

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

CARDWARE INC.
Patent Owner

Case No. IPR2025-01149
U.S. Patent No. 11,176,538

**DECLARATION OF DR. CLIFFORD NEUMAN
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 11,176,538**

TABLE OF CONTENTS

I.	INTRODUCTION.....	11
A.	EDUCATIONAL BACKGROUND AND PROFESSIONAL EXPERIENCE	11
II.	MATERIALS CONSIDERED	14
III.	OVERVIEW AND LEGAL STANDARDS.....	15
A.	PERSON OF ORDINARY SKILL IN THE ART	16
B.	OBVIOUSNESS	17
C.	CLAIM CONSTRUCTION	22
D.	PRINTED SUBJECT MATTER	22
IV.	LEVEL OF A PERSON OF ORDINARY SKILL	23
V.	OVERVIEW OF THE '538 PATENT.....	24
A.	SUMMARY OF THE '538 PATENT	24
B.	FIELD OF ENDEAVOR	24
C.	PROBLEM PURPORTEDLY SOLVED BY THE INVENTORS OF THE '538 PATENT	25
D.	THE PROSECUTION HISTORY OF THE '538 PATENT.....	26
VI.	BACKGROUND OF TECHNOLOGY	26
A.	THE EVOLUTION OF PAYMENT CARDS.....	27
1.	<i>Magnetic Stripe Cards</i>	<i>27</i>
2.	<i>Smart/Chip Cards</i>	<i>30</i>
3.	<i>Europay, MasterCard, and Visa (EMV) Standard.....</i>	<i>31</i>
B.	CONTACTLESS PAYMENTS	31
1.	<i>Near Field Communications.....</i>	<i>31</i>
	<i>Active Mode</i>	<i>33</i>
	<i>Passive Mode.....</i>	<i>35</i>
2.	<i>Contactless EMV Payment Cards.....</i>	<i>36</i>
3.	<i>Mobile Devices and Mobile Wallets</i>	<i>37</i>
VII.	CARD EMULATION MODE	40
A.	CONTACTLESS ATMS	42

B.	PAYMENT CREDENTIAL SECURITY FEATURES	46
1.	<i>Alternatives to a Payment Account Number (PAN)</i>	46
2.	<i>Alternatives to Static Card Verification Values</i>	50
VIII.	SUMMARY OF UNPATENTABILITY	52
IX.	OVERVIEW OF THE PRIOR ART.....	52
A.	LIN.....	52
1.	<i>Lin is Analogous</i>	53
B.	SMITH	55
1.	<i>Smith is Analogous</i>	56
C.	VARADARAJAN	57
1.	<i>Varadarajan is Analogous</i>	58
D.	HAMMAD	58
1.	<i>Hammad is Analogous</i>	60
E.	KRANZLEY	61
1.	<i>Kranzley is Analogous</i>	62
X.	GROUND 1: LIN, SMITH, VARADARAJAN, AND HAMMAD	64
A.	CLAIM 1	64
1.	<i>1(Pre): A method of performing a payment transaction, the method comprising:</i>	64
2.	<i>1(a): receiving an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user; and, ...</i>	65
3.	<i>1(b): wherein [] authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface, a gesture sensor, a motion sensor, and a biometric sensor; and, ...</i>	67
4.	<i>1(c): receiving a request for a transaction payment at said electronic device via an NFC interface of the device; and, ...</i>	69

5. *1(d): displaying, on a display of the device, [the] request and at least a portion of an original static issuer-supplied payment account information associated with a [selected] payment method, for a user selection in paying the [] request; and, ... 71*
6. *1(e): retrieving from a memory attached to a processor of the device, a device-specific static limited-use payment information, associated with said selected payment method; and, ... 73*
 - a) Lin's Teachings.....73
 - b) Smith's Teachings.....74
 - c) Motivation to Combine 77
7. *1(f): dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method; and, ... 81*
 - a) Varadarajan's Teachings 81
 - b) Motivation to Combine 83
8. *1(g): using said limited-use payment information[s] in place of at least a portion of said selected original issuer-supplied payment information for the transaction; and, ... 86*
9. *1(h): combining [] said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information; and, " 87*
10. *1(i): transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction; and, ... 87*
11. *1(j): receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the [] complete device payment information by a payment processor authority and a payment issuer authority; and, ... 90*

a)	Hammad's Teachings.....	92
b)	Motivation to Combine	94
12.	<i>1(k): visually conveying the transaction payment authorization status via a user-interface displayed on said display.</i>	<i>95</i>
B.	CLAIM 2	97
1.	<i>2: The method of claim 1, further comprising receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.</i>	<i>97</i>
C.	CLAIM 3	98
1.	<i>3: The method of claim 1, further comprising receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device.</i>	<i>98</i>
D.	CLAIM 4	100
1.	<i>4(a): The method of claim 3, wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment transactions performed by said device, in place of said selected issuer-payment information; and, ...</i>	<i>100</i>
2.	<i>4(b): wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.....</i>	<i>101</i>
E.	CLAIM 5	102
1.	<i>5(a): The method of claim 3, wherein the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information; and, ...</i>	<i>102</i>
a)	Hammad's Teachings.....	102

b)	Motivation to Combine	104
2.	<i>5(b): wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction; and, ...</i>	<i>107</i>
3.	<i>5(c): wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device; and, ...</i>	<i>108</i>
4.	<i>5(d): a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number; and, ...</i>	<i>109</i>
5.	<i>5(e): an adjusting of said transaction sequence counter count on a per transaction basis; and, ...</i>	<i>111</i>
6.	<i>5(f): an authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching.</i>	<i>112</i>
F.	CLAIM 7	113
1.	<i>7: The method of claim 3, wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including: ... a transaction payment amount, ... a merchant information, an original issuer payment account information, an original payment issuer information, ... [and] a payment completion status.</i>	<i>113</i>
G.	CLAIM 8	114

1.	<i>8(a): The method of claim 1, wherein the generating the limited-use payment information is comprising: a device-specific account number; and,.....</i>	<i>114</i>
2.	<i>8(b): a device-internal transaction sequence counter count; and, ...</i>	<i>114</i>
3.	<i>8(c): an information unique to the user and device which does not pass in the transaction; and, ...</i>	<i>114</i>
4.	<i>8(d): at least one payment authority-supplied information which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements, and.....</i>	<i>115</i>
5.	<i>8(e): wherein said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information.</i>	<i>116</i>
H.	CLAIM 9	117
1.	<i>9: The method of claim 8, wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number, capable of passing in at least a portion of the device transaction payment information.....</i>	<i>117</i>
I.	CLAIM 10	118
1.	<i>10: The method of claim 9, wherein the generating the limited-use payment information further utilizes a secure combination with a device key, and a payment issuer secret.....</i>	<i>118</i>
J.	CLAIM 11	119

1.	<i>11(a): The method of claim 1, wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of:</i>	119
2.	<i>11(b) a device payment transaction sequence counter count, and</i>	119
3.	<i>11(c): at least one of a set comprising:</i> <i>a device-specific internal information associated with said device and also known to a payment processing authority; and,.....</i> <i>at least one payment processing authority-specific information provided by a payment processing authority; and,.....</i> <i>a payment issuer specific information provided by a payment issuer.</i>	119 119 119 119
K.	CLAIM 12	119
1.	<i>12: The method of claim 1, wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information.</i>	119
L.	CLAIM 13	120
1.	<i>13: The method of claim 1, wherein the generating the limited-use payment information utilizes a merchant identifying information.</i>	120
M.	CLAIM 14	120
1.	<i>14: The method of claim 1, wherein the generating the limited-use payment information utilizes a transaction facility information.</i>	120
N.	CLAIM 15	121
1.	<i>15: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment amount.</i>	121
O.	CLAIM 16	121

1.	<i>16: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment facility type.</i>	<i>121</i>
P.	CLAIM 17	122
1.	<i>17: The method of claim 1, wherein the generating the limited-use payment information utilizes an online transaction information.</i>	<i>122</i>
Q.	CLAIM 18	122
1.	<i>18(a): The method of claim 1, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number; and.....</i>	<i>122</i>
2.	<i>18(b): wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number, via the incrementing of said transaction sequence counter count on a per-transaction basis, and using said updated transaction sequence counter count in said generation of said cryptogram; and, ...</i>	<i>123</i>
3.	<i>18(c): wherein said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device.....</i>	<i>123</i>
XI.	GROUND 2: CLAIM 6 IS OBVIOUS OVER LIN, SMITH, VARADARAJAN, HAMMAD AND KRANZLEY	124
A.	CLAIM 6	124
1.	<i>6(a): The method of claim 3, wherein the generating the limited-use payment information further utilizes a secure combination of said information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information; and, ...</i>	<i>124</i>

2.	<i>6(b): a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority; and, ...</i>	<i>124</i>
3.	<i>6(c): a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid; and,.....</i>	<i>125</i>
4.	<i>6(d): a conveying of said validation result as a declining or accepting of said transaction payment; and, ...</i>	<i>126</i>
5.	<i>6(e): upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction.</i>	<i>126</i>
	a) Kranzley's Teachings.....	127
	b) Motivation to Combine	127
XII.	CONCLUSION.....	130

I, Dr. Clifford Neuman declare the following:

I. INTRODUCTION

1. I have been retained by counsel for Petitioner 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. 11,176,538 (the “’538 Patent”). I understand that the Challenged Claims are 1-18, 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. For this work, I have been asked to review U.S. Patent No. 11,176,538 (“’538 Patent”) (EX1001) and the ’538 Patent’s prosecution history (“’538 File History”) (EX1002). My opinions support Apple Inc.’s petition for *Inter Partes* Review, which challenges all 30 claims of the ’538 Patent (“Challenged Claims”). In developing my opinions relating to the ’538 Patent, I have considered the materials cited or discussed herein, including those listed below.

Exhibit	Description
1001	U.S. Patent No. 11,176,538 (the “’538 Patent”)
1002	File History of the ’538 Patent (“the ’538 File History”)
1004	WO Publn. No. 2010/039337 (“Lin”)
1005	U.S. Pub. No. 2010/0125508 (“Smith”)

1006	U.S. Pub. No. 2011/0184876 (“Varadarajan”)
1007	U.S. Patent No. 7,740,168 (“Hammad”)
1008	U.S. Pub. No. 2010/0125509 (“Kranzley”)
1009	U.S. Provisional Application No. 60/884,089 (“Hammad ’089 Provisional”)

11. I have considered these materials from the viewpoint of a POSITA as of the priority date of the ’538 Patent. For the purposes of this declaration, I apply the priority date of the ’538 Patent as 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 ’538 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 ’538 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 '538 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 '538 Patent, the prior art cited herein, and the ordinary skill factors described in this section, a POSITA in the field of the '538 Patent at the time of the earliest possible priority date, March 15, 2013, would have been knowledgeable in the fields of payment processing and/or digital authentication systems. In my experience working, teaching, and performing research in this field, most workers of ordinary skill in the art at the time of the earliest possible priority date, March 15, 2013, would have had 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 and online technologies. 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 '538 PATENT

A. Summary of the '538 Patent

31. The '538 Patent generally describes emulating a standard credit card with a device “capable of generating a programmed magnetic field of alternating polarity...when used in electronic credit card readers.” *'538 Patent (EX1001)*, Abstract. The '538 Patent also describes “generating a limited-duration credit card number...which is limited in scope to a predetermined number of authorized transactions.” *'538 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. *'538 Patent (EX1001)*, 2:42-62.

B. Field of Endeavor

32. 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.

33. The '538 Patent defines the “Field of the Invention” as relating to “electronic or smart multi-function electronic devices and, more specifically, to more secure, smart credit card devices.” *'538 Patent*, 1:24-28. After reviewing the '538 Petition, it is my opinion that a POSITA would understand that the field of endeavor of the '538 Patent includes secure payment cards, devices and systems.

C. Problem Purportedly Solved by the Inventors of the '538 Patent

34. 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 '538 Patent and determine the problem that the inventors were trying to solve.

35. The '538 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.” *'538 Patent*, 1:63-67. The '538 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.” *'538 Patent*, 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.” *'538 Patent*, 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.” *'538 Patent*, 2:25-29. Thus, a POSITA would understand that the '538 Patent is directed to solving the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

D. The Prosecution History of the '538 Patent

36. I have reviewed the prosecution history for the '538 Patent. Notably, there were no substantive rejections based on prior art at any point during the review of the application that issued as the '538 Patent. *See generally '538 File History (EX1002)*. The examiner noted that available prior art references Brown, Lee, and Mullen each taught dynamic credit cards. *See '538 File History (EX1002)*, Notice of Allowability. But in the examiner's view, these references did not teach the limitations required by the claims of the application that issued as the '538 Patent. *See '538 File History (EX1002)*, Notice of Allowability.

VI. BACKGROUND OF TECHNOLOGY

37. 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 '538 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 '538 Patent.

38. 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 '538 patent.

39. 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.

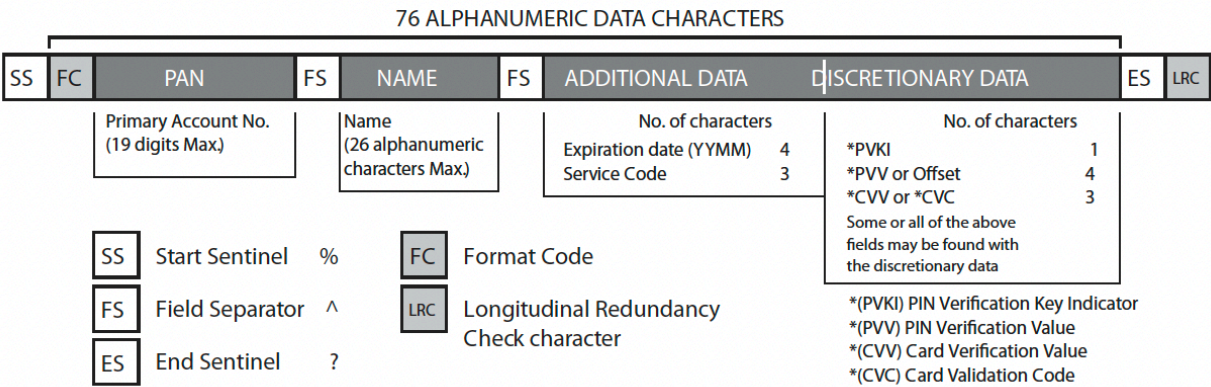
A. The Evolution of Payment Cards

1. Magnetic Stripe Cards

40. 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.

41. 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

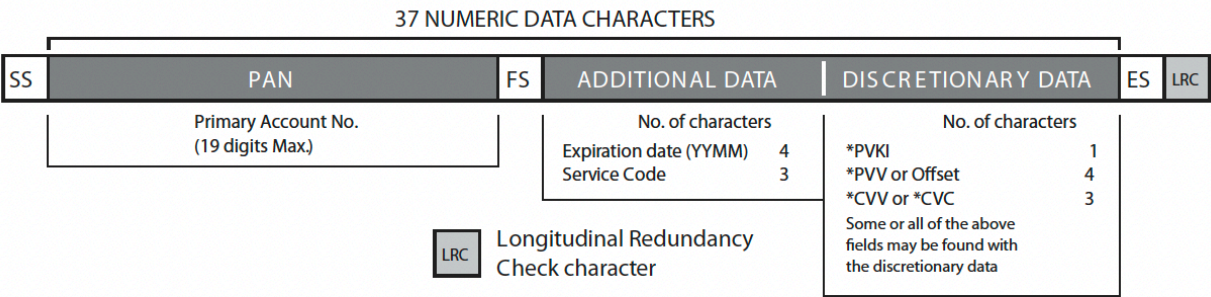


MagTek (EX1022), 1. On a card’s track:

“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.

42. 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.

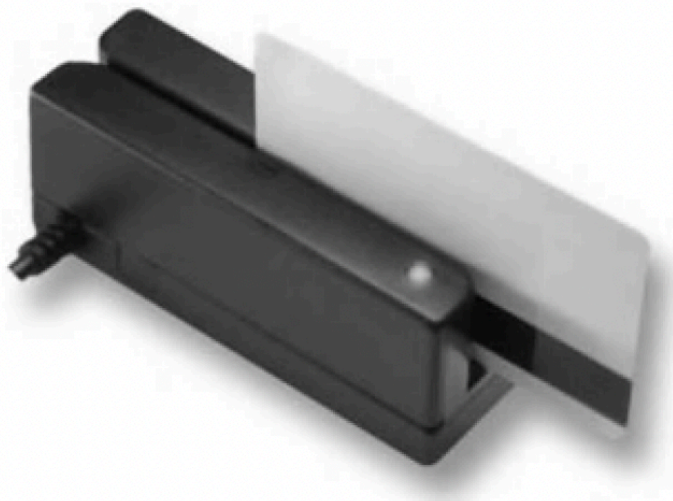


Figure 2.15 Magnetic stripe card.

Coskun (EX1021), Figure 2.15.

43. “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*

44. 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.

45. 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*

46. 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*

47. 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.

48. 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.

49. 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.

50. 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.

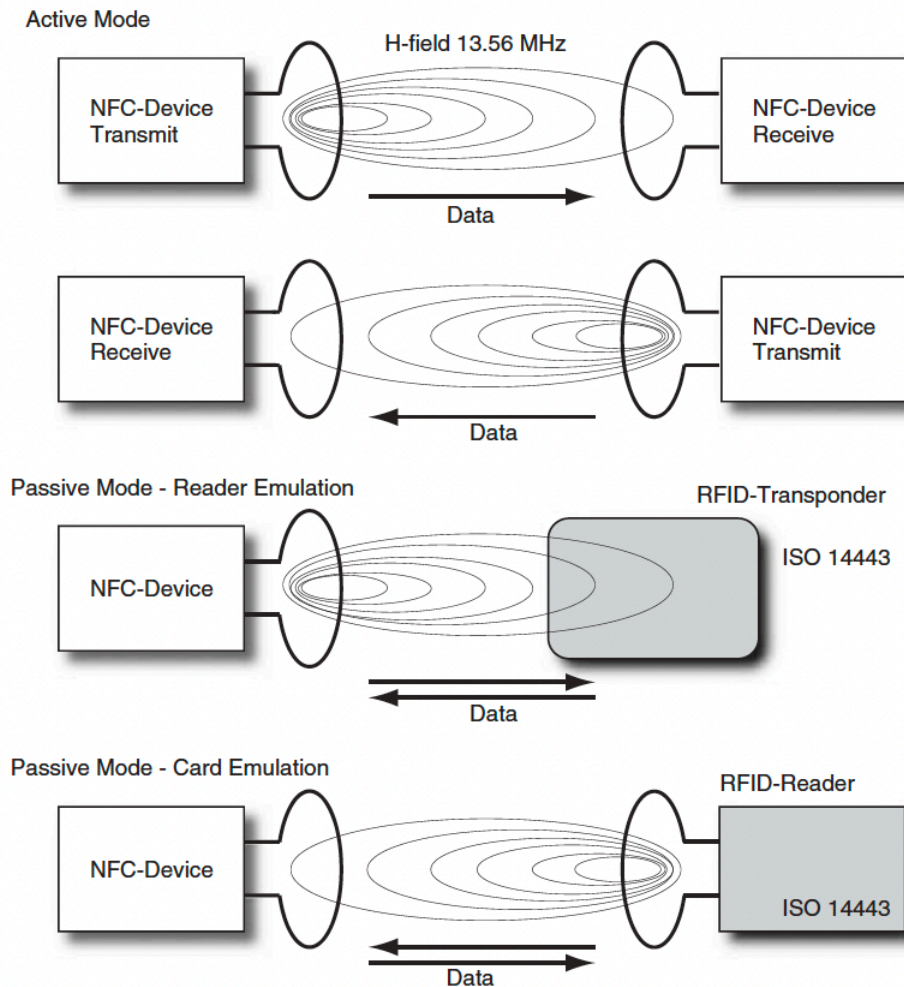


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzeller (EX1024), 58.

Active Mode

51. 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.

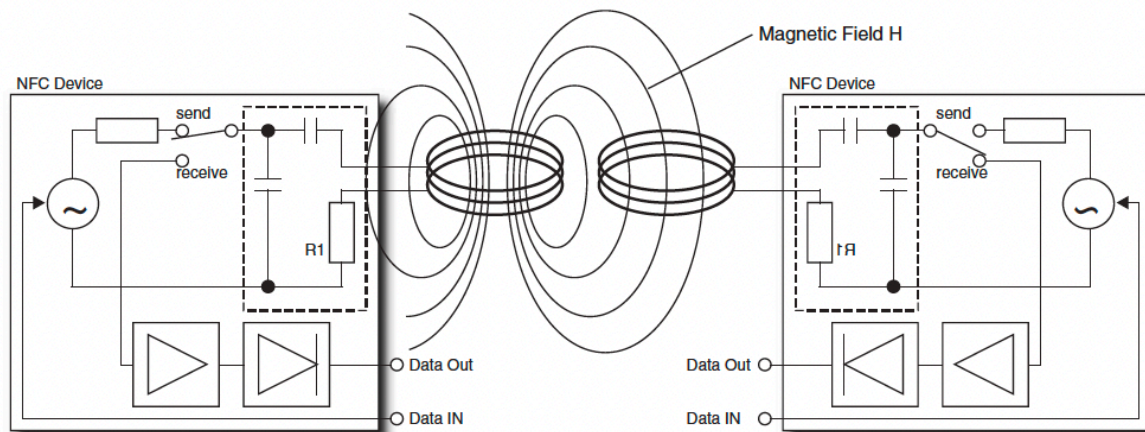


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (EX1024), 58.

52. 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.

Passive Mode

53. 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.

54. 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.

55. 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***

56. “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.

57. 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.

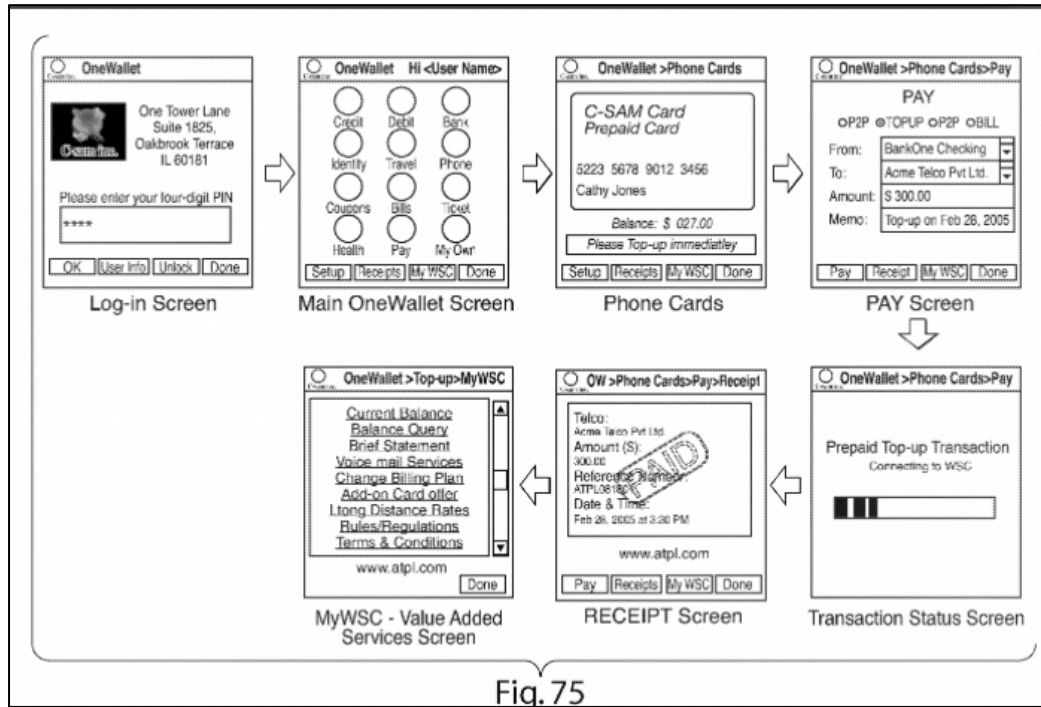
3. *Mobile Devices and Mobile Wallets*

58. Mobile devices performing contactless payments were well known before the '538 Patent.

59. 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.

60. 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.

61. A number of trials relating to mobile wallets were run prior to the '538 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.

62. 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.

63. 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.

VII. CARD EMULATION MODE

64. 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.”)

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

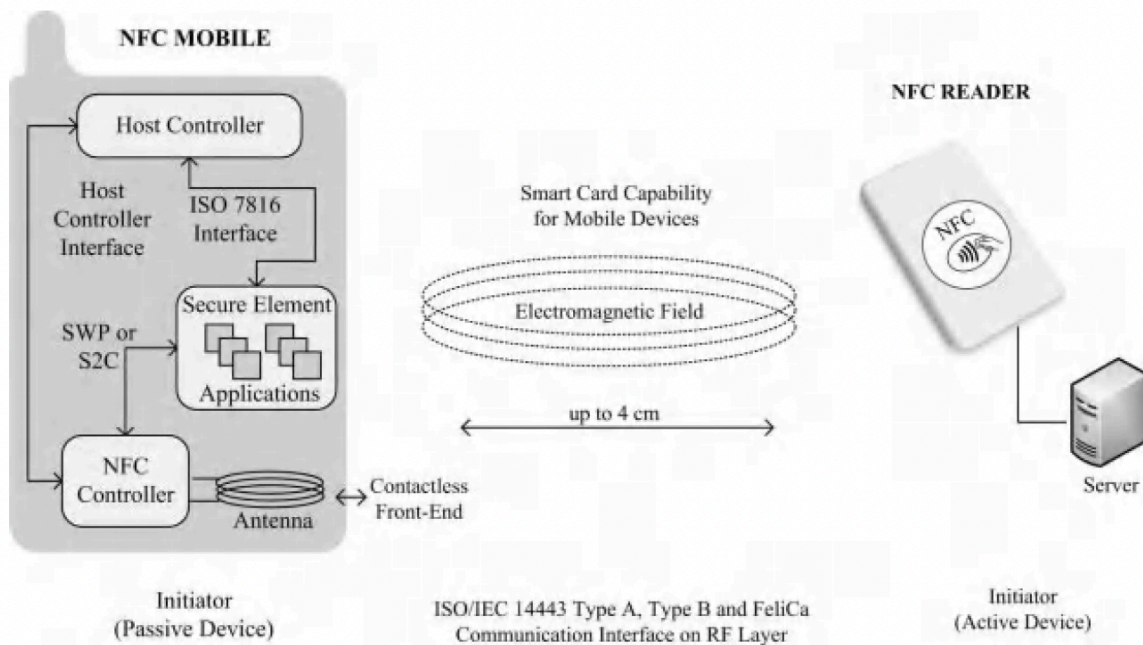


Figure 3.32 Communication architecture of card emulation operating mode.

66. 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].

A. Contactless ATMs

67. Smart devices for use with contactless ATMs were well known before the ’538 Patent.

68. 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.

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

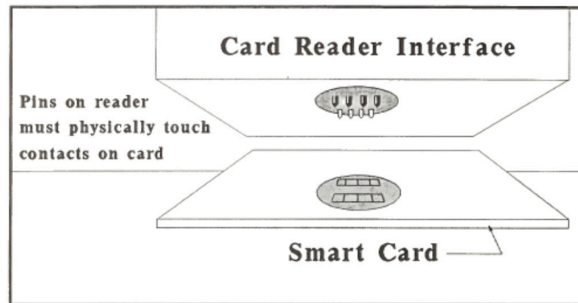


Figure 4. Contact-Type Smart Card Interface

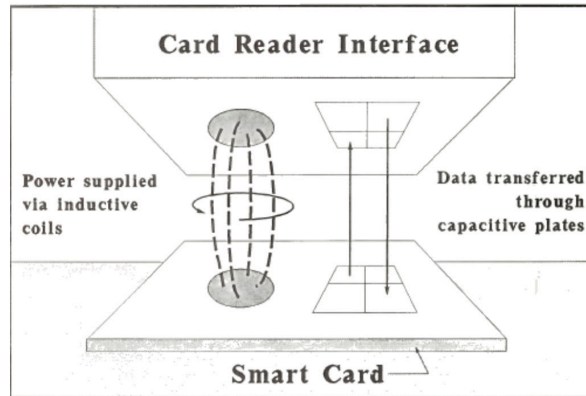
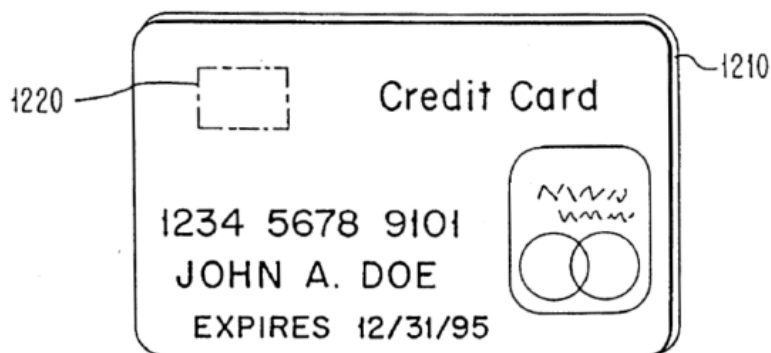


Figure 5. Non-Contact-Type Smart Card Interface

70. 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.”).

71. 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.

72. 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.

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

74. 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.

75. 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.

76. 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.

77. Thus, a POSITA was well-aware of the use of mobile devices in contactless ATM transactions prior to the ’538 Patent.

B. Payment Credential Security Features

78. 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)

79. 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.

80. 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.

81. 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].

82. 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].

83. 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*

84. 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].

85. 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].

86. 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.

87. 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].

88. As described below, all of the technology claimed in the Challenged Claims predates the '538 Patent and would have been within the knowledge of a POSITA.

VIII. SUMMARY OF UNPATENTABILITY

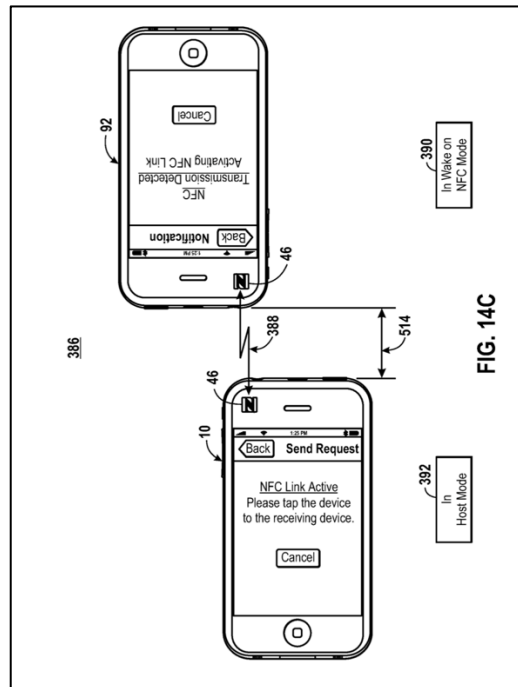
Ground	Claims	Exhibits
1	1-5, 7-18	Lin (EX1004), Smith (EX1005), Varadarajan (EX1006), and Hammad (EX1007)
2	6	Lin, Smith, Varadarajan, Hammad, and Kranzley (EX1008)

89. Above, I have reproduced the Proposed Grounds of Unpatentability from the Petition for ease of reference. Below I will address the specific teachings of these prior art references, and also the combinations of references. In so doing, I discuss the references on a limitation-by-limitation to provide overall context of the references, their relationship to the claim language, and the resulting combinations and motivations regarding the same.

IX. OVERVIEW OF THE PRIOR ART

A. Lin

90. I understand Lin teaches “the establishment of an NFC connection 388 between two devices, namely the payee device 10 and the payor device 92, by way of the tap operation 386 [.]” *Lin (EX1004)*, 68:10-13.



Lin (EX1004), Fig. 14C.

91. Once “active device 10 is placed within an acceptable distance 514 (e.g., 2-4 cm) from the payor device 92” the devices establish an “NFC connection 388...through which the payment request may be transmitted.” *Lin (EX1004)*, 68:13-25.

1. *Lin is Analogous*

92. *Lin* is analogous art to the '538 Patent because it is from the same field of endeavor because both *Lin* and the '538 Patent are directed towards conducting secure payment transactions. *See, e.g., Lin (EX1004)* at Abstract (“...one or more external financial servers 100 configured to process and determine whether the payment may be authorized.”), 33:2-7 (“Regardless of the type of connection established between the device 10 and the financial servers 100, it should be

understood that one or more of the data encryption techniques and security protocols...may be further utilized in order to facilitate the secure transmission of the transaction data 98 to the financial servers 100.”), 98:7-10 (The smart card server 874 may perform a one or more verification and/or authorization processes...wherein the payor’s smart card account 872 is verified for validity and sufficiency of funds, for example.”). *Compare* ’538 Patent (EX1001), Abstract, 1:23-28, Fig. 1 *with* Lin (EX1004), Abstract, 68:13-25, Fig. 14C.

93. Lin is also reasonably pertinent to at least one problem addressed by the ’538 Patent. Like the ’538 Patent, Lin is concerned with increasing security of payment transactions. *See, e.g.,* Lin (EX1004), 26:26–27:7 (“The security features 74 may be stored in the storage device 54 and may include one or more cryptographic protocols, such as a secure sockets layer (SSL) protocol or a transport layer security (TLS) protocol, for establishing secure communications between the device 10 and an external device. The security features 74 may also include one or more encryption applications for encrypting information sent from the device 10.”); *see also* Lin (EX1004) at 27:8–28:15; *compare* ’538 Patent (EX1001), 1:23-28, 1:63-2:4, 9:21-28 *with* Lin (EX1004), 26:26-28-15.

B. Smith

94. I understand Smith teaches a “mobile PAN” for a “mobile device” that “may...be used...with a near field communications enabled purchasing transaction.” *Smith (EX1005)*, Abstract.

95. I understand Smith teaches a “mobile PAN” is used in place of the actual PAN. *Smith (EX1005)*, [0023] (the PPAN is associated with a “related PAN[.]”); *see also Smith (EX1005)*, [0026].

600

CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE

FIG. 6

Smith (EX1005), Fig. 6.

96. The mobile PAN is “stored in the mobile device 204.” *Smith (EX1005)*, [0022].

1. Smith is Analogous

97. Smith is analogous art to the '538 Patent because it is from the same field of endeavor because both Smith and the '538 Patent are directed towards conducting secure payment transactions. Like the '538 Patent, Smith is concerned with conducting secure payment transactions. *See, e.g., Smith (EX1005)*, [0021] (“a mobile device 204 to be used to conduct a payment transaction using a payment application stored in the mobile device[.]”); [0022] (“a transaction may be initiated by the customer presenting their mobile device 204 at a merchant 214 to complete a purchase.”); [0022] (“the mobile device 204 may be presented within range of a point of sale device having NFC capabilities.”); [0024] (“a series of messages (defined by the PayPass® standard) occur, and the point of sale device is provided with information including the PPAN stored in the mobile device 204.”); *compare '538 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Smith (EX1005)*, Abstract, [0021]-[0023].

98. Additionally, a POSITA would have found Smith reasonably pertinent to the problem faced by the inventors of the '538 Patent because both Smith and the '538 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. *See, e.g., Smith (EX1005)*, [0002] (“One approach, introduced by MasterCard International Incorporated, the assignee of the present application, is to securely

install a payment application in mobile phones that are Near Field Communications (NFC)-enabled, allowing the phones to be used as a payment device in contactless payment transactions.”) [0015] (“the data elements are transmitted using a secure web service or other data protocol, such as a Simple Object Access Protocol (“SOAP”) service.”); [0020] (“a cost effective and secure method may be provided for issuers to extend NFC products by issuing and enabling over-the-air personalization of approved NFC-enabled mobile phones...The cardholder may then use his or her mobile phone as a standalone NFC payment device.”); *compare* ’538 Patent (EX1001), 1:23-28, 1:63-2:4, 9:21-28, with Smith (EX1005), [0002], [0015], [0020].

C. Varadarajan

99. Varadarajan generally teaches financial transactions between an application on a mobile device and a transaction provider. *Varadarajan* (EX1006), Abstract, [0026]. The application generates a dynamic card value (“DCV”) that replaces traditional static values, such as CVC, CVV, PAN, or account numbers. *Varadarajan* (EX1006), [0012], [0021]. The DCV is derived from device-derived information. *Varadarajan* (EX1006), [0029], [0053]. The DCV is limited in use to one or a specified time. *Varadarajan* (EX1006), [0023].

1. *Varadarajan is Analogous*

100. In my opinion, Varadarajan is analogous art to the '538 Patent. First, Varadarajan is directed to conducting secure payment transactions and, therefore, Varadarajan is in the same field of endeavor that is expressly defined in the '538 Patent. *Compare '538 patent*, Abstract, 1:23-28, Fig. 1 *with Varadarajan (EX1006)*, Abstract, [0002]-[0020], Fig. 1. Second, a POSITA would have understood Varadarajan to be reasonably pertinent to the particular problems with which the inventor of the '538 Patent was involved because Varadarajan is directed to increasing security of payment transactions. *Compare '538 Patent*, 1:23-28, 1:63-2:4, 9:21-28 *with Varadarajan (EX1006)*, [0005], [0009]-[0010].

D. Hammad

101. Hammad generally teaches methods and system for generating verification values on a portable consumer device for use in payment transaction. *Hammad (EX1007)*, 2:10-20, 2:65-3:11. The dynamically generated verification values, which are embedded in payment data sent to a service provider, are generated using two or more dynamic data elements and static data elements. *Hammad (EX1007)*, 4:21-6:42.

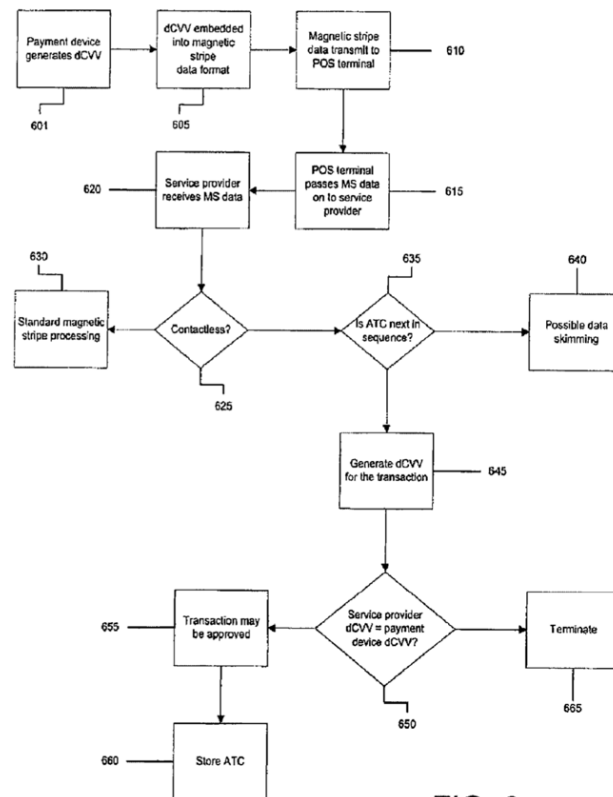


FIG. 6

Hammad (EX1006), Fig. 6.

102. For purposes of my analysis here, I note that Hammad claims priority to, and incorporates by reference, three Provisional Applications. I also note that U.S. Provisional Application No. 60/884,089 (EX1009), like Hammad, also describes the use of dCVVs. For purposes of my analysis, I am treating Hammad and the provisional applications incorporated therein as a single prior art reference. Alternatively, even if they are not considered part of a single prior art reference, it would have been obvious to use the Hammad '089 Provisional with the teachings of

Hammad as it is describing a known payment transaction system and architecture as described in the combinations below.

1. *Hammad is Analogous*

103. Hammad is analogous art to the '538 Patent because it is from the same field of endeavor. Like the '538 Patent, Hammad is concerned with increasing security of payment transactions. *See, e.g., Hammad (EX1007)*, Abstract (“The method includes generating a verification value in response to a transaction involving a portable consumer device, where the verification value is generated using a first dynamic data element and a second dynamic data element. The verification value is sent to a service provider associated with the portable consumer device so that the service provider can verify the transaction.”). *Compare '538 patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Hammad (EX1007)*, Abstract, 2:12-20, Fig. 6.

104. Hammad is also reasonably pertinent to at least one problem addressed by the '538 Patent. Like the '538 Patent, Hammad is concerned with increasing security of payment transactions. *See, e.g., Hammad (EX1007)*, 1:20-23 (“One of the primary sources of fraud, which is prevalent in the credit card industry is skimming. Skimming refers to the electronic copying of a card's magnetic stripe data to create counterfeit cards.”), 1:45-65 (“To address the above problems, a dCVV or a dynamic card verification value can be used. The dCVV can be generated using an algorithm

which uses at least a counter and input data such as an account number, expiration date, and other information. The counter can increase by one each time a transaction is conducted. The dCVV can be independently generated by either a portable consumer device or POS terminal at the front end of a transaction and can be sent to a back end computer. The counter may be sent from the merchant to the back end computer so that it knows the current counter value associated with the portable consumer device. In other cases, the counter may simply be present at the back end computer. In the latter case, the counter increments every time the back end computer sees a transaction. The back end computer, using a similar algorithm to the one that generated the dCVV at the front end, the counter value, and input data, can independently generate a second dCVV. If the received dCVV and the generated dCVV match, the transaction can be considered authentic. If the dCVVs do not match, this may indicate that the transaction is fraudulent.”); *compare* ’538 Patent (EX1001), 1:23-28, 1:63-2:4, 9:21-28 with Hammad (EX1007), 1:20-23; 1:45-65.

E. Kranzley

105. Kranzley generally teaches methods and system for conducting payment transactions with a mobile device over a network. *Kranzley* (EX1008), Abstract, [0010]. The mobile device has an application stored thereon which, during a transaction generates a static VPAN, VPAN expiration date, and dynamic data, that is sent to a payment network for authorization. *Kranzley* (EX1008), [0029],

[0035]-[0042], Fig. 1B. Kranzley teaches that “[t]he payment application of the mobile device 12 converts the data (including the PAN, expiry, and dynamic data) into a bar code image 13.” *Kranzley (EX1008)*, [0028]. Kranzley teaches displaying “the static VPAN...in plain text on a display device 14 of the mobile device 12 along with an expiry date and dynamic data.” *Kranzley (EX1008)*, [0035]; [0033]-[0036].

1. *Kranzley is Analogous*

106. Kranzley is analogous art to the '538 Patent because it is from the same field of endeavor. Like the '538 Patent, Kranzley is concerned with conducting secure payment transactions. *See, e.g., Kranzley* at Abstract (“Systems, methods processes, computer program code and means for conducting a payment transaction which include...a dynamic verification code generated by the payment application[.]”), [0003] (“It would further be desirable to provide mobile payment transactions which are secure and in which the cardholder’s presence may be confirmed.”), [0010] (“...and means for conducting a payment transaction include...at least one of a payment account number, an expiry date of said payment account number, and a dynamic verification code generated by said payment application[.]”); *compare '538 patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Kranzley (EX1008)*, Abstract, [0010], Fig. 1.

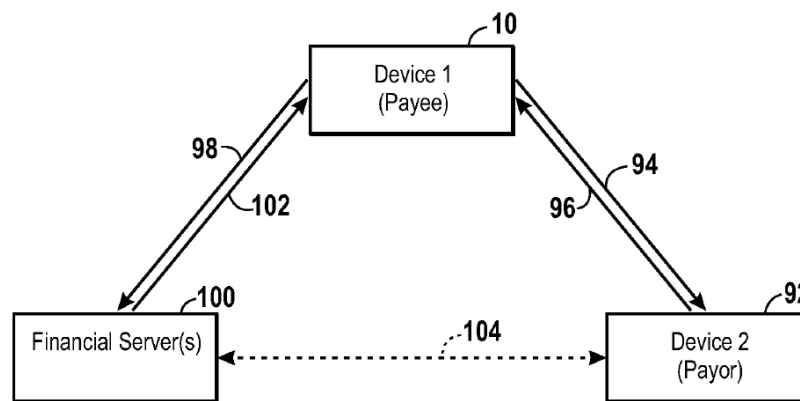
107. Kranzley is also reasonably pertinent to at least one problem addressed by the '538 Patent. Like the '538 Patent, Kranzley is concerned with increasing security of payment transactions. *See, e.g., Kranzley (EX1008)*, [0003] (“It would further be desirable to provide mobile payment transactions which are secure and in which the cardholder’s presence may be confirmed.”), [0065] (“As a specific example, for 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.”), [0067] (“The shared secret key may be used to encrypt a dynamic value transmitted from the mobile device. The payment provider 110 may use the shared secret key, in conjunction with the counter 508, to decrypt the dynamic value from the mobile device 102 to ascertain the authenticity of the transaction request.”); *compare '538 Patent (EX1001)*, 1:23-28, 1:63-2:4, 9:21-28 *with Kranzley (EX1008)*, [0003], [0065].

X. GROUND 1: LIN, SMITH, VARADARAJAN, AND HAMMAD¹

A. Claim 1

1. 1(Pre): A method of performing a payment transaction, the method comprising:

108. Lin teaches a method of performing a payment transaction² using a portable device. *Lin (EX1004)*, Abstract, 1:6-8, Fig. 1.



Lin (EX1004), Fig. 4.

109. Specifically, a payee transmits an invoice to a payor that, in turn, provides payment information to the payee. *Lin (EX1004)*, 52:25-53:9, 55:7-25. A financial server subsequently authorizes the transaction and the payor is informed. *Lin (EX1004)*, 53:15-55:6, 55:26-56:5.

¹ In my initial discussion of these references, I am analyzing the teachings and applying the combination in the context of Claim 1 of the '538 Patent. Below, I include additional claim-specific analysis, where relevant, of this combination as applied to other claims in the '538 Patent.

² Claim language identified with *italics* and underline.

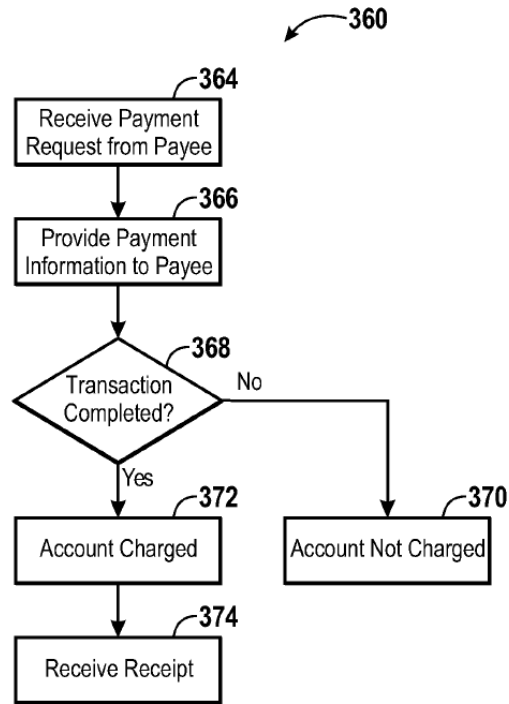


FIG. 11B

Lin (EX1004), Figs. 11A-B.

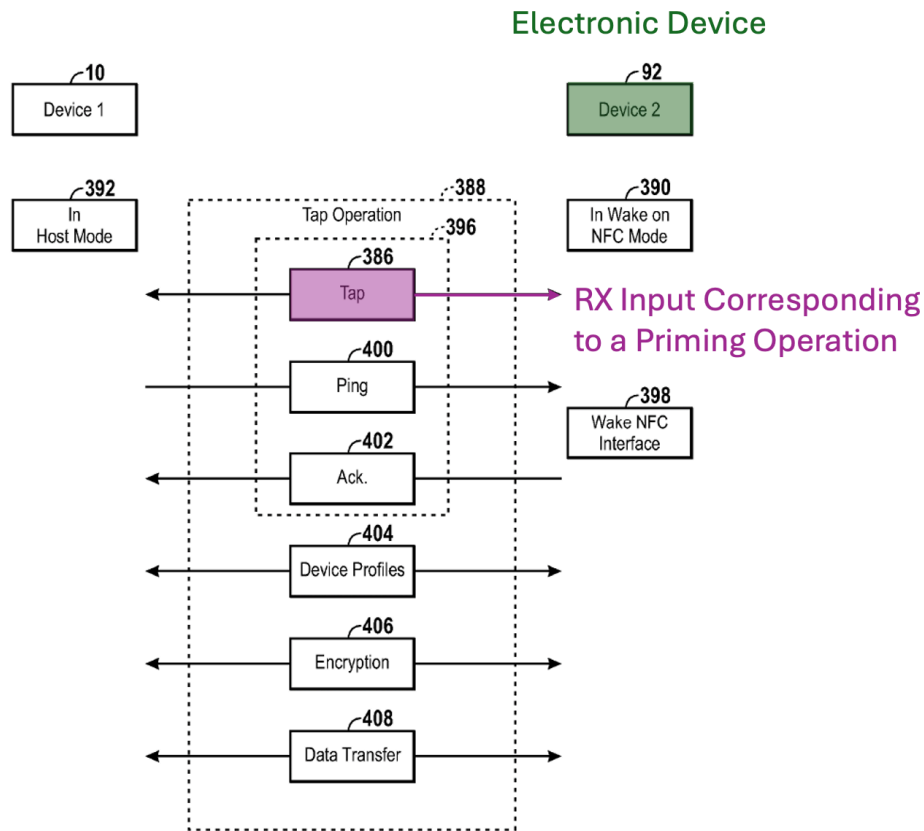
2. ***1(a): receiving an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user; and,***

110. Lin teaches receiving an input at a cellular phone (electronic device) corresponding to an NFC tap operation by an authorized user.

111. Lin teaches an “electronic device,” such as a cellular phone, having a transaction application for conducting a transaction. *Lin (EX1004)*, 14:22-29, Fig. 1. The electronic device receives input of an NFC tap operation, which is “the action of placing one NFC-enabled device within the proximity of one or more additional NFC-enabled devices such that an NFC based connection may be established

between the devices,” to initiate a transaction between the two NFC-enabled devices.

Lin (EX1004), 56:9-12, 57:3-6; *see also*, 56:28-58:9, Figs. 12A-C.



Lin (EX1004), Fig. 13 (annotated).

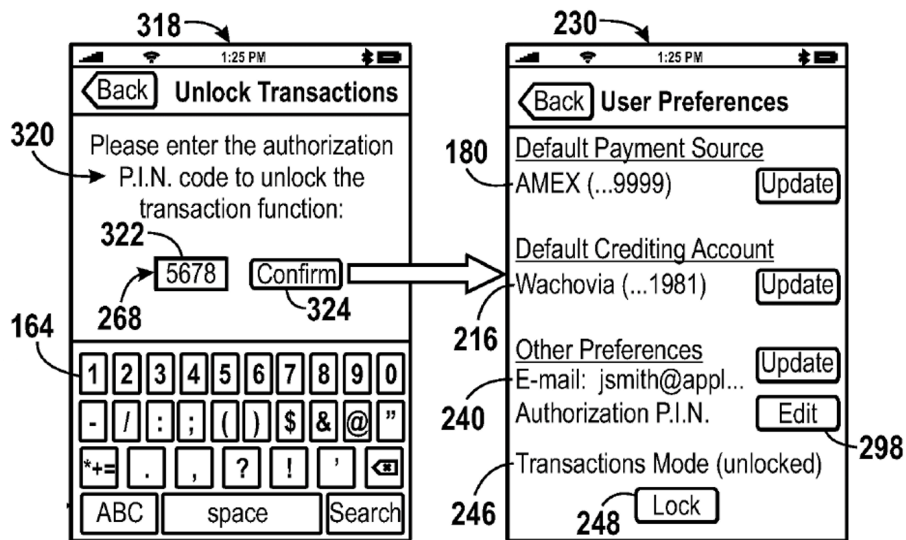
112. This is consistent with the '538 Patent's description that bringing a device within range of a reader may form part of the priming operation. '538 *Patent*, 13:65-14:1 ("The priming action can be a tap of the multi-function electronic device 601a, or tapping the multi-function electronic device 601a against the multi-function electronic device 601b.").

113. As discussed in more detail in Claim 1(b) below, the NFC tap operation is performed by an authorized user who has “unlocked” transactions by “providing an authorization PIN.” *Lin (EX1004)*, 47:25-29.

3. ***1(b): wherein []³ authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface, a gesture sensor, a motion sensor, and a biometric sensor; and,***

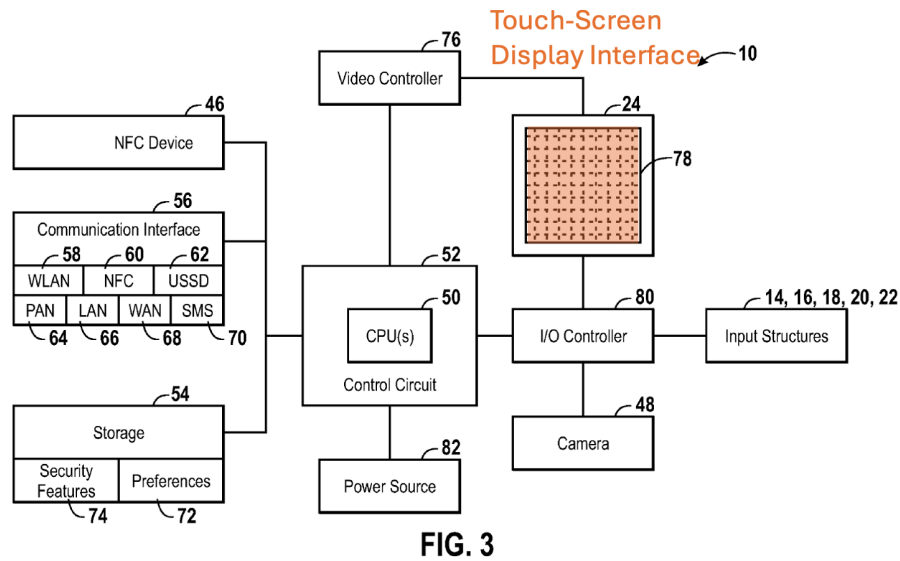
114. Lin teaches authorizing a user of the electronic device by recognizing a PIN entered on a touchscreen display. Lin teaches security features that “prevent the device 10 from being used to make payments by unauthorized persons.” *Lin (EX1004)*, 28:13-15. Specifically, the user is “unable to send or receive payments using the device” until the device’s transactions application is “unlocked upon [the user] providing an authorization PIN.” *Lin (EX1004)*, 47:25-29; *see also*, 28:4-15, 47:27-29. As shown in Fig. 10B, the user inputs an authorization PIN using “numerical keyboard 164,” which is “provided for entry of the authorization PIN 268 into the text field 322.” *Lin (EX1004)*, 52:1-15; *see also* 75:5-13, Fig. 9.

³ The word “the” was deleted in a May 10, 2022 Certificate of Correction.



Lin (EX1004), Fig. 10B (excerpt).

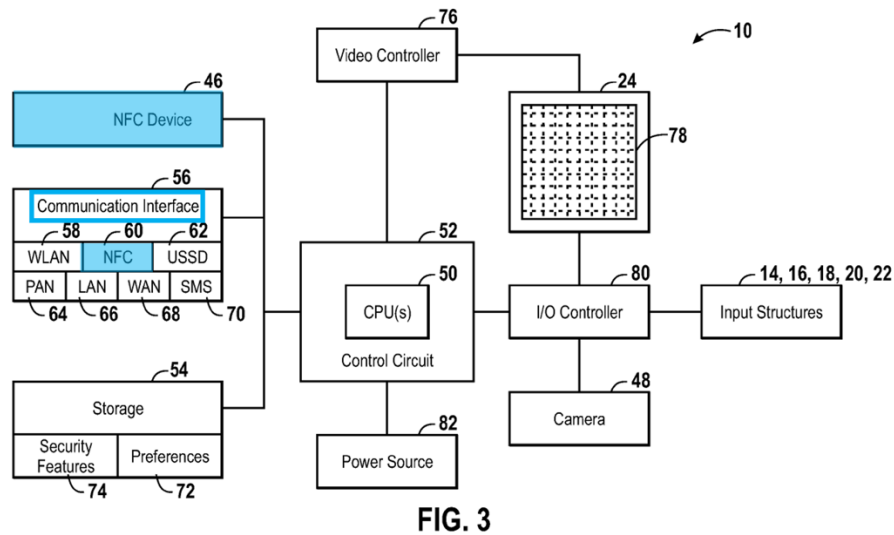
115. Lin's electronic device receives input of the PIN via "a touch screen interface" that "function[s] as an additional user input" and allows a user to "select elements displayed on the display 24 such as, for example, by touching certain elements using the user's finger or a stylus." *Lin (EX1004)*, 16:16-22; *see also*, 20:26-30, 28:28-29:14, Fig. 3.



Lin (EX1004), Fig. 3 (annotated).

4. ***1(c): receiving a request for a transaction payment at said electronic device via an NFC interface of the device; and,***

116. Lin teaches the payor and payee devices include a NFC device and NFC interface. *Lin (EX1004), 31:1-3; see also, 19:13-20:9.*



117. Lin's payor electronic device receives a payment request, such as invoice information, from a payee device. *Lin (EX1004)*, 55:7-15; *see also*, 56:24-57:2, 67:25-27, Fig. 12A.

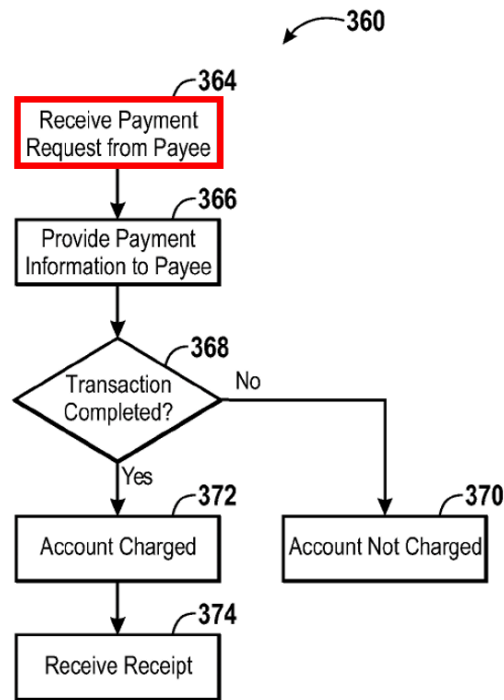
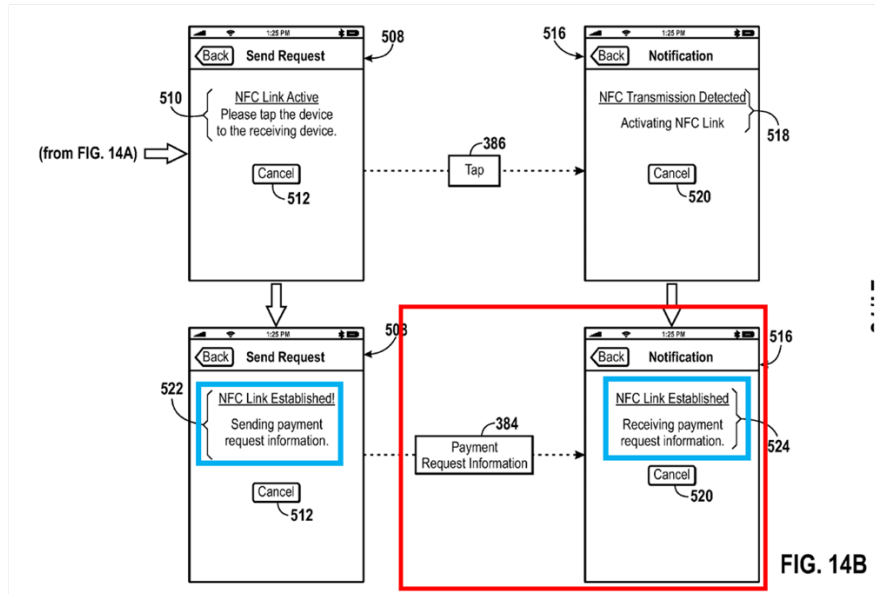


FIG. 11B

Lin (EX1004), Fig. 11B (annotated).

118. The “payment request information is ... transmitted from the payee device 10 and received by way of the corresponding NFC interface 60 in the payor device 92.” *Lin (EX1004)*, 69:28-70:4; *see also*, 55:19-22, 56:24-59:3, 59:16-18, 70:8-27, Figs. 13, 15A-B.



Lin (EX1004), Fig. 14B (annotated).

5. ***1(d): displaying, on a display of the device, [the]⁴ request and at least a portion of an original static issuer-supplied payment account information associated with a [selected]⁵ payment method, for a user selection in paying the []⁶ request; and,***

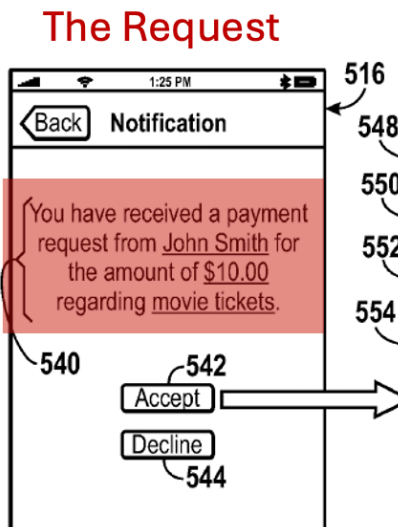
119. Specifically, Lin teaches that a payor device includes a “a display 24 configured to display various images generated by the device 10.” *Lin (EX1004)*, 16:7-8. The display “display[s] a graphical user interface (‘GUI’) 28 that allows a user to interact with the device 10.” *Lin (EX1004)*, 16:23-25. Figure 14E shows GUI “screens that may be displayed on payor device illustrating various methods for

⁴ The phrase “a transaction payment” was deleted and replaced with “the” in a May 10, 2022 Certificate of Correction.

⁵ The word “selected” was added in a May 10, 2022 Certificate of Correction.

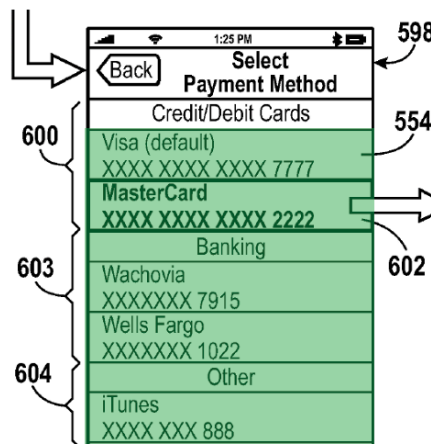
⁶ The word “payment” was deleted in a May 10, 2022 Certificate of Correction.

selecting a payment account in response to the payment request of FIG. 14A[.]” *Lin (EX1004)*, 8:6-8. As shown in FIG. 14E, “once the payment request information has been received by the payor device, the screen 516 may be updated to display the details 540 of the payment request, which may generally reflect information 10 entered by the payee into the fields 496, 498, and 500 on the screen 492 of FIG. 14A.” *Lin (EX1004)*, 71:7-13.



Lin (EX1004), Fig. 14E (annotated excerpt).

120. When paying the request, *Lin* also teaches GUI screen 598, which displays “a listing of all selectable payment accounts stored on the payor device 92, which may be provided by the screen 598.” *Lin (EX1004)*, 72:27-30; *see also*, 70:28-71:6. The payor may choose to view all available payment accounts before making a payment account selection. *Lin (EX1004)*, 72:24-73:3. Each available payment account represents a payment method.



At Least a Portion of an Original Static Issuer-Supplied Payment Account Information

Lin (EX1004), Fig. 14E (annotated excerpt).

121. As shown in Fig. 14E, the last four digits of each payment account (at least a portion of an original static issuer-supplied payment account information associated with a payment method) is displayed for a user selection in paying the selected request. The user then selects a payment account from the list to pay the selected payment request. *Lin (EX1004)*, 73:7-13; *see also*, 55:12-19, 59:18-22, 75:14-17.

6. ***1(e): retrieving from a memory attached to a processor of the device, a device-specific static limited-use payment information, associated with said selected payment method; and,***

a) *Lin's Teachings*

122. Lin teaches an electronic device that includes a CPU attached to a storage device via a data bus. *Lin (EX1004)*, 20:26-21:12, 22:5-8.

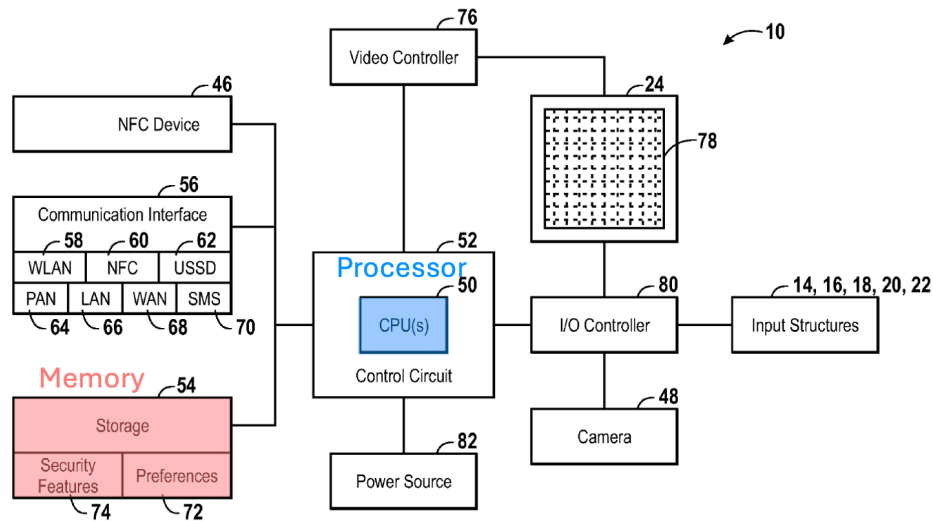


FIG. 3

Lin (EX1004), Fig. 3 (annotated).

123. Lin generally teaches “a secure access-restricted storage area (e.g., within the storage device 54) to limit access to the data that may be required by the certain aspects of the security features 74, such as encryption keys, passcodes and passwords, digital certificates, or the like.” *Lin (EX1004)*, 27:8-11. Lin also teaches that the portable device “initiates payment[s] ... by transmitting payment information corresponding to a credit account store on the device ... to an external device.” *Lin (EX1004)*, 3:17-21, 55:17-22, Fig. 11B.

b) Smith’s Teachings

124. In related art, Smith teaches a “mobile device” from which a “user may request the issuance of a payment account such that the payment account is accessible using a mobile device 104 associated with a customer.” *Smith (EX1005)*, [0014]. Whenever a user wishes to open a payment account, the issuer issues a

“temporary PAN...and establishes any risk parameters (e.g., for use in controlling the authorization of transactions involving the temporary PAN)” so the user is able to make purchases while awaiting an actual PAN. *Smith (EX1005)*, [0014]-[0016], [0026].

125. This “temporary PAN is mapped to a **mobile PAN (e.g., such as a PayPass® PAN, or PPAN).**” *Smith (EX1005)*, [0026] (emphasis added). The PPAN (device account number) is “assigned to the mobile device 104.” *Smith (EX1005)*, [0016]. The PPAN is “stored in the mobile device 204.” *Smith (EX1005)*, [0022]. The PPAN is used in an NFC payment transaction. *Smith (EX1005)*, [0022]. The PPAN is, therefore, a device-specific static limited-use payment information.

126. Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith (EX1005)*, [0026], [0040]. The PPAN (device account number) is then associated with a “related PAN[.]” *Smith (EX1005)*, [0023]. The PPAN is “initially...mapped to the temporary PAN” but whenever the issuer issues the “actual PAN” the actual PAN “replace[s] the temporary PAN” so the PPAN is now an alternate number mapped to the actual PAN. *Smith (EX1005)*, [0040]. The PPAN is a different number from the actual PAN.

600

CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE

FIG. 6

Smith (EX1005), Fig. 6.

127. The issuer can “implement dual account number structures” so that “multiple NFC-enabled handsets may be managed for a single account.” *Smith (EX1005)*, [0029]. It was well known that a dual account number has separate and distinct numbers for each device the overall account is used on. Accordingly, Smith’s PPAN is a distinct account number for a payment account on a particular “mobile device” (*a specific device*).

128. Even if the same user wants to register a new device, a user will get a different PPAN for that device to use because the PPAN is assigned immediately upon registering the device. *Smith (EX1005)*, [0026] (“an instantly-issued payment

account that may be used by the customer almost immediately after submitting a request for a new payment account.”).

129. Smith teaches the expiration date associated with the account may be updated without updating the PPAN. *Smith (EX1005)*, [0041] (“update an NFC-enabled payment account (e.g., to update an expiration month and/or year”) Therefore, a POSITA would understand because the PPAN is associated with a specific account (having an expiration date) and assigned to a mobile device, it is a device-specific static limited-use payment information associated with a payment method.

c) Motivation to Combine

130. A POSITA would have found it obvious and been motivated to store Smith’s PPAN in place of Lin’s payment account number. A POSITA would have appreciated that storing a PPAN would be safer than storing the actual account number on Lin’s device. Thus, this modification prevents bad actors from obtaining access to the actual account number if a user device is stolen. It was well known in the art that a mobile device could be vulnerable to malicious attacks and therefore storing Smith’s PPAN instead of the account number on Lin’s mobile device would have increased security for the user’s account. For example, a POSITA would have understood that it is valuable to remove account numbers from a user device so that if the device were stolen, the thief would have access only to PPAN(s). *See, e.g.,*

Bona, [0074]. A POSITA would have recognized that this is beneficial because if a user's device is lost or stolen, only the PPAN(s) would have to be cancelled. *Bona*, [0007], [0014], [0074], Fig. 6. A POSITA, therefore, would have been motivated to configure the processor executing Lin's mobile wallet application on the electronic device to retrieve the PPAN associated with the selected payment account from storage device to improve similar mobile wallet systems in the same way, i.e., preventing bad actors from accessing payment account numbers by not storing them on the mobile device.

131. A POSITA would have had a reasonable expectation of success in implementing Smith's PPAN in Lin's payment application without undue experimentation because Lin already teaches use of an account number and a POSITA would have been familiar with using account number alternatives when making mobile payments. In the combination, Smith's PPAN would perform the same function—provide an alternative account number that can be used for a payment transaction. *Smith (EX1005)*, [0021]-[0022]. A POSITA would have understood that using Smith's PPAN in place of Lin's account number, such that the PPAN is retrieved from memory by Lin's processor, would be combining prior art elements according to known methods to yield the predictable result of increased security. Indeed, as discussed in Section VI.C.1., the use of alternative identification methods for primary account numbers was a well-known way to combat fraud by

not transmitting the actual account number in a transaction. Examples of such identification methods include limited-use tokens or alternative account numbers, such as a virtual PAN (as discussed in *Kranzley (EX1042)*). An additional example is found in *Khan*, which describes using an “alias” of a credit card number in a payment transaction involving a mobile device. *Khan (EX1044)*, [0007]-[0009], [0022]-[0025], Figs. 2, 4-5. Using an alias prevents the actual card number from being transmitted over a network and provides a “secure method of executing a commercial transaction that is both secure and user friendly.” *Khan (EX1044)*, [0005]. A POSITA, therefore, would have been motivated to apply Lin and Smith’s teachings and appreciated the compatibility of their teachings because both discuss payment systems that rely on similar functionalities.

132. A POSITA would have further recognized that modifying Lin’s system according to the teachings of Smith required only basic software modifications and routine skill. For example, because the constituent hardware components are largely the same (e.g., mobile device with a processor and payment application thereon communicating payment information to one or more payment provider and processing authorities), a POSITA would realize that the electronic device of Lin could be modified to incorporate Smith’s PPAN into device memory. This modification would simply require the payment provider providing a PPAN for an account to the mobile device upon the device adding the account to the device and

registering with the payment provider, as described in Smith. Modifying Kalgi to include such a functionality would not have been challenging given providing and using alternative account numbers in payment transactions known at the time. *See Khan (EX1044); Kranzley (EX1042), Grigg (EX1041);* Section VI.C.1. Thus, such a modification to Kalgi's system would have been straightforward.

133. A POSITA would have substituted Smith's PPAN for Kalgi's account numbers when making payment transactions, as taught by Smith. *Smith (EX1005)*, [0018] ("the process of personalizing the mobile device 104 with the software (including the PPAN...[o]nce the personalization or loading of the payment application is complete, the customer 102 may use the mobile device 104 to complete payment transactions."). A POSITA would again have recognized that substitution of a PPAN would have increased security since sensitive information like an account number that would not be transmitted. *Smith (EX1005)*, [0023] ("the payment network 218 identifies the PPAN and requests a look up of the related PAN"). This is a simple substitution of one known element (Lin's account number) for another (Smith's PPAN) that a POSITA would have understood to predictably increase the security of Lin's payment system and protected the user's sensitive account number. Because Smith's PPAN is used in a transaction in the same way as a payment account number in Lin, there would have been a reasonable expectation of success configuring Lin's device to use the processor to retrieve the PPAN from

memory to make payments using the PPAN, as such would have been a combination of known elements that would yield predictable results of increased security because the PAN is not transmitted.

7. ***1(f): dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method; and,***

134. It would have been obvious to modify Lin-Smith to dynamically generat[e], by a processor of Lin's device, device-specific limited-use payment information, for said selected payment method in view of Varadarajan.

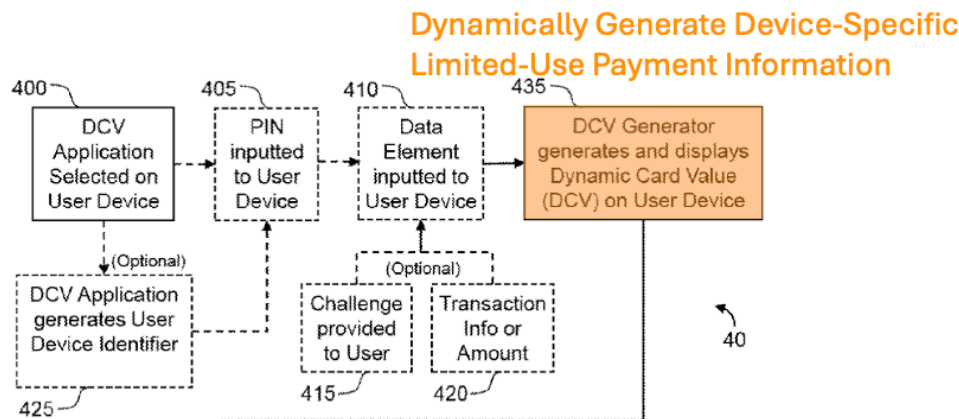
a) *Varadarajan's Teachings*

135. Varadarajan teaches a similar mobile payment application on a mobile user device for conducting contactless payment transactions. *Varadarajan (EX1006)*, [0011], [0032], [0038]-[0039], [0041]. Specifically, the "user downloads the DCV application to his mobile user device, which can be virtually any hand-held platform," including "'smart' phones such as the ... iPhone™[.]" *Varadarajan (EX1006)*, [0026]. A DCV generator, generated by the issuer/card provider, on the user device may be identified by a logo associating it with the card provider, which is then selected by the user through the application. *Varadarajan (EX1006)*, [0038], [0045]-[0049], [0052] ("The DCV application can store DCV generators for multiple credit cards, debit cards, ... and for cards from different issuers or providers, on a single user device."). Varadarajan recognizes that "[c]ard based

transactions ... have certain security vulnerabilities,” including that “[t]he security of the CVV encoded on the magstripe can be compromised in a number of ways.”

Varadarajan (EX1006), [0003], [0005], [0009].

136. To solve these problems, Varadarajan proposes using the DCV application and generator on the user’s mobile device to generate a dynamic card value (“DCV”), which is used to replace a static value, such as “a CVC, CVV, CSC, PAN, account number, partial PAN and a portion of an account number[.]” *Varadarajan (EX1006)*, [0011]-[0012], [0020]-[0021] (“The DCV is configured and provided in the same form as the static DCV for which it is being substituted.”), [0031].



Varadarajan (EX1006), Fig. 4 (annotated excerpt).

137. The DCV is provided over “any of a number of contactless communication technologies, including but not limited to Bluetooth, RFID, transponders, proximity card communication techniques, and other methods known

to those skilled in the art of near field communication technologies.” *Varadarajan (EX1006)*, [0032].

138. The DCV is limited use in that it expires “after a limited number of uses, which may be a single use[,]” which limits attacks on credit/debit card transactions. *Varadarajan (EX1006)*, [0023].

139. Varadarajan teaches, and a POSITA would understand, the DCV is also device-specific because the DCV generator uses “a device derived identification parameter ... which is unique to the user device or machine used to host the DCV generating application” such that “the included device identifier is unique to each user device ... [and] each transaction and DCV is further identifiable to the user device conducting a transaction or requesting a DCV.” *Varadarajan (EX1006)*, [0029], [0053]; *see also*, [0043], [0049], [0054].

140. Thus, a POSITA would understand Varadarajan’s DCV is device-specific limited-use payment information that is dynamically generated for a specific payment method (e.g., specific credit card).

b) Motivation to Combine

141. As described above, the Lin-Smith PPAN prevents attackers from accessing a primary account number from an electronic device that has been lost or stolen. However, a POSITA would have understood that the Lin-Smith electronic device would still be vulnerable to attacks where the PPAN and CVV values are

intercepted by an attacker and used for fraudulent transactions, as taught by Varadarajan. To prevent this type of attack, a POSITA would have been motivated to configure the Lin-Smith processor to implement Varadarajan's method of dynamically generating a DCV to be used in place of the selected payment method's CVV to improve similar mobile payment systems in the same way.

142. The concept of dynamic CVVs was well-known at this time and a POSITA would have been familiar with using such numbers in connection with mobile payment transactions to increase security. *See* Section VI.C.2. As described in Section VI.C.2, credit card companies, such as Mastercard and Visa, were using dynamic verification values that were unique to each transaction in place of static CVVs. *Bona (EX1043)*, [0037], *Ashfield (EX1033)*, [0005]. Similarly, as discussed further in Claim 5(a) below, Hammad (assigned to Visa) describes a mobile device generating dCVVs using multiple data inputs, including information relating to a "consumer's portable electronic device," and using the same in payment transactions was known before 2007 to address the problem of account information being intercepted. *Hammad (EX1007)*, 1:46-65. As such, a POSITA would have been motivated to configure Lin's mobile device to generate a dynamic card value, such as a DCV, as a replacement for the issuer provided CVV. The substitution of Lin-Smith's CVV with Varadarajan's DCV is a substitution of one known element for another and a POSITA would have understood that the substitution would have

predictably increased the security of Lin-Smith's payment system and further protected the user's sensitive account information.

143. A POSITA would have appreciated that this would have predictably prevented the risk of attacks where the PPAN and CVV are stolen by an attacker even if the user's mobile device has not been lost or stolen. Likewise, because the PPAN is still being used in place of the PAN, the Lin-Smith-Varadarajan device would still retain the benefits of allowing the user to easily cancel PPANs without cancelling the payment devices in his or her mobile wallet if the mobile device is lost or stolen, while also increasing security by preventing fraudsters from stealing the payment device data (e.g., PPAN and CVV) required to perform transactions.

144. A POSITA would have had a reasonable expectation of success in modifying Lin-Smith in this way because Lin-Smith already teaches a transaction application for conducting payment transactions. Thus, a POSITA would have recognized that modifying Lin-Smith's system according to the teachings of Varadarajan required only basic software modifications and routine skill. For example, because the constituent hardware components are largely the same (e.g., both references are compatible with NFC transactions), a POSITA would realize that the electronic device of Lin-Smith could be modified programmatically to incorporate Varadarajan's DCV into the payment information transmitted during the payment transaction. Thus, the modification would simply require including

programming in Lin's memory for generating a dynamic card value, i.e., DCV, and using the same in place of a PAN or CVV, which would have required routine skill. As such, the modification would have been a combination of a known technique (using dynamic card verification values) to improve similar devices (mobile devices performing payment transactions) in a similar way that would yield the predictable result of increased security of more secure payment transactions by dynamically generating a code verification value. Thus, given the use of dynamic account information was well known to increase security, a POSITA would have been motivated to include the same function in Lin's mobile device for performing a payment transaction.

8. *1(g): using said limited-use payment information[s]⁷ in place of at least a portion of said selected original issuer-supplied payment information for the transaction; and,*

145. For the reasons discussed above, it would have been obvious to a POSITA to use Varadarajan's DCV (said limited-use payment information) in place of the selected payment method's CVV values (a portion of said selected original issuer-supplied payment information for the transaction). See Claim 1(f).

⁷ The word "information" was replaced with "informations" in a May 10, 2022 Certificate of Correction.

9. ***1(h): combining []⁸ said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information; and,***

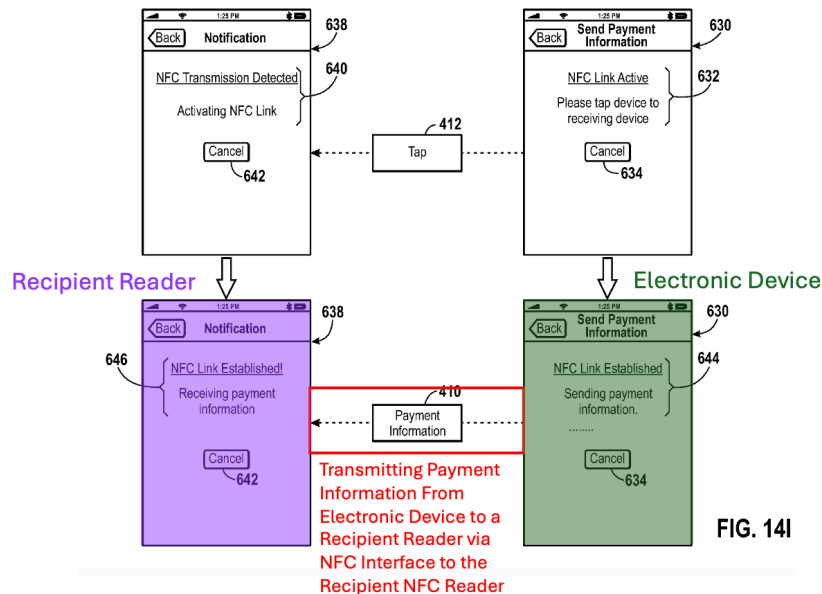
146. Lin teaches payment information for a credit card includes card number, expiration date, and CVV values. *Lin (EX1004)*, 37:16-20, Fig. 5A; *see also*, 31:29-32:6, 40:19-28. As discussed above, it would have been obvious to replace the card number/PAN with the PPAN (said static limited-use payment information), and the CVV with the DCV (said dynamically generated limited-use payment information). *See* Claims 1(e)-(f). Thus, it would have been obvious to further configure Lin's electronic device to combine the PPAN and DCV as a substitute for the card number and the CVV to form complete device payment information for the same reasons. *See* Claims 1(e)-(f).

10. ***1(i): transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction; and,***

147. Lin teaches transmitting "payment account information 96 may similarly be transmitted from the payor device 92 to the payee device 10 by way of the previously established NFC connection through each device's respective NFC interface 60." *Lin (EX1004)*, 32:1-4; *see also* Claim 1(c). Specifically, Lin's

⁸ The word "transmitted" was deleted in a May 10, 2022 Certificate of Correction.

electronic device 92 transmits the payment account information to a payee device 10 (*a recipient reader*) via the NFC interface to the payee device's NFC reader (*the recipient NFC reader*). *Lin (EX1004)*, 31:29-32:6, 59:22-60:2, 55:17-25, 77:1-8, Fig. 11B, FIG. 14I,.



Lin (EX1004), Fig. 14I (annotated).

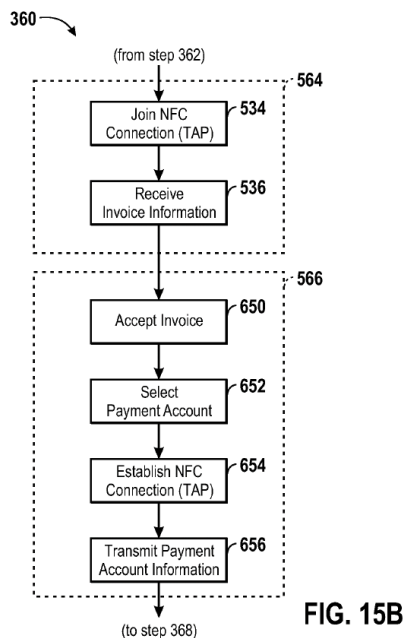


FIG. 15B

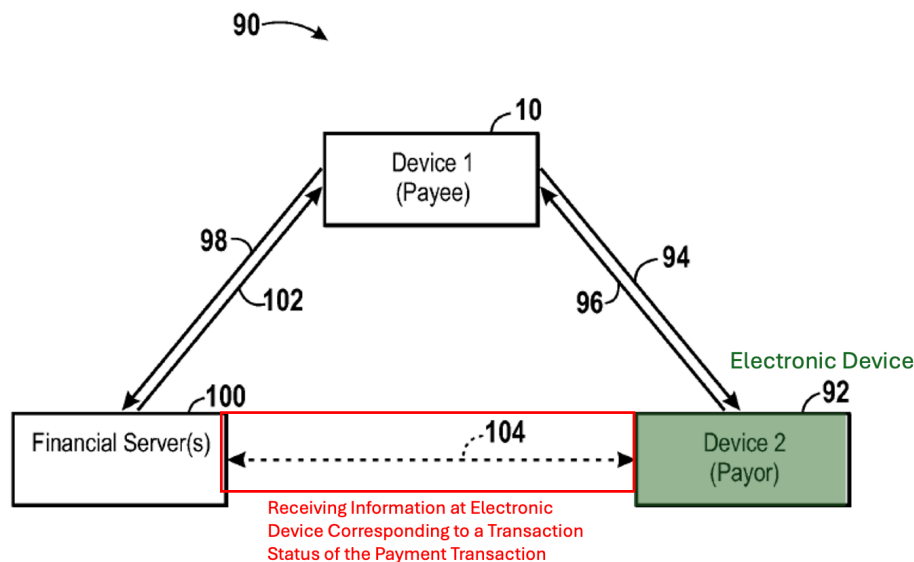
Lin (EX1004), Fig. 15B.

148. The payee device subsequently transmits the transaction information “to one or more financial servers 100 for verification of the account information and the subsequent authorization and processing of the requested payment.” *Lin (EX1004)*, 32:20-27; *see also*, 53:5-23, 54:26-55:6, 60:6-12, 60:24-61:30, 79:24-80:3, 80:25-81:82:17, Figs. 11A, 15B.

149. As discussed above, the combination of Lin-Smith-Varadarajan teaches said complete device payment information. *See* Claim 1(h). Thus, the Lin-Smith-Varadarajan combination also teaches transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction for the same reasons.

- 11. 1(j): receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the []⁹ complete device payment information by a payment processor authority and a payment issuer authority; and,**

150. Lin teaches that the electronic device receives “a confirmation message [104] in the form of an electronic receipt ... to the payor device 92 if the transaction is processed successfully.” *Lin (EX1004)*, 35:24-28. The payment receipt “may be transmitted to the payor by the payee, either directly via the payor device 10, or indirectly via one of the financial servers[.]” *Lin (EX1004)*, 55:1-6; *see also*, 35:24-30, 55:29-56:5, 61:23-30, 83:19-27, Figs. 11B, 12A, 15A, 16A.



Lin (EX1004), Fig. 4 (annotated).

⁹ The word “transmitted” was deleted in a May 10, 2022 Certificate of Correction.

151. “The electronic receipt 104 may serve as acknowledgment that the requested payment has been satisfied by the payor and received by the payee.” *Lin (EX1004)*, 35:28-30.

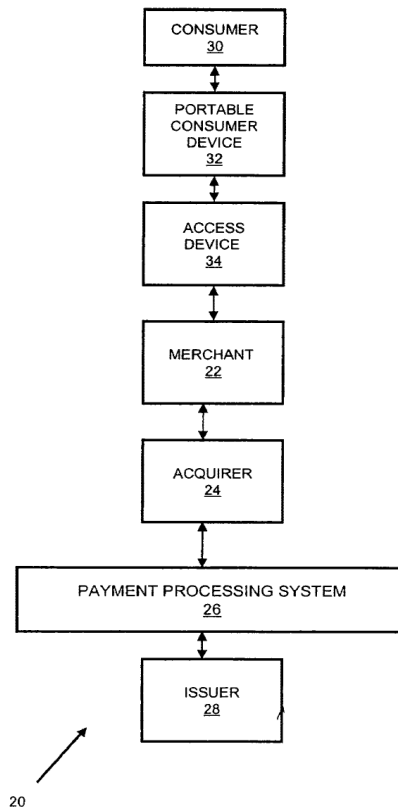
152. The validation of the payment information is performed by “financial servers 100,” which in one embodiment include a credit card verification server “which maintains the payor’s selected credit card account, such as American Express® or MasterCard®.” *Lin (EX1004)*, 33:8-34:22; *see also*, 53:15-23, 60:6-61:4, 61:9-30, Figs. 11A, 12A. The credit card verification server “verif[ies] whether credit card account information ... corresponds to a valid credit card belonging to the specified payor” and whether the line of credit has sufficient funds. *Lin (EX1004)*, 34:1-10. A POSITA would understand that such a credit card verification server, e.g., operated by MasterCard, is a payment processor authority, because it validates the credit card account, and a payment issuer authority, because it authorizes issuance of a card. An entity acting as the payment processor and issuer was commonplace at the time. *See Hammad ’089 Provisional (EX1009)*, [0025], p. 78.

153. Alternatively, and to the extent Patent Owner argues that Lin’s verification server does not teach a payment processor authority and a payment issuer authority, it would have been obvious to use these components in Lin’s financial servers based on Hammad.

a) *Hammad's Teachings*

154. Similar to Varadarajan, Hammad describes generating a dynamically generated card verification value (“dCVV”) using an application on a mobile device for use in a mobile payment transaction, including contactless transactions. *Hammad (EX1007)*, 2:65-3:11, 3:51-4:6. The dCVV is embedded in payment data that is sent to a service provider for validation via a payment network. *Hammad (EX1007)*, 7:43-46, 7:55-62. A service provider is defined as a “payment processing organization or an issuer of the portable consumer device.” *Hammad (EX1007)*, 2:18-20. The service provider, which is the payment processor or issuer, validates the payment data, including the dCVV. *Hammad (EX1007)*, 2:18-20, 7:29-8:45.

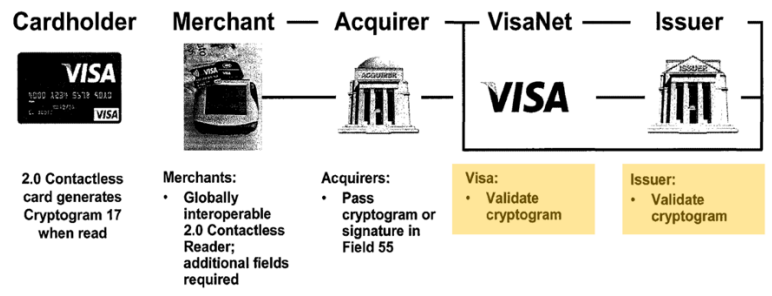
155. Hammad '089 Provisional describes a common architecture for processing credit card payments that includes a merchant, acquirer, payment processing system (a payment processor authority), and issuer of the portable consumer device (a payment issuer authority), among other components. *Hammad '089 Provisional (EX1009)*, [0012]-[0013].



Hammad '089 Provisional (EX1009), Fig. 1.

156. The payment processing system is able to “process credit card transactions” and forward authorization requests to the issuer for authorization.

Hammad '089 Provisional (EX1009), [0016], [0021]-[0022]. Hammad '089 Provisional further describes that the payment processing system and issuer “validate cryptogram,” i.e., dCVV.



Hammad '089 Provisional (EX1009), p. 78. Hammad teaches, and a POSITA would have understood, that some entities, such as Discover and American Express, perform the functions of payment processor and issuer. *Hammad '089 Provisional (EX1009)*, [0025].

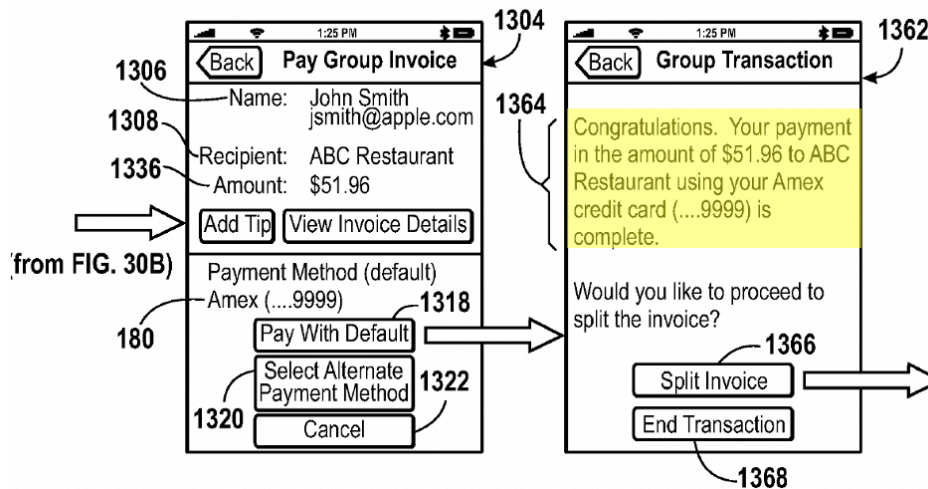
b) Motivation to Combine

157. Based on the teachings of Hammad, it would have been obvious, and a POSITA would have been motivated to implement the Lin-Smith-Hammad-Varadarajan device with the payment processing architecture described in Hammad, including a payment processing and issuer system. A POSITA would have recognized that the payment processing system and issuer of Hammad are similar to Lin's one or more financial servers, including a credit card verification server, but described at an additional level of detail. A POSITA would have understood that a payment processor and issuer, as described in Hammad, were commonly used to process authorization requests, and were often the same entity. *See Hammad '089 Provisional (EX1009)*, [0025], p. 78. Thus, it would have been obvious to implement the known elements of Hammad's payment processing and issuer server in Lin's financial servers according to known methods to process a payment transaction. Given the ubiquity of payment processing and issuer servers, as performed by separate or the same entity, for validating payment information, there would have been a reasonable expectation of success.

12. 1(k): visually conveying the transaction payment authorization status via a user-interface displayed on said display.

158. As discussed in Claim 1(j), Lin teaches that the electronic device receives “a confirmation message in the form of an electronic receipt, represented herein by reference numeral 104, to the payor device 92 if the transaction is processed successfully.” *Lin (EX1004)*, 35:24-28, Fig. 4; *see also* Claim 1(j). Lin further teaches that “a payment receipt may be transmitted to the payor by the payee ... directly via the payor device[.]” *Lin (EX1004)*, 55:1-3. A POSITA would have understood that the confirmation message/payment receipt received by the payor would be displayed on the user-interface.

159. Alternatively, this limitation is rendered obvious by Lin. Lin teaches another embodiment where “if the primary transaction 1172 is authorized by the financial servers 100” the electronic device displays a screen including “the notification message 1364 indicating to the initiator that the group invoice 180 has been paid using the selected default payment account 180.” *Lin (EX1004)*, 131:29-132:32.



Lin. Fig. 30C (annotated excerpt).

160. Based on this express teaching, it would have been obvious, and a POSITA would have been motivated to configure Lin's electronic device to visually convey the confirmation message 104 (transaction payment authorization status) via a user-interface displayed on said display for every transaction completed by the device. Providing visual feedback to users of mobile devices was well-known to a POSITA and expected by users of such mobile devices, such as smartphones. It was also well known to POSITAs that users expected feedback to let them know when a transaction was successfully completed. Visual feedback was a well-known and reliable way to provide this type feedback to users. Such visual feedback is depicted throughout Lin. See Lin (EX1004), Figs. 5A-10B, 14A-J, 17A-B, 19A-D, 22A-C, 30A-L. Indeed, Lin already teaches providing the payor device with a confirmation message indicating a status of a transaction. See Lin (EX1004), 131:29-132:32, Fig. 30C. Modifying Lin in this way would have predictably increased the user

experience to visually see the status of a transaction. Thus, there would have been a reasonable expectation of success configuring Lin's device to generate a screen displaying a notification message to visually convey whether a transaction was authorized or not as the same is already depicted in another embodiment of Lin. As such, it would have required routine skill and programmatic changes to simply display a confirmation or denial message or a receipt to user on the display.

B. Claim 2

- 1. 2: *The method of claim 1, further comprising receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.***

161. Lin teaches that “the payee device 10 may also transmit a confirmation message [104] in the form of an electronic receipt [confirmation] ... to the payor device 92 if the transaction is processed successfully.” *Lin (EX1004)*, 35:24-30, Fig. 4; *see also*, 54:26-55:3, 56:2-5, 85:7-19, Figs. 11B, 16A; *see also*, Claim 1(j).

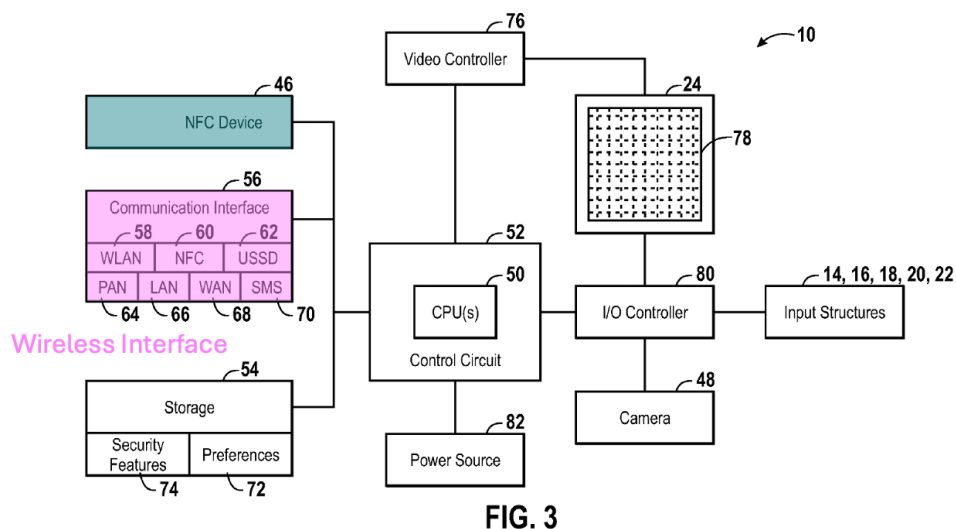
162. As discussed above, the payor device and the payee device communicate via said NFC interface. *See* Claim 1(c); *see also Lin (EX1004)*, 20:4-9, 62:4-8. The transaction processed successfully if the credit card verification server “determines that the specified credit card account is valid and is authorized to make the requested payment[.]” *Lin (EX1004)*, 34:1-10, 62:9-18, Figs. 4, 12A; *see also* Claim 1(i). In the Lin-Smith-Varadarajan-Hammad combination, the payment information is authorized by the server. *See* Claim 1(h).

C. Claim 3

1. **3: The method of claim 1, further comprising receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device.**

163. Lin teaches that the “financial servers 100 ... transmit a confirmation message [104] in the form of an electronic receipt ... to the payor device 92 if the transaction is processed successfully.” *Lin (EX1004)*, 35:24-30, 55:4-6, Fig. 4 (depicting receipt of confirmation message 104 from servers 100). As discussed in Claim 2, the payor receives the confirmation message over an NFC interface.

164. In addition to the NFC interface, Lin’s device also includes “a plurality of communication interfaces 56.” *Lin (EX1004)*, 20:23-30; 14:31-15:7.



Lin (EX1004), Fig. 3 (annotated).

165. Thus, Lin teaches receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least ... NFC interface.

166. Lin's communication interfaces 56 also include wireless interfaces including "a wireless LAN, such as an IEEE 802.11 x wireless network" and "a cellular data network, such as the Enhanced Data rates for GSM Evolution (EDGE) network or the 3G network (e.g., based on the IMT-2000 standard)." Lin (EX1004), 22:21-23:30. Lin teaches that a payment receipt can be sent by the financial server to the payor device over these network connections "established by way of a communications interface available on the ... payor device." Lin (EX1004), 61:31-62:4, Figs. 4, 11A, 12A. As discussed above, Lin's financial servers including a credit card verification server, which a POSITA would understand to include a payment processing authority. See Claim 1(j). It would have been obvious for the confirmation message 104 to be received from the financial server (payment processing authority) via a wireless interface of the payor device.

167. Alternatively, it would have been obvious for Lin's financial servers to utilize Hammad's payment processing system (a payment processing authority). See Claim 1(j). For the same reasons, it would have been obvious to configure Lin's payor device 92 to receive the confirmation message indicating that the transaction has been processed successfully from Hammad's payment processing system. *Id.*

D. Claim 4

1. ***4(a): The method of claim 3, wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment transactions performed by said device, in place of said selected issuer-payment information; and,***

168. For the reasons discussed in Claim 1(f), it would have been obvious to configure Lin's electronic device to generate a DCV (limited-use payment information) as taught by Varadarajan. Varadarajan further describes "including a device identifier in the DCV generator ... unique to each user device" in the DCV generation process." *Varadarajan (EX1006)*, [0053]. When using the DCV generator, "the DCV application ... generate[s] a user device identifier." *Varadarajan (EX1006)*, [0054]. There is a DCV generator for each card, e.g., selected issuer payment method. *Varadarajan (EX1006)*, [0052] ("[T]he DCV application can store DCV generators for multiple credit cards, debit cards, other DCV authorized payment or transaction cards, and for cards from different issuers or providers, on a single user device."). A POSITA would have understood, therefore, that in the DCV generation process the mobile device utilizes a unique device [e.g., device identifier] generated information. A POSITA would have been motivated to the use a device identifier in the DCV generation process to "further increase user security ... by detecting whether the application has been ported to another (unauthorized) device by an attacker." *Varadarajan (EX1006)*, [0052]

[0054]. As discussed, the DCV is used to replace issuer provided information, such as the “a CVC, CVV, CSC, PAN, account number, partial PAN and a portion of an account number[.]” *Varadarajan (EX1006)*, [0012]; *see also*, [0012]-[0013]. *Varadarajan* further teaches the verification values, such as the CVC, CVV, and CSC values are limited-in-use to specific issuer payment methods. *Varadarajan (EX1006)*, [0007].

169. Thus, it would have been obvious to configure Lin’s device to dynamically generate the DCV to replace a CVV, which is part of the issuer-payment information for the selected account.

2. 4(b): wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.

170. *Varadarajan* teaches that the proper verification value must be included in the payment information in order to complete a card-based transaction. *Varadarajan (EX1006)*, [0003], [0024], [0043]. Specifically, if the device-generated DCV, i.e., device generated limited-use information, does not match the authority-generated DCV, the transaction will not be authorized, i.e., rejected as invalid.

171. *Hammad* similarly teaches that if the service provider generated dCVV does not match the dCVV provided by the mobile device, the transaction is terminated. *Hammad (EX1007)*, 3:36-40, 8:47-50, Fig. 6.

172. Thus, it would have been obvious that when modifying Lin to include generation of DCV/dCVVs, Smith's PPAN, i.e., device account information, would be rejected if the DCV/dCVV generated by the device does not match the authority-generated DCV/dCVV.

E. Claim 5

1. ***5(a): The method of claim 3, wherein the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information; and,***

173. As discussed above, Varadarajan teaches generating a DCV (limited-used payment information) for use in a financial transaction. See Claim 1(f); *Varadarajan (EX1006)*, [0011], [0015], [0020], Fig. 4. Varadarajan teaches that the DCV generator includes a "device identifier" that identifies the user device conducting a transaction or requesting a DCV. *Varadarajan (EX1006)*, [0053]. In addition to the device information, account number, and CVV, Varadarajan teaches that the DCV generator uses a "data element," e.g., a string of alphanumeric characters representing a "challenge," or transaction related information, to generate a DCV which "authenticate[s] the user, user device ... or transaction to the provisioning server." *Varadarajan (EX1006)*, [0055].

a) Hammad's Teachings

174. Similar to Varadarajan, Hammad teaches dynamically generating a dynamic card verification value (“dCVV”) using an application on a mobile device for use in a mobile payment transaction. *Hammad (EX1007)*, 2:65-3:11, 3:51-4:6. The dCVV is generated from “at least two (e.g., at least three or four) dynamic data elements,” including an “application transaction counter (ATC),” “a cryptogram, digital signature, or hash value based on transaction data,” “a time of day, a current transaction amount, a terminal ID, a merchant ID, and a randomly generated number from a terminal, etc.,” or information “relat[ing] to a consumer’s portable consumer device ...and/or the consumer generally.” *Hammad (EX1007)*, 4:21-56, 4:62-7:5, Fig. 1. The dynamic data elements can also be used with “static data elements,” including “telephone number, a SIM card number, an account number, birthday, home address, expiration date, etc.” and “service code” to generate a dCVV. *Hammad (EX1007)*, 4:52-60, 5:2-5. The dCVV is generated by combining this information with multiple encryption keys, including a master derivation key, to the dynamic and static data elements, resulting in a 3-digit dCVV. *Hammad (EX1007)*, 5:34-6:39, Figs. 1-3. The master derivation key is provided by the service provider and used by the consumer device to derive additional keys and generate the dCVV. *Hammad (EX1007)*, 5:38-57, Fig. 2.

175. A dCVV is generated for each transaction and included with other payment data. *Hammad (EX1007)*, 4:61-65; *see also*, 4:61-6:34. The dCVV is

embedded into the payment data, which includes the account number, service code, PVKI, and/or PIN verification data, and transmitted to the point of sale terminal and then to the service provider. *Hammad (EX1007)*, 6:40-42, 6:49-7:27, 7:55-61, Figs. 4-5. The service provider uses the dCVV to determine the authenticity of the payment service. *Hammad (EX1007)*, 7:29- 7:61-8:50, Fig. 6. The service provider is a “payment processing organization or an issuer[.]” *Hammad (EX1007)*, 2:18-20.

b) Motivation to Combine

176. Based on the teachings of Hammad, it would have been obvious, and a POSITA would have been motivated to include multiple dynamic and static data elements, as taught by Hammad, in the DCV generation process as implemented in Lin-Smith-Varadarajan. For example, Hammad teaches generating a dCVV from “at least three or four” dynamic data elements and static data elements, which makes it “highly unlikely that a skimmer can determine a CVV.” *Hammad (EX1007)*, 4:46-51. These data elements include an ATC (transaction sequence counter); service code, expiration date, or PIN verification data (payment processing authority recognizable information); information relating to a “portable consumer device” (device-unique information); and an account number associated with a portable consumer device, which are combined using a master derivation key. *Hammad (EX1007)*, 4:21-5:5, 5:38-58.

177. Similarly, Varadarajan teaches combining a unique device identifier in its DCV generator (device-unique information) and “challenge” information from the service provider (payment processing authority recognizable information), among other information, to generate a DCV such that each DCV is “identifiable to the user device.” *Varadarajan (EX1006)*, [0053], [0055]. Varadarajan recognizes that it may be helpful to include provide additional data elements. *Varadarajan (EX1006)*, [0055]. A DCV is generated using a DCV key, which is generated by the issuer by combining a card verification key with the user’s account number and service code. *Varadarajan (EX1006)*, [0050].

178. A POSITA would have found it obvious to include this information in addition to Smith’s PPAN (device account number), in the generation of a DCV. As discussed in Section VI.C.2 and Claim 5(a), the use of dynamic card verification values was prevalent before 2012. Indeed, Hammad teaches including at least three or four dynamic data elements and static data elements, including an account number, in the generation of a dCVV. *Hammad (EX1007)*, 4:54-58, 4:61-5:5, Fig. 1. According to Hammad, the purpose of including more data elements in generating a dCVV is to combat, for example, a bad actor intercepting and re-using account information sent to a wireless POS terminal. *Hammad (EX1007)*, 1:38-45, 1:66-2:4, 3:60-67. A POSITA, therefore, would have recognized that including more data elements in generation of the DCV would decrease the likelihood that, even if the

payment data were intercepted, that the DCV could be regenerated. Indeed, Hammad recognizes that only including one data element to generate a dCVV is still susceptible to fraud and, therefore, proposes using “at least two (e.g., at least three or four) dynamic data elements to create a DCVV,” in addition to static data elements. *Hammad (EX1007)*, 1:46-2:4, 4:45-60. And Hammad provides an example of how to generate a dCVV using these types of data elements. *Hammad (EX1007)*, 4:60-6:47, Fig. 1-3. Thus, a POSITA would have been motivated to include more data elements in generating a DCV in Lin-Smith-Varadarajan, as taught by Hammad, in order to further prevent fraud.

179. A POSITA would have further recognized that modifications to Lin-Smith-Varadarajan-Hammad would be minimal as it would simply require additional inputs to Varadarajan’s DCV generator, in addition to the PPAN and CVV. Indeed, there are a finite number of combinations of data elements from which a DCV/dCVV can be generated and the determination of which data elements to use are simply an obvious design choice, any of which in combination increase security of the transaction and future transaction if the information were intercepted. Given Hammad’s teachings regarding how to generate such a dynamic verification value, and that a dCVV can be used in a contactless transaction (like Lin, Smith, and Varadarajan), a POSITA would have had a reasonable expectation of success. This modification is applying known techniques (e.g., using various data elements to

generated a card verification value to replace a static value) to improve similar devices (e.g., mobile devices used in payment transactions) in the same way that would have yielded the predictable result of increasing security of the transaction.

2. 5(b): wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction; and,

180. Hammad teaches generating a dCVV “for each transaction and for utilizing such value to verify that the payment service is authentic.” *Hammad (EX1007)*, 2:65-3:2; *see also*, 4:61-65. The dCVV is generated using at least two dynamic data elements that “change with each transaction.” *Hammad (EX1007)*, 4:40-42. Specifically, because the dCVV is generated from the ATC, which will change with each transaction, the dCVV will also change. *Hammad (EX1007)*, 4:22-33, 4:63-5:5.

181. As implemented in Lin-Smith-Varadarajan-Hammad, the DCV/dCVV is used to authorize a payment for a single transaction for the selected payment method.

3. ***5(c): wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device; and,***

182. As discussed in Claim 1(j), Varadarajan teaches that an authenticating server (*payment processing authority*) “independently generates on or more DCVs” (i.e., “verifiable dynamic CVV”) “with an equivalent method” to the user device. *Varadarajan (EX1006)*, [0045]; *see also*, [0033], [0056]. The authenticating server “regenerates a DCV independently and compares it with the user provided DCV for validity.” *Varadarajan (EX1006)*, [0056]. If the device-generated and authenticating server-generated DCV match, the DCV is authenticated and the transaction is authorized. *Varadarajan (EX1006)*, [0045], [0056], Fig. 4.

183. Hammad similarly teaches that a service provider, e.g., issuer or payment processing organization, both of which may be a payment processing authority (*see* Claim 1(j)), can “independently re-generate the dCVV for the given transaction” utilizing an “analogous process as described above” for the consumer device. *Hammad (EX1007)*, 8:37-41. If the dCVVs match, the service provider deems the payment application to be authentic and the transaction is approved. *Hammad (EX1007)*, 8:41-45, Fig. 6.

184. A POSITA would understand, therefore, that in order regenerate a DCV/dCVV in the proposed combination independently and authorize a transaction, an authenticating server or service provider (i.e., payment processing authority) would need to use the same method and information elements used by the mobile device to generate the DCV/dCVV. The two DCV/dCVVs are then compared to determine whether the transaction is authorized. *See* Claim 5(a); *see also* Claim 5(f).

185. It would have been obvious to modify the Lin with these teachings of Varadarajan and/or Hammad for the same for the reasons discussed in Claims 1(f), 1(j), and 5(a).

4. ***5(d): a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number; and,***

186. As discussed, Varadarajan teaches that an authenticating server “independently generate[s] one or more DCVs” (i.e., “verifiable dynamic CVV”) “with an equivalent method” to the user device. *Varadarajan (EX1006)*, [0045]; *see also*, [0033], [0056]. Hammad similarly teaches that “the service provider computer can independently re-generate the dCVV for the given transaction 645 utilizing a similar or analogous process” as described for the user device. *Hammad (EX1007)*, 8:37-41.

187. Hammad teaches that the dCVV can be generated from an ATC (device transaction sequence counter count), service code (issuer payment information), and information about the user (device user information). See Hammad (EX1007), 4:21-60, 4:62-7:5, Fig. 1; see also Claims 1(j), 5(a). Hammad further teaches that the service provider compares a received ATC with “the corresponding ATC stored on the service provider computer” (expected device transaction sequence counter count). Hammad (EX1007), 8:2-5, 8:41-47. Hammad also teaches that the service provider may determine if the other data elements match data elements at the service provider. Hammad (EX1007), 8:9-11. Hammad also teaches the service provider can “update the additional data which was previously stored on the service provider computer with the additional data received from the portable consumer device for subsequent authentications.” Hammad (EX1007), 9:23-27. Hammad teaches that the service provider is a “payment processing organization.” Hammad (EX1007), 2:18-20.

188. Smith teaches that the PPAN is stored at the financial institution server along with the actual account number. Smith (EX1005), [0014]-[0016], [0034]-[0037], [0039]-[0040], Figs. 1-3, 5-6.

189. Thus, a POSITA would understand that in the proposed combination, in order to independently generate a DCV/dCVV during the authorization process, the payment processing authority stores the ATC (device transaction sequence

counter count), PPAN (device account number), actual account information (expected issuer payment information), and user information (expected device user information). Further, a POSITA would understand that this information is, at a minimum, transitorily stored by a processor at the payment processing authority in order to be used during the independent DCV/dCVV generation process.

5. 5(e): an adjusting of said transaction sequence counter count on a per transaction basis; and,

190. As discussed in Claim 5(d), Hammad teaches that the consumer device maintains an ATC that is initially set by the service provider and that can be “incremented with each transaction.” *Hammad (EX1007)*, 4:23-26. The service provider will also adjust its ATC with that received from the consumer device after the dCVV is authenticated. *Hammad (EX1007)*, 8:41-47.

191. Thus, in the proposed combination, a POSITA would understand that ATC counter in the user device and at the payment processing authority are adjusted on a per-transaction basis. The use of such ATC counters in connection with payment transactions was prevalent at the time. *See* Section VI.A.1 (discussing Bona). A POSITA would have been very familiar with using such a counter in connection with mobile payment transactions. Thus, a POSITA would have recognized that implementing transaction counters in Lin’s system required only basic software modifications and routine skill. This modification would have been a combination of known elements (e.g., ATCs) to improve similar devices (e.g.,

mobile devices used in payment transactions) in the same way and that would yield the predictable result of increased security.

6. ***5(f): an authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching.***

192. Varadarajan teaches that if the “user inputted DCVs are matching to verifiable DCVs, the inputted DCVs are authenticated to the transaction server.” *Varadarajan (EX1006)*, [0044]; *see also*, [0033], [0045], [0056]. If the device-generated and authenticating server-generated DCV match, the DCV is authenticated and the transaction is authorized. *Varadarajan (EX1006)*, [0033], [0045], [0056], Fig. 4.

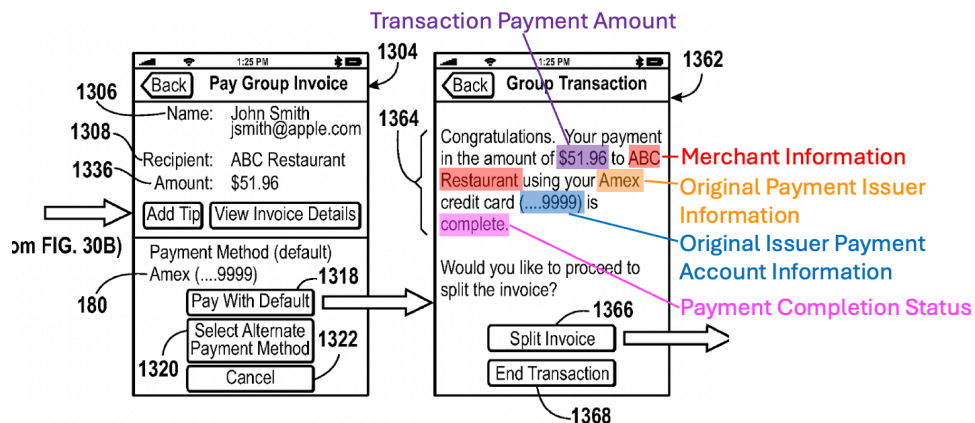
193. Hammad similarly teaches that the service provider authorizes the payment transaction “if the generated dCVV matches the dCVV received from” the consumer device. *Hammad (EX1007)*, 8:41-44; *see also*, 2:36-39, 8:21-23. If the dCVVs match, the service provider deems the payment application to be authentic” and the transaction is approved. *Hammad (EX1007)*, 8:41-44, Fig. 6 (steps 650, 655).

194. Thus, a POSITA would understand that in the proposed combination, the payment processing authority would authorize a transaction only if the device-generated and authority-generated DCV/dCVVs match.

F. Claim 7

1. **7: The method of claim 3, wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including: ... a transaction payment amount, ... a merchant information, an original issuer payment account information, an original payment issuer information, ... [and] a payment completion status.**

195. For the reasons described above, Lin teaches, or alternatively, renders obvious, visually conveying the received a confirmation message in the form of an electronic receipt, such as shown in Figure 30C. *See Claim 1(k).* As shown below, the electronic receipt visually conveyed includes a transaction payment amount, a merchant information, an original issuer payment account information, an original payment issuer information, and a payment completion status.



Lin (EX1004), Fig. 30C (annotated excerpt); see also, 131:29-132:2.

G. Claim 8

- 1. 8(a): The method of claim 1, wherein the generating the limited-use payment information is comprising: a device-specific account number; and,**
- 2. 8(b): a device-internal transaction sequence counter count; and,**

196. As discussed in Claim 5(a), the proposed combination teaches generating limited-use payment information using a PPAN (device-specific account number) and an ATC (device-internal transaction sequence counter).

- 3. 8(c): an information unique to the user and device which does not pass in the transaction; and,**

197. The proposed combination teaches, or renders obvious, generating the limited-use payment information unique to the user and device which does not pass in the transaction.

198. As discussed in Claim 1(f), Varadarajan teaches using a DCV generator to generate the DCV using a DCV key. *Varadarajan (EX1006)*, [0015], [0034] [0050]. The DCV key is information unique to a user because it is generated from a user's account number, expiration date, and service code (information unique to a user) and the DCV generator uses a device identifier (unique to the user and device) in generating a DCV that is "identifiable to the user device ... requesting a DCV." *Varadarajan (EX1006)*, [0049], [0053]. This information does not pass in the

transaction. This is because Varadarajan does not teach transmitting the DCV key or device identifier to the authenticating server.

4. ***8(d): at least one payment authority-supplied information which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements, and***

199. Varadarajan teaches that a DCV can be generated from a security challenge “provided by” the authentication server (payment authority). *Varadarajan (EX1006)*, [0055]. In the proposed combination, when a DCV/dCVV is generated from the security challenge (payment authority-supplied information), among other information, the security challenge does not pass in the transaction because it is received prior to any transaction being initiated (and outside the context of a transaction because it is a different interface) and would be hashed into the DCV during the DCV generation process. In other words, only the DCV passes during a specific transaction, not the security challenge or response to the security challenge itself.

200. Additionally, in the combination, it would have been obvious to use the actual account number or CVV in generating a DCV/dCVV. Hammad teaches using static data elements that “do not change from transaction to transaction,” such as the account number, to generate a dCVV. *Hammad (EX1007)*, 4:54-58. It would have been obvious to a POSITA use the actual account number or CVV (both static data

elements that do not change between transactions) in generating the dCVV for the same reasons detailed in Claim 5(a). *See also* Section VI.C.2. This would have further secured the transaction by allowing the validating authorities, which have knowledge of the actual account number and CVV, to determine whether a valid account number and/or CVV are used in the transaction. In the combination, the actual account number or CVV would not pass in the transaction, only the PPAN and DCV/dCVV passes with other payment data.

201. The complete device payment information (e.g., DCV/dCVV and other payment data) is only valid for payment if the numbers used to generate the DCV/dCVV comprise the same data as generated by the processing payment authority. *See* Claims 5(a), (c), (f).

5. ***8(e): wherein said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information.***

202. The generating of a DCV/dCVV in the proposed combination is limited in scope of use to the user-selected payment information for a single transaction by that device. *See* Claims 1(d)-(e). For example, because the ATC is used, it is limited to one transaction. *See* Claim 5(a)-(b). Similarly, because an account number is used, it is for the selected user payment method. *See* Claim 1(d).

203. As discussed in Claims 5(a) and 8(a)-(c), the combining includes an ATC (*transaction-specific sequence count*), device identifier or PPAN (*device-specific information*), user name, address or birthday (*user-specific information*), and service code, expiration date, or security challenge (*authority-specific information*). A POSITA would have found it obvious, and been motivated, to use additional dynamic or static data elements to generate a DCV/dCVV for same reasons discussed in Claim 5(a).

H. Claim 9

1. ***9: The method of claim 8, wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number, capable of passing in at least a portion of the device transaction payment information.***

204. Varadarajan teaches that the DCV, when used to replace the CVV, is a three-digit number. *Varadarajan (EX1006)*, [0021]. The DCV is generated using an ARQC generating algorithm in compliance with EMV standard protocol. *Varadarajan (EX1006)*, [0051]. A POSITA would understand that these algorithms generate cryptograms and that a DCV/dCVV are a cryptogram. As discussed in Sections VI.B.2 and VI.C.1, dynamic card verification values for use in a single financial transaction were well-known at the time and such dynamic numbers, e.g., a dynamic CVV, were, and still are, referred to as cryptograms. For example, Yeager describes a cryptogram as “encrypted data” that is “typically calculated from a series

of input data. *Yeager (EX1029)*, [0162]. Yeager further describes a dCVV as the “Cryptogram [] Name” for Visa’s dCVV and MasterCard’s CVC3. *Yeager (EX1029)*, [0162] (Table 4); *see also Collinge (EX1045)*, [0050] (describing a “payment cryptogram” as including a “CVC3”). The DCV/dCVV passes along with any other payment data to the authenticating server. *Varadarajan (EX1006)*, [0011], [0027], [0045], [0056].

I. Claim 10

- 1. 10: The method of claim 9, wherein the generating the limited-use payment information further utilizes a secure combination with a device key, and a payment issuer secret.**

205. Varadarajan teaches using a DCV key (device key) and a data element such as a server challenge (payment issuer secret) to generate a DCV. *Varadarajan (EX1006)*, [0055]. Hammad similarly teaches combining a master derivation key with the static and dynamic data elements to generate a dCVV. *Hammad (EX1007)*, 5:34-57. A POSITA would have found it obvious to combine this information, in addition to that described in Claims 5(a) and 8(a)-(c), (e), in generating the DCV/dCVV to further increase the security of the transaction. *See also* Claim 5(a).

J. Claim 11

1. *11(a): The method of claim 1, wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of:*
2. *11(b) a device payment transaction sequence counter count, and*

206. See Claim 5(a).

3. *11(c): at least one of a set comprising:*

a device-specific internal information associated with said device and also known to a payment processing authority; and,

at least one payment processing authority-specific information provided by a payment processing authority; and,

a payment issuer specific information provided by a payment issuer.

207. See Claims 5(a), (d), 8(e), 10 (describing combining service code, expiration date, service code, PIN verification data, server challenge (payment processing authority recognizable information), DCV key, and PPAN (payment issuer specific information) in generating a DCV/dCVV).

K. Claim 12

1. *12: The method of claim 1, wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information.*

208. As described in Claim 5, Hammad teaches generating a dCVV using various dynamic data elements, including a “terminal ID” and “a randomly

generated number from a terminal” (*NFC facility provided information*). Hammad (*EX1007*), 4:37-40. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction and tie the DCV/dCVV to the NFC reader. *See also* Claim 5(a).

L. Claim 13

- 1. 13: The method of claim 1, wherein the generating the limited-use payment information utilizes a merchant identifying information.**

209. Hammad teaches generating a dCVV using various dynamic data, including a “merchant ID” (*merchant identifying information*). Hammad (*EX1007*), 4:37-40. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction with information regarding the merchant. *See also* Claim 5(a).

M. Claim 14

- 1. 14: The method of claim 1, wherein the generating the limited-use payment information utilizes a transaction facility information.**

210. As discussed in Claim 13, Hammad teaches and a POSITA would have found it obvious to include a merchant ID (also *transaction facility information*) as a data element in generating the limited-use information to further increase the security of the transaction. *See also* Claim 5(a).

N. Claim 15

- 1. 15: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment amount.**

211. Varadarajan teaches generating the DCV from “total purchase or payment amount.” *Varadarajan (EX1006)*, [0055]. Hammad similarly teaches generating a dCVV using various dynamic data, including a “current transaction amount.” *Hammad (EX1007)*, 4:37-41. A POSITA would have found it obvious to include payment amount as additional data elements in generating the limited-use information to further increase the security of the transaction. *See also* Claim 5(a).

O. Claim 16

- 1. 16: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment facility type.**

212. Varadarajan teaches that the first six-digits of a PAN are an issuer identification number (payment facility type). *Varadarajan (EX1006)*, [0021]. Thus, when a DCV is generated from the entire PAN, it would use transaction facility information. Hammad also teaches generating a dCVV using various dynamic data, including a “terminal ID” (payment facility type). *Hammad (EX1007)*, 4:37-40. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction. *See also* Claim 5(a).

P. Claim 17

- 1. 17: The method of claim 1, wherein the generating the limited-use payment information utilizes an online transaction information.**

213. Varadarajan teaches that the data element used to generate the DCV can be a “payment amount.” [0055]. Varadarajan further teaches that its system can generate DCVs in card-not-present transactions, including “online transactions.” [0010], [0021]-[0022], [0029], [0042], [0045], Fig. 1.

214. A POSITA would understand the payment amount for an online transaction is online transaction information. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction. *See also* Claim 5(a).

Q. Claim 18

- 1. 18(a): The method of claim 1, further comprising:

dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number; and**

215. As discussed in Claim 5(a) and 10, the proposed combination renders obvious generating a DCV/dCVV by cryptographically combining an ATC (transaction sequence counter count), a PPAN (device account number) and a

server-provided challenge or master derivation key (payment processing authority secrets). A POSITA would understand that a DCV/dCVV is a cryptogram number. See Claim 9. The DCV/dCVV is used in place of a CVV (card validation value) that originated from the issuer. See *Varadarajan (EX1006)*, [0021].

2. ***18(b): wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number, via the incrementing of said transaction sequence counter count on a per-transaction basis, and using said updated transaction sequence counter count in said generation of said cryptogram; and,***

216. As discussed in Claim 5(b) and 8(e), the DCV is a one-time CVV (one-time limited-use card validation value number). *Varadarajan (EX1006)*, [0020], [0023], [0045], [0047]. Hammad further teaches that an ATC is incremented on a per-transaction basis and the updated count is used in generating the dCVV. *Hammad (EX1007)*, 4:22-31. The current value of the ATC, incremented from the previous transaction, is used in generating the dCVV. *Hammad (EX1007)*, 6:61-8:34.

3. ***18(c): wherein said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device.***

217. The DCV/dCVV is used in place of the CVV (issuer supplied card validation value number) in performing the payment transaction by the device. See Claims 1(f), 18(a).

**XI. GROUND 2: CLAIM 6 IS OBVIOUS OVER LIN, SMITH,
VARADARAJAN, HAMMAD AND KRANZLEY**

A. Claim 6

1. ***6(a): The method of claim 3, wherein the generating the limited-use payment information further utilizes a secure combination of said information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information; and,***

218. See Claim 3.

219. As discussed in Claim 5(a) and 8(d), the generating of a DCV/dCVV (limited-use payment information) in the proposed combination utilizes a secure combination of Smith's PPAN (device account number), Hammad's ATC (a device sequence counter count), Varadarajan's DCV generator (device-specific information), and DCV key or security challenge (payment processing authority specific information).

2. ***6(b): a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority; and,***

220. As discussed in Claim 5(c), the payment processing authority performs the same combination of the same information to verify the DCV.

221. Hammad teaches that the ATC is stored at the service provider. *Hammad (EX1007)*, 8:2-5, 8:41-47. Smith teaches that the PPAN is stored at the

financial institution server along with the actual account number. *Smith (EX1005)*, [0014]-[0016], [0034]-[0037], [0039]-[0040], Figs. 1-3, 5-6.

222. Varadarajan teaches that the authenticating server independently generates a DCV using the same process as the user device, i.e., using the same DCV generator and DCV key as used by the user device. *See* Claim 5(c). A POSITA would have understood that the DCV key and DCV generator used to regenerate a DCV at the authentication server would have been stored at the authenticating server. *See Varadarajan (EX1006)*, [0043] (“The authenticating server 150 uses information specific to the user’s DCV generator 100 provided by the provisioning server 155 to independently generate DCVs for that user’s credit/debit card account, for the purpose of verifying the inputted DCVs as authenticated DCV inputs for that user’s credit/debit card.”). Thus, a POSITA would have understood, or found it obvious, to store at the authenticating server the information required to independently generate a DCV.

3. *6(c): a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid; and,*

223. As discussed in Claims 5(c) and (f), Varadarajan’s authenticating server and Hammad’s payment processing authority (each a payment processing authority) validates a payment by determining whether the device generated DCV/dCVV matches the authenticating server DCV/dCVV.

4. 6(d): a conveying of said validation result as a declining or accepting of said transaction payment; and,

224. As discussed in Claim 2, Lin teaches transmitting a confirmation message in the form of a receipt if the transaction is processed successfully (accepting of said transaction payment). Specifically, the credit card verification server “determines that the specified credit card account is valid and is authorized to make the requested payment[.]” *Lin (EX1004)*, 34:1-10, 62:9-18, Figs. 4, 12A. Lin also teaches that if the payment transaction is not authorized (declining ... of said transaction payment), the payor may be notified to select a different payment option that has sufficient funds. *Lin (EX1004)*, 54:6-11, 80:30-81:5, Figs. 12A-B, 14J; *see also* Claims 2, 4. As discussed in Claim 1(k), it would have been obvious and a POSITA would have been motivated to configure Lin’s device to convey these results to the user.

5. 6(e): upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction.

225. As discussed in Claim 1(i), Hammad teaches a system including a service provider, such as a payment processing system or issuer, that validates a dCVV. In the case of only a payment processing system validating a dCVV, a POSITA would have understood that the payment data, including the original account number, would still be sent to the issuer to determine whether the account has sufficient funds (settlement of said transaction).

a) Kranzley's Teachings

226. Like Lin, Smith, Varadarajan, and Hammad, Kranzley teaches a mobile device having a payment application thereon for conducting payment transactions. *Kranzley (EX1008)*, [0019]. Similar to Varadarajan and Hammad, the mobile device generates a dynamic code or other dynamic variable that is sent, along with other payment information, to a payment processing system for validation. *Kranzley (EX1008)*, [0023]-[0027], [0030], [0035], Figs. 3, 6. In certain instances, the mobile device sends a static VPAN, i.e., account number different than the actual account number (similar to Smith's PPAN), and an expiration date for the static VPAN and dynamic code (used in place of a CVV) to a payment provider to confirm validity of the dynamic code and determine an actual account number associated with the static VPAN. *Kranzley (EX1008)*, [0035]-[0037], [0041]-[0042], [0044]-[0045], Figs. 1B, 3, 5-6. Once confirmed, the payment provider sends the actual PAN to the issuer for authorization, including determining whether the account has sufficient funds (settlement of said transaction). *Kranzley (EX1008)*, [0037], [0048].

b) Motivation to Combine

227. Based on the teachings of Kranzley, it would have been obvious, and a POSITA would have been motivated to include Kranzley's payment processing authority to validate dynamic payment data and subsequently send, at least, original account information to an issuer for authorization. Kranzley teaches having the

payment provider, and not the issuer, check the dynamic code allows for new validation processes (including generating and tracking VPANs) to be implemented or deployed without having to update issuer systems. *Kranzley (EX1008)*, [0049].

228. Lin, Varadarajan, and Hammad already teach using multiple financial servers (e.g., transaction server, authenticating servers, payment processing and issuer systems) in authorizing a payment. A POSITA would have been motivated to configure the Lin-Smith-Varadarajan-Hammad system to use these servers, such as payment processor and issuer, in the way and for the same reasons expressly taught by Kranzley. Specifically, it would allow for Smith's PPANs to be generated and tracked by the payment processing authority. This would free up resources at the issuer and also not require updates to the issuer when changes were made to the generation and distribution of PPANs in the combination, as taught by Kranzley.

229. A POSITA would recognize that modifying Lin-Smith-Varadarajan-Hammad in this way would only require basic software modifications and routine skill as Hammad teaches using a payment processing authority to validate the DCV/dCVV (*limited-use payment information*). See Claim 1(j). Thus, the payment processing system would simply send the payment information to the issuer for authorization, while retaining the additional benefits taught by Kranzley.

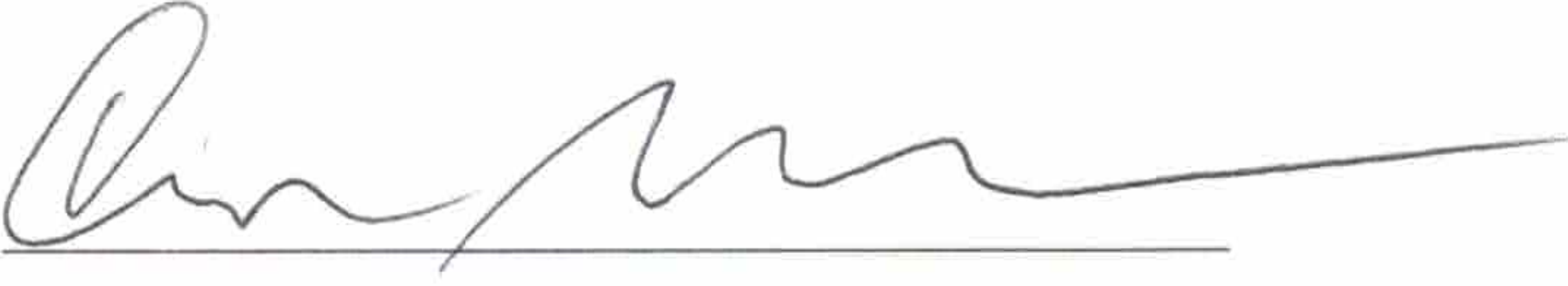
230. Because the components and functionalities are largely the same, there would have been a reasonable expectation of success configuring Lin's financial

servers to include a payment processing system and issuer system in this way. *See also* Claim 1(j). This would have been a combination of known elements that would yield the predictable result of a secure payment in the existing payment processing architecture.

XI. CONCLUSION

231. 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.

Date: 6/23/2025

By: 
Dr. Clifford Neuman

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.