operations of the device, including withdrawing, depositing and transferring funds. *Gill (EX1004)*, 13:12-16, 14:9-37, Fig. 7 (715-720) (depicting the user inputting instructions to the external apparatus 120 to execute the desired transaction); *see also*, 14:31-37.

b) Kay's Teachings

163. In the combination, Kay also discloses the mobile device receiving user input information from a user interface indicating an amount of cash to withdraw (amount of currency) for a transaction. *Kay (EX1006)*, [0043] (“In 340, the customer enters the amount of cash to withdraw and confirms the transaction. A 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 ...”); *see also* Claim 18(d).



Kay (EX1006), Fig. 4D (annotated).

c) Motivation to Combine

164. A POSITA would have understood and/or it would have been obvious that Gill's mobile device would allow for the input of a currency amount. *See* Claim 18(d). Gill already teaches that the customer inputs instructions to the mobile device to, for example, withdraw funds. *Gill (EX1004)*, 14:31-36, Fig. 7; *see also* Claims 18(c)-(d). It would have been obvious to a POSITA to apply Kay's teachings of allowing for input of a currency amount for such withdrawal because, absent such input, the ATM would not know how much money to disperse. A POSITA would have been motivated to implement this functionality in order to make the mobile device carry out the functionality described by Gill on the mobile device, e.g., withdraw or transfer funds. Kay's GUI allowing entry of a currency amount provides

a concrete design element for a GUI similar in context to Gill that would allow a user to enter such instructions in a logical and intuitive way. Mobile payment devices that allowed for input of similar functions on a touch-screen were well-known at the time. As one example, WO 2010/039337 to Lin describes a mobile phone having a transaction application for conducting an NFC transaction with another electronic device. *Lin (EX1049)*, Abstract, 3:29-4:5, 14:1-9, 14:22-29, 20:4-9, Fig. 1. A user can input financial accounts, e.g., credit card account to be used in transactions through a touchscreen interface. *Lin (EX1049)*, 37:16-25, 38:17-39:31, 43:30:44:2, Figs. 5A, 6A. The user can also unlock the transaction application through entry of a PIN. *Lin (EX1049)*, 52:1-15, Fig. 10B. Then, the user can select an account to be used in the transaction and authorize the transaction, such as by entering a PIN. *Lin (EX1049)*, 71:7-72:6, 75:14-76:12, 130:22-29, Figs. 14E-H. Lin further teaches that a currency amount can be entered, e.g., the amount of a tip. *Lin (EX1049)*, Fig. 30B. As another example, U.S. Publn. No. 2009/0307132 to Phillips describes a mobile phone through which a user can add an account, select an account to use in a contactless transaction. and also select an amount of currency to add to an account. *Phillip (EX1050)*, [0024]-[0026], [0029], [0036]. [0054], Figs. 2, 4, 8. The user may be required to enter a PIN to conduct a transaction. *Phillip (EX1050)*, [0052]-[0054], [0059], [0065], Figs. 7, 9.

165. This combination would have involved the predictable use of a known GUI, as taught by Kay, to improve similar devices with GUIs in performing an ATM transaction and would have achieved a predictable result of a payment device that guides a user various steps of a transaction. A POSITA would have had a reasonable expectation of success combining the teachings of Kay with those of Gill and Smith in this manner.

166. In the combination, therefore, at least an amount of currency, payment vehicle information, instructions for device operations, and username and PIN are input to the mobile device user interface.

7. *18(f): wherein the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC; and,*

167. Gill-Smith-Kay renders obvious that the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC.

168. Gill discloses that information exchanged between the mobile device and the ATM, such as a PIN and transaction information, occur wirelessly via near-field communications (NFC) (exchanged wirelessly between the electronic device and the ATM via NFC). Gill (EX1004), 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 *nearfield communication (NFC) technology*”), 4:28-34, 14:13-20 (“[T]he customer may first authenticate himself prior to the contactless connection being established. For instance, 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, 6:43-50, 13:41-46 (“typical content to be transferred from the external apparatus 120 includes data identifying the financial account associated with the external apparatus”); *see also* Section VII.A.2 (discussing Gill). 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 Claims 18(a) and (c)-(e). *Gill (EX1004)*, 13:51-14:37; *see also*, 13:32-51, Figs. 1-3, 5-6.

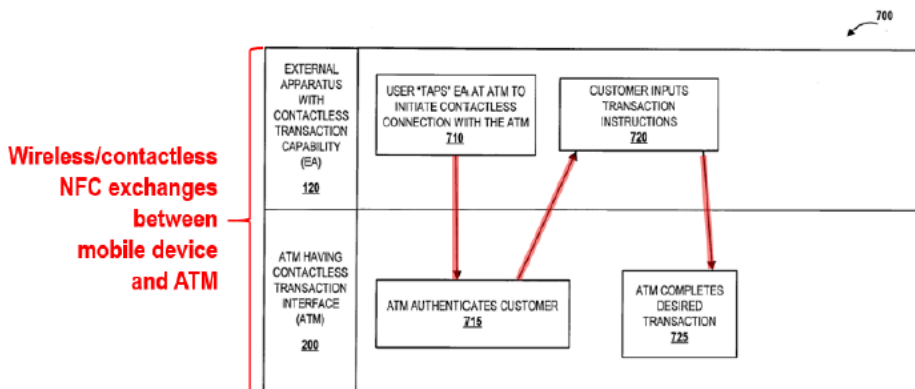


FIG. 7

Gill (EX1004), Fig. 7 (annotated); *see also* Figs., 1-3, 5.

169. Smith also discloses, and the combination provides, for the exchange of payment credentials (including information relating to the selected account, the MCA, payment cryptogram and PIN) via NFC between the mobile device and a terminal. *Supra*, Claim 18(a); Section VII.B (discussing Smith). 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. *Smith (EX1005)*, [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[] ..."); *see also* [0034]), [0045], [0058]-[0059] (describing user's selection of a payment account for a transaction), Figs.5- 6; *supra*, Claim 18(a).

170. In the combination, therefore, the identification, selection, information and authorizing operations discussed in Claims 18(a) and (c)-(e) are exchanged wirelessly between the electronic device and the ATM via NFC, as taught by Gill and Smith.

8. ***18(g): wherein the ATM is configured for performing the user selected account operation using the identification and authorizing information; and,***

171. Gill-Smith-Kay renders obvious configuring the ATM to perform the user selected account operation using identification and authorization information received wirelessly from the mobile device. *Supra*, Claims 18(a), (c)-(f). For example, Gill teaches that the ATM authenticates the customer based on credentials (e.g., account name, expiration date, security code, username and/or PIN) (identification and authorizing information) received wirelessly from the mobile device. *Gill (EX1004)*, 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”), 13:47-51 (“ATM 200 authenticates the user”), Figs. 6 (612, 614), 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.” *Gill (EX1004)*, 14:31-37, Fig. 7 (720, 725); *see also*, 5:11-20, 7:29-46 (“ATM 200 will initiate, perform, complete, and/or facilitate a transaction”).

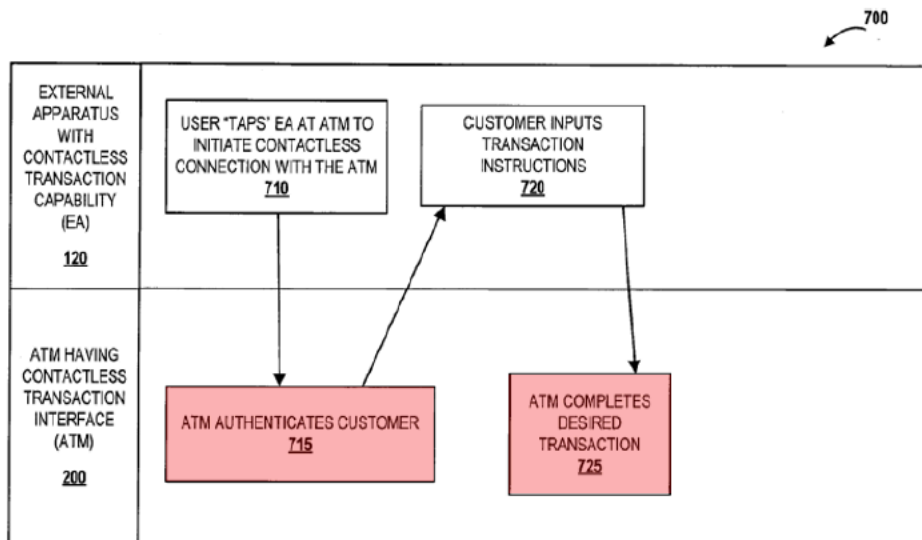


FIG. 7

Gill (EX1004), Fig. 7 (annotated).

172. Smith similarly describes that payment credentials, e.g., MCA and payment cryptogram (*identification and authorizing information*), are transmitted to a contactless terminal. *Smith (EX1005)*, [0035], [0045], [0059], [0061], [0067]-[0068]; *see also* Claim 18(a). The contactless terminal authenticates a PIN and forwards the payment credentials for authorization. *Smith (EX1005)*, [0036]-[0039], [0068]-[0071].

173. In the combination, the ATM is configured to perform the user selected account operation using the identification and authorizing information, such as the MCA, payment cryptogram, username and PIN transmitted to the ATM, as discussed

above in Claim 18(a). *See Smith (EX1005)*, [0035], [0041], [0045], [0049], [0061], [0067]-[0068]; Claim 18(a).

9. ***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,***

174. Gill-Smith-Kay renders obvious exchanging wirelessly with an ATM transaction data including account, identification, and authorizing information, including at least the MCA and payment cryptogram, as discussed above. *Supra*, Claims 18(a), (b)-(f).

175. As discussed in Claim 18(a), it would have been obvious for the wireless exchange to involve transmission of a mobile card account number (MCA) and a payment cryptogram (*identification and authorizing information*) from a mobile device to a terminal, as taught by Smith. *Smith (EX1005)*, [0067]-[0068] (“In step 602, the user 302 may ‘tap’ the contactless terminal 104 using the mobile device 102 with payment credentials loaded into the mobile card let 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*** ... The mobile device 102 may also transmit additional credentials to the contactless terminal ... includ[ing] a mobile personal identification number (PIN)[.]”), Fig. 6; *see also*, [0035]-[0036], [0045], [0051] (“MCAs for use in conducting contactless payment transactions”), [0061].

176. 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. *Smith (EX1005)*, [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. *Smith (EX1005)*, [0086] (“the generated MCA may include an expiration date”).

177. Further, according to Smith, the payment cryptogram (dynamically generated limited-use number portions) can be a “dynamic card validation code” or an “authorization request cryptogram,” either of which a POSITA would have understood to be a dynamically generated limited-use number portion of the payment credentials. *Smith (EX1005)*, [0103], [0067], [0096]-[0097], [0063]. Smith specifically explains that the payment cryptogram is “generated” for each transaction “based on mobile cloud account data” (limited-use)—in contrast to the MCA which is read from memory of the device. *Smith (EX1005)*, [0067]; *see also* [0099], [0103], Fig. 12. Because the cryptogram is generated for each transaction, it is “dynamic.”

178. 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, such as a dynamic card validation code, on a frequent basis (e.g., with each transaction or some other period of time) 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. *See* Section VI.C.2. Smith explains that the service provider can identify and authorize a transaction request by verifying the cryptogram using known techniques. *Smith (EX1005)*, [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”). 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. *Smith (EX1005)*, [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. *Supra*, Claims 18(a), (f)-(g).

10. 18(i): wherein said static and dynamic information is combined to perform the user selected ATM operation.

179. Smith discloses, and the combination renders obvious, that the MCA and payment cryptogram (said static and dynamic information) are combined into “payment credentials” to form an authorization request for performance of a user selected operation. *Smith (EX1005)*, [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*, [0035]-[0036], [0045], [0059] (“the user 302 may (e.g., via

the display UI 204), select an MCA for use in funding a contactless payment transaction”), [0061].³

180. In the combination as described above (*supra*, Claims 18(a), (g)), the MCA and cryptogram are combined as payment vehicle data or payment credentials with additional information, to perform a user-selected ATM operation such as a deposit, withdrawal, or funds transfer operation like those described in Gill, Smith, and Kay. *Gill (EX1004)*, 14:34-37; *see also, Smith (EX1005)*, [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”); *Kay (EX1006)*, [0017]

³ Smith alternately refers to the MCA and payment cryptogram being combined to form “transaction data.” *Smith (EX1005)*, [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.”).

(“Financial transactions include ... deposits, withdrawals, account transfers[.]”),
[0031], [0040]; Claims 18(a), (c)-(g).

B. Claim 19

1. ***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.

181. Gill teaches that “account information” and/or “payment vehicle data” that includes an account name (*user identification* or *username*), an account number (*payment numbers, ATM accounts, bank account*), and an expiration date and debit/credit account (*transaction information*) is provided to the ATM. *Gill* (EX1004), 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.)”), 11:7-16, 12:29-32, 13:12-16.

182. Gill further describes identification and authentication information is provided through user input, such as a user's name and PIN (secrets, passwords, passcodes) or biometric information (biometric user identification). *Gill (EX1004)*, 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. This information is identification and authorizing information used by the ATM in performing the transaction.

183. Smith further discloses, and the combination provides, that the mobile device generates transaction data or payment credentials for identification and authorization, including an MCA, payment cryptogram and PIN. *Supra*, Claims 18(a), (h)-(i); *Smith (EX1005)*, [0067]-[0068]. The MCA corresponds to a real card account, such as a credit or debit card, and constitutes a device account number (having been provided to that device), payment number, bank accounts, and/or payment device identifier. *Smith (EX1005)*, [0067]-[0068]; *see also*, [0031].

184. The cryptogram is generated based on secret mobile cloud account data stored on the mobile device, including the MCA, secrets and a key. *Smith (EX1005)*, [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”). It was well known to use multiple data elements in generating a dynamic cryptogram for authorization to increase the security of the transaction. For example, U.S. Patent No. 7,740,168 to Hammad, et al. (assigned to VISA) (“Hammad”) recognized that using multiple data elements beyond a counter to generate a dCVV would further secure the transaction by decreasing the likelihood of a bad actor being able to recreate the dCVV. *Hammad (EX1045)*, 1:66-2:4. Specifically, Hammad describes the use of multiple dynamic and static data elements to use in generating a dCVV. *Hammad (EX1045)*, 4:21-60. The dCVV is then embedded in the Track 1/Track 2 payment data used in the transaction. *Hammad (EX1045)*, 4:7-20, 6:40-42, 6:49-7:28, Figs. 4-5. A dynamic CVV (i.e., dCVV) is described as CVC3 in the context of MasterCard’s PayPass and a dCVV in the context of Visa (to which Hammad is assigned). *Yeager (EX1029)*, [0162] (Table 4). A CVC3 and dCVV are “dynamic” cryptograms “as the input to the calculation of the cryptogram change

with each interrogation [i.e., transaction].” *Yeager (EX1029)*, [0177]; *see also* [0162].

185. Accordingly, a POSITA would have been well aware of the benefits of using multiple data elements to generate a dynamic cryptogram, unique to the transaction, device, and account, as described in Hammad, for use in a financial transaction and, therefore, would have been motivated to do the same in order to make the transaction and the user’s account information more secure.

186. Thus, the MCA and cryptogram (identification and authorizing information) are generated from at least a device account number/payment number/bank account/device identifier, secret and a key. The PIN is a passcode. In the combination, the complete transaction data or payment credentials are generated from these pieces of information.

C. Claim 20

1. ***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.

187. Based on Gill, the mobile device records user-entered identification and authorization information through a user interface (GUI), including entry of a “username, password, PIN, biometric information, and/or one or more other credentials.” *Gill (EX1004)*, 7:32-38; *see also*, 5:18-20 (“require at least the input of the proper PIN associated with the account”), 6:13-26, 13:47-51, 14:9-30, Figs. 6-7; *supra*, Claim 18(e). Gill further discloses that “[t]he user input devices 540” of the mobile device can include a “touchscreen” and “keypad.” *Gill (EX1004)*, 12:33-44, 6:22-26. Smith similarly teaches that payment credentials may include a PIN entered on the mobile device. *Smith (EX1005)*, [0068]. Kay similarly teaches that the user enters a “PIN,” “username and password, or a biometric credential” to the mobile device. *Kay (EX1006)*, [0041]-[0042], Figs. 3, 4C (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).

188. A POSITA would have understood and/or it would have been obvious that the user’s entry of a PIN, passcode, or like credentials (*user entered identification and authorization information*) recorded through the user interface 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. See also Claims 18(c)-(e).

D. Claim 21

1. ***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.***

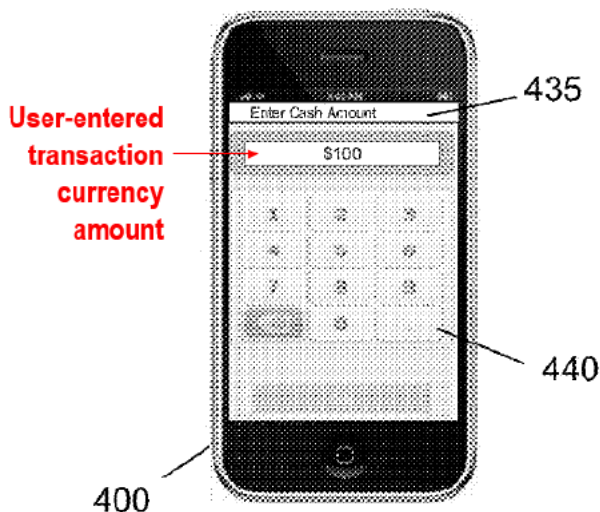
189. As discussed in Claims 18(e) and 20, *supra*, Gill discloses, and the combination renders obvious, identification and authorization information recorded responsive to the user inputting information using input methods provided by the ATM to record a PIN number, password, and biometric information (biometric identification).

E. Claim 24

1. ***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.***⁴

⁴ 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.

190. As discussed with respect to Claim 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” (cash amount) for a transaction. *Kay (EX1006)*, [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 ...”).



Kay (EX1006), Fig. 4D (annotated); *see also Gill (EX1004)*, 12:33-34, 13:9-17 (describing mobile device GUI).

191. As shown in Figure 4D, the “amount of currency” is expressly identified as a “Cash Amount”—e.g., a cash amount intended for a withdrawal transaction. *Kay (EX1006)*, [0043].

X. OPINIONS REGARDING GROUND 2: CLAIMS 18-24 ARE OBVIOUS OVER *GILL, SMITH, KAY, AND GOMEZ*

192. In my opinion, the combination of Gill, Smith Kay, and Gomez renders obvious as a whole claims 18-24 of the '520 Patent.

A. Claim 18

193. The combination based on Gill in view of Smith, and Kay would have rendered obvious and provided each element of independent claim 18 for the reasons described above with respect to corresponding claim elements in Ground 1.

194. Although Smith discloses that the payment cryptogram can be dynamic in the form of an authorization request cryptogram or a dynamic card validation code generated based on at least a portion of the mobile cloud account data (e.g., issuer public and private key and MCA) securely stored on the mobile device, Smith does not expressly disclose all 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. *See* Section VI.C.2; Claims 18(h), 19. 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, such as described by Gomez.

1. Gomez's Teachings

195. Gomez teaches computing an authentication cryptogram based on a “temporal signal” that changes from transaction to transaction. *See, e.g., Gomez (EX1007)*, 1:58-2:1 (“[A] payment card systems that utilizes a secure authentication cryptogram which is ***generated uniquely for each attempted used of the payment card***, and which expires within a short period of time thereafter. 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”), 8:36-41. In Gomez, the temporal signal is combined with other data stored on the device (e.g., a seed value, such as a “unique customer key”) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. *Gomez (EX1007)*, 2:45-50, 7:26-48, 8:25-51, 16:64-17:12, Figs. 3, 5. The cryptogram is then formed by encoding the output of the hash function. *Gomez (EX1007)*, 2:14-17, 8:52-9:11. Gomez further teaches that the cryptogram can be transmitted with other account information (e.g., card number) in an NFC transaction. *Gomez (EX1007)*, 7:47-57, 8:11-24, 10:54-57, 14:3-7.

196. 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.” *Gomez (EX1007)*, 5:43-47; *see also*, 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, 14:37-39, 21:37-48.

2. Motivation to Combine

197. In the Gill-Smith-Kay combination of Ground 1, the mobile device generates contactless ATM transaction payment credentials that include a mobile card account number (MCA) and a payment cryptogram as taught in Smith. *Supra*, Claim 18. In the Gill-Smith-Kay-Gomez combination, the payment cryptogram is dynamically generated based on a temporal signal as taught in Gomez, in addition to mobile cloud account data of Smith, and constitutes “dynamically generated limited use number portions” as recited in Claim 18(h). *Gomez (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*”).

198. It would have been obvious and a POSITA would have been motivated to further modify the Gill-Smith-Kay combination of Ground 1 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.

199. 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 Gomez (EX1007)*, 1:58-63, 2:21-25, 5:43-47, 13:63-14:2. The use of dynamic cryptograms was well-known at the time. *See* Claim 19. It was also known to use time as an input data element to generate the cryptogram to prevent replay attacks. For example, Hammad (EX1045) teaches that a dCVV (i.e., cryptogram may be generated using time as one of the dynamic data elements. *Hammad (EX1047)*, 3:9-11, 4:37-40, 4:61-5:5, 6:49-57, 7:4-14, Figs. 4-5. In addition, I wrote papers on using timestamps for a similar purpose (i.e., preventing replay attacks) as early as 1993. *See* EX1046, *A Note on the Use of Timestamps as Nonces*. Using timestamps as a security measure to prevent replay attacks in credit card transactions was also known as early as 1997. *See* U.S. Publication No. 2002/0174075 to Mirlas (EX1047), Abstract, [0038]-[0039], [0124] (describing a payment message sent for an online transaction that includes payment info and timestamp “to prevent replay attack, among other information), Figs. 1-2; U.S. Patent No. 5,903,721 to Sixtus (EX1048), Abstract 8:57-66 (“The time stamp is an additional security feature ... which is preferred since it changes with every transaction request and makes it more difficult to spoof (trick) the system.”). Sixtus cites my paper titled “Requirements for Network Payment: The NetCheque Perspective,” on its face (although he misspells my last name). Implementing this feature in the proposed combination would have predictably yielded the result of increased security by limiting the time for which a generated cryptogram could be

used. This modification would not change the operation of the combination or require any additional hardware; rather, it would require only minor programmatic changes.

200. 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 (e.g., using multiple data elements to generate a cryptogram) that would have achieved no more than predictable results (e.g., increased transaction security). 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 in Gomez) paired with a cryptogram that is specifically generated to facilitate validation or authorization of a requested transaction. *See, e.g., Smith (EX1005), [0070]-[0071]; Gomez (EX1007), 8:11-23, 14:3-11, 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. *Smith (EX1005), [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 given the similarities in the systems.

B. Claims 19-21, 24

201. The combined teachings of Gill in view of Smith, Kay, and Gomez would have rendered obvious the features recited in claims 19-21 and 24 for the reasons described above for these same claims in Ground 1.

C. Claim 22:

1. *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.*

202. 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. *Smith (EX1005)*, [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 the MCA, issuer public key certificate, and ICC public key certificate. *Smith (EX1005)*, [0086] (“The mobile cloud account data 802 may include at least the issuer public key certificate, the ICC public key certificate, and the MCA.”).

203. In the combination, Gomez further teaches that the cryptogram can be generated based on a temporal signal including a “date/time of attempted use” (date, time of day,) or the instance of attempted use or “sequence value (or sequential number) of the attempted use” (sequence count or count of past transactions). *Gomez (EX1007)*, 7:17-27, 8:36-41, 10:58-11:6, 17:5-12. In addition, the cryptogram is based on a seed value that is “unique for each payment card,” such as a “unique customer key” (user key). *Gomez (EX1007)*, 7:26-48, Fig. 3. *Gomez (EX1007)*, 7:27-43 (“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.”); *see also*, Ground 2, Claim 18. It would have been similarly obvious to use a sequence count as an additional data element in generating the cryptogram. The use of transaction sequence counters in this way was well-known at the time. For example,

Hammad teaches using an application transaction counter as a dynamic data element to generate a dCVV (i.e., cryptogram). *Hammad*, 4:21-5:5. Accordingly, a POSITA would have been well aware of the benefits of using dynamic data elements, such as a sequence count, to generate a dynamic cryptogram for use in a financial transaction and, therefore, would have been motivated to do the same. *See* Ground 1, Claim 19; *see also Hammad*, 1:66-2:4, 4:45-60. A POSITA would have had a reasonable expectation of success in doing the same to generate the predictable result of increasing security given it is simply utilizing known techniques in a known way to improve similar systems (e.g., mobile payment systems).

D. Claim 23:

- 1. 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.***

204. As discussed above in Ground 1, the mobile device in the Gill-Smith-Kay combination generates and transmits payment information that includes a mobile card account number (MCA) and a payment cryptogram as taught in Smith. *Supra*, Ground 1, Claims 18(h)-(j). Further, and as described above in Claim 18 of Ground 2, it would have been obvious to further modify the Gill-Smith-Kay combination in view of Gomez such 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*, Claim 18.

205. In this context, the Gill-Smith-Kay-Gomez combination provides the additional features recited in Claim 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. *Smith (EX1005)*, [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 (plurality of static portions), as the corresponding digits from the RCA are fixed and the remaining digits likewise unchanged for the lifetime of the MCA. *Smith (EX1005)*, [0086]. The MCA is a token account number with a limited-duration expiration date for use in place of the RCA (issuer-provided information). *Smith (EX1005)*, (“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.”). As discussed in Section VI.C.1, the

use of a token, such as an MCA, in place of a PAN (e.g., RCA) was well known prior to the '520 Patent.

206. Moreover, Gomez teaches and the combination renders obvious that the cryptogram can be generated by combining a “date” and a “time” (*a plurality of dynamically-generated limited use portions*) to form a temporal signal used in calculating the cryptogram. *Gomez (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.

207. As another example, Gomez describes techniques for encoding the cryptogram into a sequence of characters (e.g., 32 characters). *See generally Gomez (EX1007)*, 14:36-17:13. A POSITA would have understood that with this type of encoding, each character represents a different portion of the message digest, and the characters (*a plurality of dynamically generated limited-use portions*) are combined to form the complete cryptogram. *Gomez (EX1007)*, 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. *Gomez (EX1007)*, 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). *Gomez (EX1007)*, 15:17-60; *see also*, 15:57-58 (“Such a code could be useful in a NFC environment”).

208. A POSITA would have been motivated to use and had a reasonable expectation of success of using an MCA and payment cryptogram generated from a temporal signal in this way for the same reasons discussed in the proposed combination of Ground 2, Claim 18.

XI. CONCLUSION

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

Dated: 6/23/2025

By: 

Curriculum Vitae

(June 2025)

B. Clifford Neuman

Education:

- Ph. D. Computer Science, June 1992, University of Washington
Thesis: The Virtual System Model, A Scalable Approach to Organizing Large Systems. Supervised by Professor Edward D. Lazowska
- M.S. Computer Science, May 1988, University of Washington
- S.B. Computer Science and Engineering June 1985, Massachusetts Institute of Technology
Thesis: Sentry, A Discretionary Access Control Server.
Supervised by Dr. David D. Clark

Employment:

- Research Scientist, Information Sciences Institute, University of Southern California, 1991-Present.
- Associate Division Director, Computer Networks Division, Information Sciences Institute, University of Southern California, 2001-June 2005.
- Director, Center for Computer Systems Security, University of Southern California, 2002-Present.
- Associate Professor of Computer Science Practice, Department of Computer Science, University of Southern California, 2016-.
- Research Associate Professor, Department of Computer Science, University of Southern California, 2008-2016.
- Research Assistant Professor, Department of Computer Science, University of Southern California, 1992-2008.
- Chief Scientist, CyberSafe Corporation, 1992 – 2001.
- Pre-Doctoral Research Associate, Department of Computer Science, University of Washington, 1987-1991.
- Project Athena, Massachusetts Institute of Technology 1985-1986.

- Systems Programmer, EECS Computer Facility, Massachusetts Institute of Technology 1982-1985.

Advisory Boards:

- NTT Communications Security Advisory Board, 2003-2006.
- Eyematic Corporation, 1999-2001.
- Net Research Inc / BayBuilder, 2000-2001.

Courses taught:

- DSci429/ENGR599, Security Privacy and Policy in the Age of the Internet. Fall 2019-2024.
- INF/DSci-523 Computer Systems Assurance, Spring 2016, Fall 2017-2024.
- INF 524 Distributed Systems and Network Security, Summer 2015
- INF-526 Secure System Administration, Summer 2016, Spring 2017, Spring 2021.
- INF 527 Secure Systems Engineering, Fall 2015
- INF/DSci-529 Privacy and Security for Informatics, Spring 2016-2025.
- CSci 530 Computer Security Systems (University of Southern California), Fall 2003-2024.
- CSci 555 Advanced Operating Systems (University of Southern California), Fall 1992-2003, 2006-2012, 2014, 2020.
- CSci599 Trusted Computing (University of Southern California), Spring 2007.
- CSci532 Hacking for Defense, Innovation for Defense Applications, Spring 2018-2020, Spring 2022- 2025.
- CSci 451 Operating Systems (for University of Washington Extension), Spring 1987.

Tutorials taught:

Electronic Payment Systems, presented at:

- Usenix Workshop on Electronic Commerce, New York, July 1995.
- Usenix Workshop on Electronic Commerce, Oakland, CA, November 1996.
- Internet Society Symposium on Network and Distributed Systems Security, March 1998.
- Usenix Workshop on Electronic Commerce, Boston, MA, September 1998.
- Internet Society Symposium on Network and Distributed Systems Security, February 1999.
- 8th International World Wide Web Conference, Toronto, Canada May 1999.

Web Security and Beyond: Protecting your Electronic Commerce Application, presented at:

- Internet Society Symposium on Network and Distributed Systems Security, March 1998.
- Internet Society Symposium on Network and Distributed Systems Security, February 1999.

Research Interests:

Dr. Neuman conducts research in distributed computer systems with emphasis on scalability and computer security, especially for cyber-physical systems and critical infrastructure.

In his research, Dr. Neuman works to design and develop scalable information, security, and computing infrastructure for the Internet. He is the principal designer of the Kerberos system, an encryption based authentication system used among other things as the primary authentication method for Microsoft's Windows 2000, XP and many other systems. He has used Kerberos as a base for more comprehensive computer security infrastructure providing authorization, accounting, and audit.

Recent research includes managing computer security policies in federated and coalition environments, and using policy as a unifying element for integrating all security services including authorization, audit, and intrusion detection with systems and applications. This work extends the application of trusted computing to protect mutually suspicious entities from one another and forms the basis for the TrustView security architecture.

Most recently, Dr. Neuman has focused on security for cyber-physical systems, with an emphasis on protection of critical infrastructure, including the power grid. Recent publications discuss cross-domain threat propagation in such systems, and mitigation techniques applied in both the cyber and physical domains.

Dr. Neuman has designed systems for network payment which build upon security infrastructure to provide a secure means to pay for services provided over the Internet. The NetCheque and NetCash systems, which are suitable for micropayments (payments on the order of pennies where the cost of clearing a credit card payment would be prohibitive). NetCheque provides accounting for the flow of funds through the system whereas NetCash supports anonymous transactions.

He is the principal designer of the Prospero system which is used to organize and retrieve information distributed on the Internet. The Prospero system applies the Virtual System Model to construct views of the information available on the network. Prospero is an embedded system that is used by several commercial products.

The Prospero Resource Manager (PRM) supports the management of computing resources in distributed systems. PRM provides multiple views of the available resources by supporting multiple resource managers, each controlling a subset of the resources in the system, independent of other managers of the same type. The functions of resource management are distributed across three types of managers: system managers, job managers, and node managers. The complexity of these management roles is reduced because each is designed to utilize information at an appropriate level of abstraction.

Awards

- InfoWorld Top Ten Technology Innovators, InfoWorld Magazine, February 2002.
- 2001 Usenix Software Tools User Group Award recipient for contributions to the development of Kerberos.
- DARPA Dynamic Coalitions Program 2003 award for excellence in academic research.
- Usenix Security 2022 Test of Time Award for Kerberos: An Authentication Service for Open Network Systems, Published in 1988 Winter USENIX Technical Conference Proceedings.

Memberships and Professional Activities:

Memberships

- Association for Computing Machinery (ACM) – Life member.
- Institute of Electrical and Electronic Engineers (IEEE) - Senior member
- IEEE Computer Society
- Internet Society (ISOC)
- Internet Engineering Task Force (IETF) - Participant
- Usenix Association

Program and General Chair

- Program Chair, Fourth Annual PKI R&D Workshop: “Multiple Paths to Trust”, Gaithersburg, MD. April 2005.
- General Chair, 2004 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2004.

- General Chair, 2003 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2003.
- Vice Program Chair, Security Track, International Conference on Distributed Computing Systems (ICDCS), Vienna Austria, 2002.
- Program Chair, 2002 Workshop on Accelerating Trustworthy Internetworking.
- General Chair, 2002 Internet Society Symposium on Network and Distributed System Security. San Diego, CA, February 2002.
- Program Chair, 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland. April 1997.
- Program Chair, 4th Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1997.
- Program Chair, 3rd Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1996.

Editorial and Publication Advisory Boards

- Guest Editor, Journal of High Speed Networking, special issue on managing security policies, 2006.
- Contributed/Edited section of Report of the Workshop on Responding to the Unexpected, February 27, 2002, New York City.
- Editorial Board, International Journal of Electronic Commerce, June 1996 - Present.
- Editorial Board, ACM Transaction on Information and Systems Security, 1998 – 2001.

Program Committees

- Program Committee, 2015 Industrial Control Systems Security Workshop at ACSAC, December 2015, Los Angeles.
- Program Committee, 2015 IEEE International Conference on Intelligence and Security Informatics, May 2015. Baltimore MD, USA.
- Steering Group, 2013 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2014.

- Program Committee, 2012 IEEE International Conference on Intelligence and Security Informatics, Washington DC, June 2012.
- Program Committee, ACM SIGKDD Workshop on Intelligence and Security Informatics 2012 (ISI-KDD 2012), Beijing China.
- Steering Group, 2013 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2013.
- Steering Group, 2012 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2012.
- Steering Group, 2011 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2011.
- Program Committee, 2010 ACM Symposium on Access Control Models and Technologies (SACMAT2010). Pittsburgh, June 2010.
- Program Committee, 2011 IEEE International Conference on Intelligence and Security Informatics. 011, Beijing China.
- Program Committee, 2010 IEEE International Conference on Intelligence and Security Informatics. May 2010, Vancouver, BC, Canada.
- Program Committee, 9th Symposium on Identity and Trust on the Internet (IDtrust 2010), Gaithersburg, MD, April 2010.
- Steering Group, 2010 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2010.
- Program Committee, 2009 ACM Symposium on Access Control Models and Technologies (SACMAT2009). Stresa, Italy, June 2009.
- Program Committee, 2009 IEEE International Conference on Intelligence and Security Informatics. June 2009, Dallas TX, USA.
- Program Committee, 8th Symposium on Identity and Trust on the Internet (IDtrust 2009), Gaithersburg, MD, April 2009..
- Steering Group, 2009 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2009
- 2008 IEEE International Conference on Intelligence and Security Informatics. June 2008, Taipei, Taiwan.

- Program Committee, 7th Seventh Symposium on Identity and Trust on the Internet (IDtrust 2008), Gaithersburg, MD, March 2008.
- Program Committee, 2007 IEEE International Conference on Intelligence and Security Informatics. May 2007, New Brunswick NJ. USA.
- Program Committee, 6th Annual PKI R&D Workshop, Gaithersburg, MD. April 2007.
- Steering Group, 2007 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2007.
- The First Workshop on Security, Trust and Privacy in Grid Environments STPG2008), at The 8th IEEE International Symposium on Cluster Computing and the Grid (CCGRID2008), 19-22 May 2008, Lyon, France
- 2006 IEEE Workshop on Policies for Distributed Systems and Networks (Policy2006), London Ontario, June 2006.
- 11th ACM Symposium on Access Control Models and Technologies (SACMAT2006). Lake Tahoe, June 2006.
- 2006 IEEE International Conference on Intelligence and Security Informatics. May 2006, San Diego USA.
- Fifth Annual PKI R&D Workshop, Gaithersburg, MD. April 2006.
- Second International Workshop on Security in Distributed Computing Systems. (in conjunction with 25th International Conference on Distributed Computing Systems ICDCS-2005), Columbus, OH, USA. June 2005.
- 2005 IEEE International Conference on Intelligence and Security Informatics. May 2005, Atlanta USA.
- 2004 IEEE International Conference on Intelligence and Security Informatics. June 2004, Tucson USA.
- 2003 IEEE International Conference on Intelligence and Security Informatics. June 2003, Tucson USA.
- IEEE Sixth International Workshop on Policies for Distributed Systems and Networks (Policy2005). June 2005, Stockholm Sweden..
- IEEE Fifth International Workshop on Policies for Distributed Systems and Networks (Policy2004). June 2004, New York.

- Steering Group, Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2001 to 2006.
- 21st International Conference on Distributed Computer Systems (ICDCS-21), Phoenix, AZ, April 2001,
- Ninth International World Wide Web Conference, Amsterdam, May 2000.
- 2001 Symposium on Applications and the Internet (SAINT), San Diego, CA, January 2001. (IEEE Computer Society).
- Eighth Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2000.
- Sixth ACM Conference on Computer and Communications Security, Singapore, November 1999.
- First ACM Conference on Electronic Commerce (EC-99), Denver, CO, November 1999.
- Eighth International World Wide Web Conference, Toronto, May 1999.
- Third International Conference on Financial Cryptography, Anguilla, British West Indies, February 1999.
- Seventh IEEE International Symposium on High Performance Distributed Computing, Chicago, IL, July 1998.
- First International Conference on Financial Cryptography, Anguilla, British West Indies, February 1997.
- Second Usenix Workshop on Electronic Commerce, Oakland, CA, November 1996.
- 1996 Conference on The Convergence of Telecommunications and Distributed Computing Technologies (TINA), Heidelberg, Germany, September 1996.
- Sixth Usenix Security Symposium, San Jose, CA July 1996.
- Third ACM Conference on Computer and Communications Security, New Delhi, India, March 1996.
- First Usenix Workshop on Electronic Commerce, New York City, July 1995.
- Second Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1995.

- Second ACM Conference on Computer and Communications Security, Fairfax VA, November 1994.
- First Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1994.
- First ACM Conference on Computer and Communications Security, Fairfax VA, November 1993.
- PSRG Workshop on Network and Distributed System Security, San Diego, CA, February 1993.

Other positions

- Panel member, National Research Council, CSTB Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government, October 2001.
- Publications Chair, 3rd ACM Conference on Computer and Communications Security, March 1996.

Publications (Journals):

- Wadhawan, Yatin, Clifford Neuman, and Anas AlMajali. "IGNORE: A Policy Server to Prevent Cyber-Attacks from Propagating to the Physical Domain." *Applied Sciences* 10, no. 18 (2020): 6236.
- AlMajali, Anas, Yatin Wadhawan, Mahmood S. Saadeh, Laith Shalalfeh, and Clifford Neuman. "Risk assessment of smart grids under cyber-physical attacks using Bayesian networks." *International Journal of Electronic Security and Digital Forensics* 12, no. 4 (2020): 357-385.
- Anas Al Majali, W. Yatin., Neuman, C, Saadeh. Mahmood, Shalalfeh. Laith. "Risk Assessment of Smart Grids under Cyber-physical Attacks using Bayesian Networks". Accepted in 2019 for *International Journal of Electronic Security and Digital Forensics*

- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks", MDPI: A special issue of Electronics: Cyber-Physical Systems. 2018.
- Anas AlMajali, Arun Viswanathan, Clifford Neuman, Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats. Electronics 6(1), 2016.
- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. (A retrospective) Electronic Networking: Research, Applications and Policy, 20(4): 408-419, Winter 2012. (refereed journal)
- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. A Tatyana Ryutov, Clifford Neuman, Li Zhou and Noria Foukia, *Initial Trust Formation in Virtual Organizations*, International Journal of Internet Technology and Security Transactions, 2007.
- Tatyana Ryutov, Clifford Neuman, Dongho Kim and Li Zhou. Integrated Access control and Intrusion Detection for Web Servers. IEEE Transaction on Parallel and Distributed Systems, Vol 14, No. 9, September 2003.
- R. Bajcsy, et. al. Cyber Defense Technology Networking and Evaluation, Communications of the ACM, March 2004.
- Tatyana Ryutov, Grig Gheorghiu, and Clifford Neuman, An Authorization Framework for Metacomputing Applications, Cluster Computing 2(1999), 165-175.
- B. Clifford Neuman and Theodore Ts'o. Kerberos: An Authentication Service for Computer Networks, IEEE Communications, 32(9):33-38. September 1994.
- B. Clifford Neuman and Santosh Rao. The Prospero Resource Manager: A scalable framework for processor allocation in distributed systems, Concurrency: Practice and Experience, 6(4):339-355, June 1994.
- B. Clifford Neuman. Enabling Commerce on the Internet, IEEE Computer29(4):91-92. April 1996.
- B. Clifford Neuman. Security, Payment, and Privacy for Network Commerce, IEEE Journal on Selected Areas in Communications, 13(8):1523-1531. October 1995.
- B. Clifford Neuman. The Prospero File System: A global file system based on the Virtual System Model. Computing Systems, 5(4):407-432, Fall 1992.

- Michael F. Schwartz, Alan Emtage, Brewster Kahle, and B. Clifford Neuman A Comparison of Internet Resource Discovery Techniques. Computing Systems, 5(4):461-493, Fall 1992.
- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. Electronic Networking: Research, Applications and Policy, 2(1): 30-37, Spring 1992. (refereed journal)

Publications (Other):

- C. Pandit, H. Kothari and C. Neuman, "Privacy in time of a pandemic," 2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275), 2020, pp. 1-6, doi: 10.1109/CMI51275.2020.9322737.
- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "PSP: A Framework to Allocate Resources to Power Storage Systems under Cyber-Physical Attacks", 5th International Symposium for ICS-SCADA Cyber Security. 2018.
- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "A Systematic Approach to Analyze Multiple Cyber-Physical Attacks on Smart Grid", International Conference on Cyber Security of Cyber Physical Systems. 2018.
- Yatin Wadhawan , Dr. Clifford Neuman. "RL-BAGS: A Tool for Smart Grid Risk Assessment", International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). 2018.
- Wadhawan, Yatin and Neuman, Clifford, "BAGS: A Tool to Quantify Smart-Grid Resilience", September 2017, In Proceedings of the 4th International Workshop on Cyber-Physical Systems at the Federated Conference on Computer Science and Information Systems, Prague, Czech Republic.
- Wadhawan, Yatin and Neuman, Clifford, and AlMajali, Anas "Analyzing Cyber-Physical Attacks on Smart Grid Systems", 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), April 2017, Pittsburgh.
- Wadhawan, Yatin and Neuman, Clifford, "Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology", ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC) 2016.
- Yatin Wadhawan and Clifford Neuman. Defending Cyber-Physical Attacks on Oil Pipeline Systems: A Game-Theoretic Approach Yatin Wadhawan and

Clifford Neuman. International Workshop on AI for Privacy and Security (PRAISE) from 29 August to 2 September 2016, at the Hague, Netherlands.

- Yatin Wadhawan and Clifford Neuman, A Roadmap to Evaluate Resilience of Oil and Gas Cyber-Physical Systems. 2015 ACSAC Workshop on Industrial and Control System Security, Los Angeles, December 2015.
- Tatyana Ryutov, Anas AlMajali, Clifford Neuman, Modeling Security Policies for Mitigating the Risk of Load Altering Attacks on Smart Grid Systems, in Proceedings of the 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES) (IEEE), Seattle, April 2015.
- Anas AlMajali, Eric Rice, Arun Viswanathan, Kymire Tan, Clifford Neuman, *A Systems Approach to Analysing Cyber-Physical Threats in the Smart-Grid*, in Proceedings of the 4th International Conference on Smart Grid Communications (IEEE SmartGridComm), Vancouver, October 2013.
- Arun Viswanathan, Kymie Tan, Clifford Neuman, *Deconstructing the Assessment of Anomaly-Based Intruding Detectors for Critical Applications*, in Proceedings of the 16th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID2013) St. Lucia, October 2013.
- Hashem Alayed, Fotos Frangoudes, and Clifford Neuman, *Behavioral-Based Cheating Detection in Online First Person Shooters using Machine Learning Techniques*, in Proceedings of IEEE 2013 Conference on Computational Intelligence in Games, Niagara Falls, Canada, August 2013.
- Anas AlMajali, Arun Viswanathan, and Clifford Neuman, *Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack*, in Proceedings of the 5th Workshop on Cyber Security Experimentation and Test (CSET'12) Bellevue, Washington, August 2012.
- Clifford Neuman and Kymie Tan, *Mediating Cyber and Physical Threat Propagation in Security Smart Grid Architecture*, in Proceedings of the 2nd International Conference on Smart Grid Communications (IEEE SmartGridComm), Brussels, October 2011.

Clifford Neuman, *Challenges in Security for Cyber-Physical Systems*, DHS Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, July 22-24, 2009.

- Arun Viswanathan, Clifford Neuman, Secure System Views: A new Paradigm for Secure Usable Systems. USC-ISI Technical Report Number ISI-TR-654, January 2009.
- Terry Benzel, Robert Braden, Dongho Kim, Clifford Neuman, Anthony Joseph, Keith Sklower, Ron Ostrenga, Stephen Schwab, Design Deployment

and use of the DETER testbed.. In Proceedings of the DETER Community Workshop on Cyber-Security and Test, August 2007, Boston.

- Tatyana Ryutov, Clifford Neuman, A Trust Based Approach for Improving Data Reliability in Industrial Sensor Networks, in proceedings of the joint ITRUST and PST Conference on Privacy, Trust Management, and Security, New Brunswick Canada, August 2007. Also, ISI-TR-631, January 2007.
- Tatyana Ryutov, Clifford Neuman, Situational Identity: A Person-centered Identity Management Approach, USC ISI Technical report ISI-TR-630, January 2007.
- Tatyana Ryutov, Clifford Neuman, Ronak Shah, Automated Management of Vulnerability Mitigation Prescriptions. USC ISI Technical report ISI-TR-630, January 2007.
- Clifford Neuman, Managing Multiple Perspectives on Trust, *in proceedings of the 2007 Cyber Security and Information Infrastructure Research Workshop*, Oak Ridge Tennessee, May 2007.
- Clifford Neuman. *Understanding Trust in SCADA Systems*. Proceedings of Beyond SCADA: Network Embedded Control for Cyber-Physical Systems. Pittsburgh, November 9, 2006. (Refereed Workshop Position Statement)
- Sukumal Kitisin and Clifford Neuman. *Reputation-Based Trust-Aware Recommender System*. Proceedings of the 2nd IEEE Workshop on the Value of Security Through Collaboration (SECOVAL), September 2006, Baltimore. (refereed workshop)
- Ho Chung and Clifford Neuman. *Modeling the Relative Strength of Security Protocols*. Proceedings of the 2nd ACM CCS Workshop on Quality of Protection, October 2006, Alexandria VA. (refereed workshop)
- Clifford Neuman, Chinmay Shah, Kevin Lahey. *Running Live Self-Propagating malware on the DETER Testbed*. Proceedings of the DETER Community Workshop, Arlington VA, June 2006.
- Noria Foukia, Liz Zhou and Clifford Neuman. *Multilateral Decision for Collaborative Defense Against Unsolicited Bulk e-mail*. Proceedings of the 4th International Conference on Trust Management. Pisa, Italy, May 2006. (refereed conference)
- Terry Benzel, Bob Braden, Dongho Kim, Clifford Neuman Anthony Joseph and Keith Sklower Ron Ostrenga and Stephen Schwab, *Experience with DETER: A Testbed for Security Research*. Second IEEE Conference on testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), March 2006, Barcelona. (refereed conference)

- L. Li, I. Hamadeh, S. Jiwasurat, G. Kesidis, P. Liu, C. Neuman, *Emulating Sequential Scanning Worms on the DETER Testbed*, In Proceedings of 2nd International IEEE/CreateNet Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), March 2006. (refereed conference)
- Tatyana Ryutov, Clifford Neuman, Li Zhou and Noria Foukia, *Establishing Agreements in Dynamic Virtual Organizations*, in Proceedings of the Workshop on the Value of Security through Collaboration, part of IEEE SecureComm, September 2005, Athens. (refereed workshop)
- Tatyana Ryutov, Clifford Neuman, Noria Foukia, Travis Leithead, Kent Seamons, Li Zhou, *Adaptive Trust Negotiation and Access Control for Grids*. 6th IEEE/ACM International Workshop on Grid Computing, Seattle, November 2005. (refereed workshop)
- Sultan Almuhammadi and Clifford Neuman, "Security and Privacy using One-Round Zero Knowledge Proofs", 7th IEEE Conference on E-Commerce Technology, Munich, July 2005. (refereed conference)
- Tatyana Ryutov, Li Zhou, Clifford Neuman, Travis Leithead, and Kent E. Seamons, "**Adaptive Trust Negotiation and Access Control**," in *Proceedings of the ACM Symposium on Access Control Models and Technologies* (SACMAT'05), Stockholm, June 1-3, 2005. (refereed conference)
- Tatyana Ryutov, Clifford Neuman, Dongho Kim and Li Zhou. Integrated Access control and Intrusion Detection for Web Servers. In proceedings of the 23rd International Conference on Distributed Computing Systems, Providence, Rhode Island, May 2003. (refereed conference)
- Tatyana Ryutov, Clifford Neuman and Dongho Kim. Dynamic Authorization and Intrusion Response in Distributed Systems. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition (DISCEX III), April 2003. (refereed conference)
- Tatyana Ryutov and Clifford Neuman. The Specification and Enforcement of Advanced Security Policies. To be published In Proceedings of the Third International Conference on Policies for Distributed Systems and Networks (POLICY 2002), June 2002, in Monterey, California. (refereed conference)
- Tatyana Ryutov and Clifford Neuman, The Set and Function Approach to Modeling Authorization in Distributed Systems, in Proceedings of the Information Assurance in Computer Networks Methods, Models, and

Architectures for Network Security, May 2001, St. Petersburg, Russia, 189-206. (refereed conference)

- Tatyana Ryutov and Clifford Neuman, Representation and Evaluation of Security Policies for Distributed System Services, in Proceedings of the DARPA Information Survivability Conference and Exposition, January 2000. Hilton Head, SC. (refereed conference)
- Sukumal Imudom and B. Clifford Neuman, A Framework Supporting Collaborative Filtering for Internet Information, AAAI-98 Workshop on Recommender Systems, Madison, WI, July 1998. (refereed conference)
- G. Gheorghiu, T. Ryutov, and B. Clifford Neuman, Authorization for Metacomputing Applications, in Proceedings of the 7th IEEE Symposium on High Performance Distributed Computing, Chicago, IL, July 1998. (refereed conference)
- Sung-Wook Ryu and B. Clifford Neuman, Garbage Collection for Distributed Persistent Objects, in Proceedings of the Workshop on Compositional Software Architectures, Monterey, CA January 1998. (referred conference)
- B. Clifford Neuman and Gennady Medvinsky. Requirements for Network Payment: The NetCheque Perspective In Proceedings of IEEE COMPCON'95. March 1995. (referred conference)
- Clifford Neuman and Genaddy Medvinsky, *NetCheque, NetCash, and the Characteristics of Internet Payment Services*, MIT Workshop on Internet Economics, March, 1995
- Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman. Endorsements, Licensing, and Insurance for Distributed System Services, In Proceedings of 2nd the ACM Conference on Computer and Communication Security. November 1994. (refereed conference)
- B. Clifford Neuman. How to Trust a Distributed System. In Proceedings of the National Computer Security Conference. Baltimore MD, October 1994. (invited conference)
- Gennady Medvinsky and B. Clifford Neuman. Electronic Currency for the Internet, *Electronic Markets* 3(9/10):23-24, October 1993. Also appeared in *Connexions* 8(6):19-23, June 1994. (unrefereed journal)
- Gennady Medvinsky and B. Clifford Neuman. NetCash: A design for practical electronic currency on the Internet. In Proceedings of the 1st ACM Conference

on Computer and Communication Security. November 1993. (refereed conference)

- B. Clifford Neuman, Steven Seger Augart, and Shantaprasad Upasani. Using Prospero to support integrated location independent computing. In Proceedings of the Symposium on Mobile and Location Independent Computing, August 1993. (refereed conference)
- B. Clifford Neuman. Prospero: A base for building information infrastructure. In Proceedings of INET'93, August 1993. (referred conference)
- B. Clifford Neuman and Santosh Rao. Resource Management for Distributed Parallel Systems. In Proceedings of the 2nd International Symposium on High Performance Distributed Computing, July 1993. (refereed conference)
- B. Clifford Neuman. Proxy-Based Authorization and Accounting for Distributed Systems. In Proceedings of the 13th International Conference on Distributed Computing Systems, pages 283-291, May 1993. (refereed conference)
- B. Clifford Neuman and Stuart G. Stubblebine. A Note on the Use of Timestamps as Nonces. Operating Systems Review, 27(2):10-14, April 1993. (unrefereed)
- B. Clifford Neuman. Prospero: A virtual directory service for the Internet, Connexions 6(7):2-9, July 1992. (unrefereed)
- B. Clifford Neuman. The Prospero File System: A global file system based on the Virtual System Model. In Proceedings of the 1st Usenix Workshop on Filesystems May 1992. (refereed conference)
- B. Clifford Neuman. Protection and Security Issues for Future Systems. In Proceedings of the Workshop on Operating Systems of the 90s and Beyond . Dagstuhl Castle, Germany. July 1991.(invited workshop)
- B. Clifford Neuman. The Need for Closure in Large Distributed Systems. Operating Systems Review, 23(4): 28-30, October 1989. (unrefereed)
- B. Clifford Neuman. Workstations and the Virtual System Model. In Proceedings of the 2nd IEEE Workshop on Workstation Operating Systems, pages 91-95, September 1989. (refereed conference)
- B. Clifford Neuman and Jennifer G. Steiner. Authentication of Unknown Entities on an Insecure Network of Untrusted Workstations. In Proceedings of the Usenix

Workshop on Workstation Security, Portland, OR. August 1988. (refereed conference)

- J. G. Steiner, B. Clifford Neuman, and J.I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In Proceedings of the Winter 1988 Usenix Conference. February, 1988. (Version 4) (refereed conference)
- B. Clifford Neuman and Wayne Yamamoto. Adding Packet Radio to the Ultrix Kernel. In Proceedings of the Winter 1988 Usenix Conference February, 1988. (refereed conference)
- B. Clifford Neuman. Packet Radio and IP for the Unix Operating System. In Proceedings of the Sixth ARRL Computer Networking Conference, Redondo Beach, CA. August, 1987. (refereed conference)

Book Chapters:

- Sanjay Goel, Stephen F. Bush, Clifford Neuman, Smart Grid Security (Chapter 10) in IEEE Vision for Smart Grid Communications: 2030 and Beyond, IEEE Standards Association, 2013.
- Frank Siebenlist, Nataraj Nagaratnam, Von Welch, Clifford Neuman, Security for Virtual Organizations: Federating Trust and Policy Domains. in The GRID 2: Blueprint for a New Computing Infrastructure (edited by Kesselman and Foster), Morgan, Kauffman Publishers, 2004. (invited)
- Clifford Neuman, Security and Privacy, in Cancer Informatics: Essential Technologies for Clinical Trials, Springer-Verlag Inc, 2002. (invited)
- B. Clifford Neuman, Security, Accounting, and Assurance, in The GRID: Blueprint for a New Computing Infrastructure (edited by Kesselman and Foster), Morgan, Kauffman Publishers, 1999. (invited)
- B. Clifford Neuman and Gennady Medvinsky, Internet Payment Services, in Internet Economics, MIT Press. 1997. (refereed conference -> book)
- Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman, Endorsements, Licensing, and Insurance for Distributed Services, in Internet Economics, MIT Press. 1997. (refereed conference -> book)
- B. Clifford Neuman, A Flexible Framework for Network Payment, in Readings in Electronic Commerce, Addison-Wesley. 1996. (invited)

- B. Clifford Neuman, Scale in Distributed Systems, Readings in Distributed Computing Systems, IEEE Computer Society Press, 1994. (refereed book chapter)
- John T. Kohl, B. Clifford Neuman, and Theodore Y. T'so, The Evolution of the Kerberos Authentication System. In Distributed Open Systems, pages 78-94. IEEE Computer Society Press, 1994. (refereed conference -> book)

Theses, Technical Reports, and Working Documents:

- Clifford Neuman, Tom Yu, Sam Hartman, Ken Raeburn, The Kerberos Network Authentication System, RFC 4120. July 2005 (standards specification).
- Dongho Kim and B. Clifford Neuman. Reconstructing Interconnections on Disconnected Mobile Hosts, ISI Technical Report ISI-TR-528, University of Southern California / Information Sciences Institute, April 2000
- John Kohl and B. Clifford Neuman. The Kerberos Network Authentication Service (Version 5). Internet Request for Comments RFC-1510. September 1993.
- B. Clifford Neuman, The Virtual System Model: A Scalable Approach to Organizing Large Systems, Ph.D. Thesis, University of Washington, Department of Computer Science and Engineering Technical Report 92-06-04, June 1992.
- B. Clifford Neuman. Proxy-Based Authorization and Accounting for Distributed Systems. Technical Report 91-02-01, Department of Computer Science and Engineering, University of Washington, March 1991.
- B. Clifford Neuman. The Virtual System Model: A Scalable Approach to Organizing Large Systems (A Thesis Proposal). Technical Report 90-05-01, Department of Computer Science and Engineering, University of Washington, May 1990.
- B. Clifford Neuman. The Virtual System Model for Large Distributed Operating Systems. Technical Report 89-01-07, Department of Computer Science, University of Washington, April, 1989.
- S.P. Miller, B. C. Neuman, J. I. Schiller, and J.H. Saltzer. Section E.2.1: Kebreros Authentication and Authorization System. Project Athena Technical Plan, MIT Project Athena, Cambridge, Massachusetts, October 1988. (Describes Version 4)
- B. Clifford Neuman. Sentry: A Discretionary Access Control Server. Bachelor's Thesis, Massachusetts Institute of Technology, June 1985.

Students who completed Ph.D. under Dr. Neuman

- Ho Chung, - Ph.D. USC 2009. Modeling the Relative Strength of Security. Now a researcher at Samsung.
- Li Zhou, - Ph.D. USC 2006. Negotiation of Multilateral Security Decisions. Now a researcher at Microsoft, Redmond WA.
- Sultan Almuhammadi – Ph.D. USC 2005, Security and Privacy Using One-Round Zero-Knowledge Proofs, now faculty at King Fahd University, Saudi Arabia.
- Noria Foukia (postdoc at USC 2004/05), currently Lecturer at University of Otago, Dunedin NZ.
- Xuhua Ding, Ph.D. USC 2003 (co-advisor with Gene Tsudik). Fine-grained control of security services. Now assistant professor at Singapore Management University.
- Yongdae Kim, Ph.D. USC 2002 (co-advisor with Gene Tsudik). Group Key Agreement: Theory and Practice, now faculty at University of Minnesota.
- Tatyana Ryutov - Ph.D. USC 2002, The Condition-driven Authorization Model for Distributed System Services, Now at USC Information Sciences Institute
- Dongho Kim – Ph.D. USC 2001, Reconstructing Interconnections on Disconnected Mobile Hosts, Now at USC Information Sciences Institute
- Sukumal Imudom – Ph.D. USC 2001, Distributed Annotation Framework Supporting Collaborative Filtering of Information, now faculty at Kasetsart University, Thailand.
- Eul Gyu Im - Ph.D. USC 2001, A Flexible Framework for Replication in Distributed Systems, now at National Security Research Institute, South Korea.
- Gennady "Ari" Medvinsky - Ph.D. USC 1996, Electronic Payment Services To CyberSafe Corporation, to Excite - @ Home, to Keen.com, to Microsoft.
- Santosh Rao - Ph.D. USC 1996, Resource Management, Parallel Debugging, and PRM, Now at Veritas Software
- Brenda Timmerman - Ph.D. USC - Traffic Flow Confidentiality, Faculty at Cal State Northridge
- Sung-Wook Ryu - Ph.D. USC - Garbage Collection for Prospero, Now at Veritas Software

- Konstadinos Kutsikos – Ph.D. USC - Electronic Commerce and Economics, now faculty at University of the Aegean, Greece.
- Anas Almajali – Ph.D. USC – Analysis of Threats in Cyber-Physical Systems. Now faculty at Hashemite University, Jordan.
- Hashem Alayed – Ph.D. USC – Security in Online games, now faculty at King Saud University, Saudi Arabia.
- Arun Viswanathan – Ph.D. USC – Situational Awareness and Intrusion Detection in Cyber-physical systems. Now working for NASA Jet Propulsion Lab.
- Yatin Wadhawan – Ph.D. USC - Analyzing Cyber-Physical Attacks on Industrial Control Systems. Now working at Microsoft.
- Abdulla Alwabel – Ph.D. USC Overcoming Challenges Facing Malware Behavioral Analysis.