

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

CARDWARE INC.
Patent Owner

Case No. IPR2025-01150
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	15
A.	EDUCATIONAL BACKGROUND AND PROFESSIONAL EXPERIENCE	15
II.	METHODOLOGY AND MATERIALS CONSIDERED	18
III.	OVERVIEW AND LEGAL STANDARDS.....	19
A.	PERSON OF ORDINARY SKILL IN THE ART	20
B.	OBVIOUSNESS	21
C.	CLAIM CONSTRUCTION	26
D.	PRINTED SUBJECT MATTER	26
IV.	LEVEL OF A PERSON OF ORDINARY SKILL.....	27
V.	BACKGROUND OF TECHNOLOGY.....	28
A.	THE EVOLUTION OF PAYMENT CARDS	29
1.	<i>Magnetic Stripe Cards.....</i>	<i>29</i>
2.	<i>Smart/Chip Cards.....</i>	<i>31</i>
3.	<i>Europay, MasterCard, and Visa (EMV) Standard</i>	<i>32</i>
B.	CONTACTLESS PAYMENTS.....	33
1.	<i>Near Field Communications</i>	<i>33</i>
a)	Active Mode.....	35
b)	Passive Mode	37
2.	<i>Contactless EMV Payment Cards</i>	<i>38</i>
3.	<i>Mobile Devices and Mobile Wallets</i>	<i>39</i>
VI.	CARD EMULATION MODE.....	42
A.	CONTACTLESS ATMS.....	44
B.	PAYMENT CREDENTIAL SECURITY FEATURES.....	48
1.	<i>Alternatives to a Payment Account Number (PAN)</i>	<i>49</i>
2.	<i>Alternatives to Static Card Verification Values</i>	<i>52</i>
VII.	OVERVIEW OF THE '538 PATENT	54
A.	SUMMARY OF THE '538 PATENT	54

B.	FIELD OF ENDEAVOR.....	54
C.	PROBLEM PURPORTEDLY SOLVED BY THE INVENTORS OF THE '538 PATENT	55
D.	THE PROSECUTION HISTORY OF THE '538 PATENT	56
VIII.	SUMMARY OF UNPATENTABILITY	57
IX.	OVERVIEW OF THE PRIOR ART	57
A.	KALGI.....	57
1.	<i>Kalgi is Analogous</i>	58
B.	KHAN.....	58
1.	<i>Khan is Analogous</i>	59
C.	VARADARAJAN	59
1.	<i>Varadarajan is Analogous</i>	60
D.	HAMMAD	60
1.	<i>Hammad is Analogous</i>	62
E.	SMITH	63
1.	<i>Smith is Analogous</i>	64
F.	BAUER	66
1.	<i>Bauer is Analogous</i>	66
G.	KRANZLEY	67
1.	<i>Kranzley is Analogous</i>	67
X.	GROUND 1: CLAIMS 19 AND 24 ARE OBVIOUS OVER KALGI, KHAN, AND VARADARAJAN	69
A.	CLAIM 19.....	69
1.	<i>19(pre): A method of performing an online payment transaction, the method comprising:</i>	<i>69</i>
2.	<i>19(a): receiving an input signal at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface of the electronic device;.....</i>	<i>70</i>
a)	Khan's Teachings	74

b)	Motivations to Combine.....	75
3.	<i>19(b): a displaying of the payment request notification at a touch-screen display user-interface of the electronic device; and, ...</i>	<i>76</i>
4.	<i>19(c): upon an authorizing of a valid device user, displaying at least one user-selectable payment account option, and requesting a user approval of payment, via the touch-screen display user-interface;</i>	<i>77</i>
5.	<i>19(d): receiving, from a valid device user, a payment selection and authorization approval input on the electronic device;</i>	<i>79</i>
6.	<i>19(e): generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and</i>	<i>80</i>
a)	Varadarajan's Teachings.....	82
b)	Motivations to Combine.....	84
7.	<i>19(f): combining said at least one limited-use numbers, with said selected account information, to form a complete payment information; and, ...</i>	<i>86</i>
8.	<i>19(g): wherein the receiving of a user payment approval authorization through the user-interface of the electronic device, is comprising a displaying on said display at least a portion of information comprising: the payment request, the merchant, the amount, and the transaction information; and,.....</i>	<i>87</i>
9.	<i>19(h): receiving a user input providing for at least one transaction authorization actions, from a set of actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method; and,.....</i>	<i>87</i>
10.	<i>19(i): on receiving said user payment approval authorization input, a transmitting by the wireless</i>	

	<i>interface of the approved complete payment information for the online transaction.</i>	88
B.	CLAIM 24.....	90
1.	<i>24: The method of claim 19, wherein the user selecting of a payment method at an electronic device comprises receiving a user touch input selection, via the user interface, of a displayed payment method option, on the device touch-screen display interface.</i>	90
XI.	GROUND 2: CLAIMS 20 AND 22 ARE OBVIOUS OVER KALGI, KHAN, VARADARAJAN, AND HAMMAD	91
A.	CLAIM 20.....	91
1.	<i>20(a): The method of claim 19, further comprising:.....</i>	<i>91</i>
	<i>dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuing authority, and wherein dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count, a user information, a payment account number, information and secrets known to a payment processing authority; and.....</i>	<i>91</i>
a)	Varadarajan's Teachings	91
b)	Hammad's Teachings	92
c)	Motivation to Combine	94
2.	<i>20(b): wherein further, said dynamically generating said card validation value number results in a one-time limited-use payment information, on incrementing the device transaction sequence counter count on each transaction payment, and said device combining said current transaction sequence count at the instant of generating said cryptogram number.</i>	<i>96</i>
B.	CLAIM 22.....	96

1. 22(a): *The method of claim 19, further comprising:.....* 96
generating a limited-use security code number for
use in place of a card issuer card security
code, by cryptographically combining
information from at least one of a set of
information comprising: a device
transaction sequence counter; a device
account number; a payment account
information, device secrets; payment
processing authority secrets; and..... 96
2. 22(b): *displaying the limited-use security code*
number on the user-interface of the device display. 97

**XII. GROUND 3: CLAIM 21 IS OBVIOUS OVER KALGI,
KHAN, VARADARAJAN, AND SMITH 98**

- A. CLAIM 21 98
 1. 21(a): *The method of claim 19, wherein at least a*
portion of said limited-use number comprises a
static device account number,..... 98
and wherein the static device account number is of
a limited scope of valid use to a specific
device, ... 98
 - a) Smith's Teachings 98
 - b) Motivation to Combine 101
 2. 21(b): *and wherein further a payment processing*
authority provides said device account number
unique for the specific electronic device, in place
of payment issuer information, in performing
payment transactions by the electronic device, and
further comprising: 105
 3. 21(c): *performing a payment transaction by the*
electronic device including the dynamically
generated limited-use number;..... 106
 4. 21(d): *combining the dynamically-generated*
number and the static device account number
within a device-generated complete payment
information; and..... 106

5. *21(e): conveying said device-generated complete payment information, in place of a selected payment issuer information, when the device is performing payment transactions; and 106*
6. *21(f): wherein a using of said static device account number without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage. 107*

XIII. GROUND 4: CLAIM 25 IS OBVIOUS OVER KALGI, VARADARAJAN, AND SMITH 107

A. CLAIM 25.....107

1. *25(pre): A non-transitory, computer-readable medium storing computer executable instructions that when executed by one or more processors, cause the one or more processors to:..... 107*
2. *25(a): accept a priming action of the electronic device by an identified valid device user, identified from the device inputs; 108*
3. *25(b): enable the electronic device for imminent performance of a payment operation responsive to the priming action of said valid user; 110*
4. *25(c): display a summary of online purchase information including the merchant information and the purchase amount; and, ... 112*
5. *25(d): display at least one selectable issuer payment account methods on a display; and, ... 112*
6. *25(e): receive a payment selection and approval authorization from said valid device user via a human input sensing at the device; and 113*
7. *25(f): responsive to receiving a valid user transaction payment approval, generate a device-specific limited-use payment information for use in place of at least a portion of said selected issuer payment account information on the device,..... 113*
8. *25(g): form a complete combined device payment information from a dynamically generated portion*

*and a statically generated portions stored in a
memory of the device,..... 114*

9. *25(h): wherein the communication interface is
operable to transmit said complete device payment
information from said electronic device to the
recipient of the online purchase transaction; and..... 115*
10. *25(i): wherein further the processor is operable to
receive an approval and a denial confirmation
from an online payment facility of the complete
device payment information, and cause the display
to visually convey a status of the online purchase
transaction..... 116*

**XIV. GROUND 5: CLAIMS 28-30 ARE OBVIOUS OVER
KALGI, KHAN, VARADARAJAN, HAMMAD AND
SMITH 118**

A. CLAIM 23 118

1. *23(a): The method of claim 19, wherein a payment
processing authority verifying and authorizing a
transmitted limited-use number based on a time of
use, and cryptographically combining a
transaction sequence count information; a device
account number; a user account information; a
payment issuer information; a payment processing
authority secrets; a transaction information; and,..... 118*
2. *23(b): further comprising: receiving an
authorization of said transaction, responsive to
verifying a valid limited-use number appearing in
a transaction information in place of the payment
issuer information; and 120*
3. *23(c): a rejecting by the payment processing
authority, on a detecting as invalid at least one
verification test, from a set of tests comprising:..... 121*
*a mis-matching of the transacted limited-use
number, and the authority
cryptographically-combined number;..... 121*

	<i>a transactional use of a device account number outside of its limited scope of valid payment reader facility use;</i>	<i>121</i>
	<i>a transactional use outside of a valid time window;</i>	<i>121</i>
	<i>a transactional re-use of a number limited to a one-time use; and, ...</i>	<i>121</i>
	<i>a transactional use of an expired number outside of a limited time-of-use.</i>	<i>121</i>
B.	CLAIM 28.....	122
1.	<i>28(a): The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further causes the one or more processors to perform:</i>	<i>122</i>
	<i>a combining of a static device-specific payment account information, a device generated information, and other user and account information stored on the device which is uniquely identifying the specific user, specific selected account, and the specific device; and, ...</i>	<i>122</i>
2.	<i>28(b): a generating of a limited-use payment information by the one or more device processors cryptographically generating at least one one-time limited-use cryptogram numbers; and, ...</i>	<i>123</i>
3.	<i>28(c): wherein the one or more device processors are further operable to combine said limited-use static device account information and said one- time use cryptogram number(s) to produce the complete combined device payment information; and, ...</i>	<i>123</i>
4.	<i>28(d): wherein the one or more device processors are further operable to transmit said complete payment information in place of said user-selected payment account information in a device payment transaction; and, ...</i>	<i>124</i>

5. 28(e): wherein the one or more device processors are further operable to display at least a portion of said user-specific selected account information associated with said complete device payment information used during said transaction, via a user interface disposed of the device..... 124
- C. CLAIM 29.....125
1. 29(a): The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more processors to dynamically generate a one-time limited-use cryptogram number, via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority, and selected from a set of information known and stored at both said payment authorities, and on said device, including:..... 125
- a transaction sequence counter, ... 125
- a device account number, ... 125
- ... 125
- a payment processing authority secret, ... 125
- a user information, ... 125
- a payment account information, ... 125
- ... 125
- a payment amount, transactional information; and, ... 125
2. 29(b): wherein said one or more processors uses said one-time limited-use cryptogram number in place of at least a portion of an issuer's static payment information, in a payment transaction using said payment account; and, ... 128
3. 29(c): wherein said payment authorities are operable to recognize from the transactional payment information, the correct set of user, device

and account specific information to be cryptographically combined into an authority computed cryptogram, for comparing with device transmitted limited-use payment information; and, ... 128

4. *29(d): wherein said payment processing authorities are operable to deny as invalid a transaction including a cryptogram not matching an authority computed cryptogram; and,..... 128*

5. *29(e): wherein said payment authorities are operable to approve as valid a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,..... 129*

6. *29(f): wherein said device is operable to receive an approval and a denial status of said transaction, from said payment authorities, and visually convey said transaction status in the user-interface on the display disposed of the device. 129*

D. CLAIM 30 130

1. *30(a): The electronic device of claim 25, further comprising a processor and a non-transitory, computer-readable medium storing computer executable instructions that when executed by the one or more processors, cause the one or more device processors to dynamically generate a one-time limited-use cryptogram number by a cryptographic combination, of at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic device, and selected from a set of information including: 130*
a transaction sequence counter; 130
a user payment account number; 130
a device payment account number; 130
a device secret; device keys;..... 130
a payment issuer original account information; 130
a payment issuer device account information; 130

a payment processing authority secret; 130

a transaction information; 130

and a user private information; and, ... 130

2. *30(b): wherein said cryptogram is operable to be used in place of at least a portion of an issuer's static payment information, in a payment transaction for said selected payment account; and, ... 131*

3. *30(c): wherein said payment processing authority is operable to deny as invalid, a transaction including a cryptogram not matching a payment processing authority computed cryptogram; and, ... 131*

4. *30(d): wherein said payment processing authority is operable to approve as valid, a transaction including a cryptogram matching the payment processing authority computed cryptogram; and, ... 131*

5. *30(e): wherein said user device is operable to receive an approval and a denial status of said transaction information validation, and visually convey said transaction status in the user-interface on the display disposed of the device; and, ... 131*

6. *30(f): wherein said user device is operable to emulate the behavior of an issuer account payment transaction, when said complete device payment information is used in electronic payment facilities. 132*

XV. GROUND 6: CLAIM 26 IS OBVIOUS OVER KALGI, VARADARAJAN, HAMMAD, SMITH AND BAUER 132

A. CLAIM 26 132

1. *26(a). The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more processors to: 132*

receive the priming action of a user via the device human input sensors; 132

2. 26(b): *identify an authorized valid device user through a human to device inputs, selected from at least one security challenge, of a set of human to device input challenges comprising: 133*
a correct passcode touch entry sequence, ... 133
a correct touch gesture, ... 133
... 133
a biometric recognition of a valid user, ... 133
... 133
a security question which a valid user could answer correctly, and 133
3. 26(c): *receiving a correct user response input, from a security challenge presented on the device display; and 133*
4. 26(d): *responsive to receiving an incorrect user response input, offer a reduced number of additional challenge attempts before failing the user authorization at the device, and denying the payment authorization. 134*
 - a) Bauer's Teachings 135
 - b) Motivations to Combine 136

XVI. GROUND 7: CLAIM 27 IS OBVIOUS OVER KALGI, VARADARAJAN, HAMMAD, SMITH, AND KRANZLEY 137

- A. CLAIM 27 137
1. 27(pre): *The non-transitory, computer-readable medium of claim 25, wherein the one or more processors include a cryptographic processor, and wherein the executable instructions further cause the one or more processors to: 137*
 - a) Khan's Teachings 137
 - b) Motivation to Combine 138
 2. 27(a): *cryptographically compute a dynamically generated one-time-use cryptogram number, ... 139*

3.	<i>27(b): and combine said dynamically generated portion with a static device-specific account number known to a payment processing authority and limited in use to the device use in place of an issuer payment method; and,.....</i>	<i>140</i>
4.	<i>27(c): wherein further said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count, a payment account information, a user information, and information stored in the device and specific to the device and which is not communicated in the transaction; and, ...</i>	<i>140</i>
5.	<i>27(d): wherein said transaction sequence counter, said information and said secrets are known to both said device, and to said payment processing authority; and, ...</i>	<i>140</i>
6.	<i>27(e): wherein further said static device-specific device account number is known to a payment issuer, and has a device-specific expiration date of limited duration of validity; and,.....</i>	<i>141</i>
	a) Kranzley's Teachings	141
	b) Motivations to Combine.....	141
7.	<i>27(f): wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram, ...</i>	<i>142</i>
8.	<i>27(g): and transmitting said complete device payment information when said issuer payment account method is selected.</i>	<i>143</i>
XVII.CONCLUSION		144

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 19-30, and my opinions are limited to those claims. A true and correct copy of my Curriculum Vitae, which provides further details about my background and experience, is appended to this Declaration.

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. METHODOLOGY AND 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. 2013/0013499 (“Kalgı”)
1005	U.S. Pub. No. 2014/0019367 (“Khan”)
1006	U.S. Pub. No. 2011/0184876 (“Varadarajan”)
1007	U.S. Patent No. 7,740,168 (“Hammad”)
1008	U.S. Pub. No. 2010/0125508 (“Smith”)
1009	WO Publn. No. 2012/042262 (“Bauer”)
1010	U.S. Pub. No. 2010/0125509 (“Kranzley”)
1011	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. BACKGROUND OF TECHNOLOGY

31. 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.

32. 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.

33. 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,

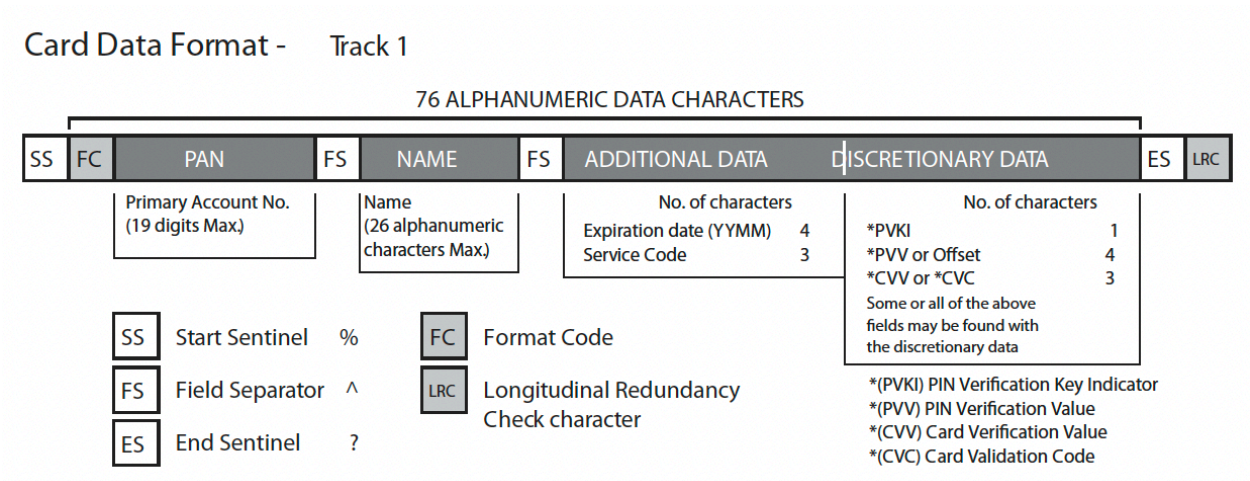
slow, and prone to errors” therefore a need for magnetic stripe cards arose. *IBM (EX1020)*, 1.

A. The Evolution of Payment Cards

1. Magnetic Stripe Cards

34. 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.

35. 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:

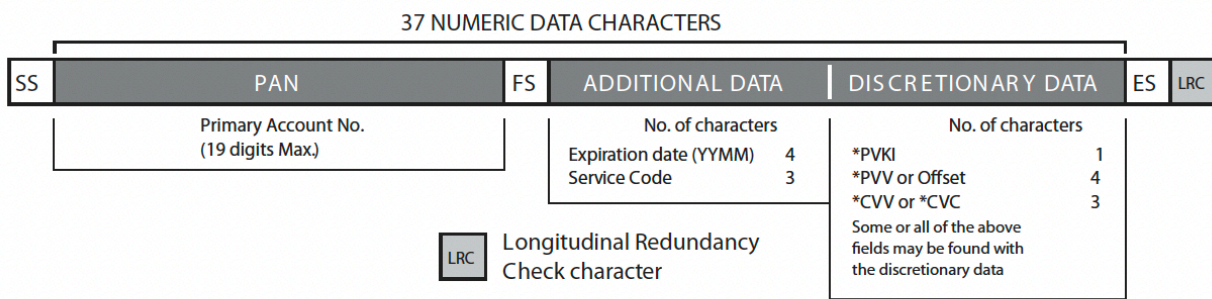


MagTek (EX1022), 1. On a card’s track:

“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 or 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 (EX1043), [0102]. Track 2 data includes the following data:

Card Data Format - Track 2



Magtek (EX1022), 1.

36. 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.

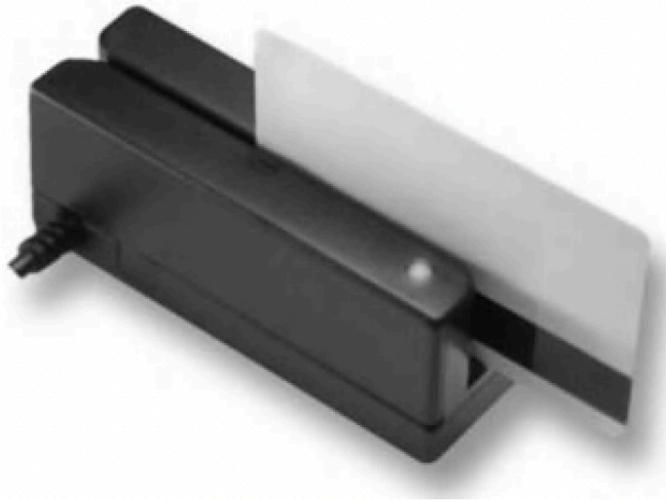


Figure 2.15 Magnetic stripe card.

Coskun (EX1021), Figure 2.15.

37. “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

38. 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.

39. 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*

40. 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

41. 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.

42. 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.

43. 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.

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

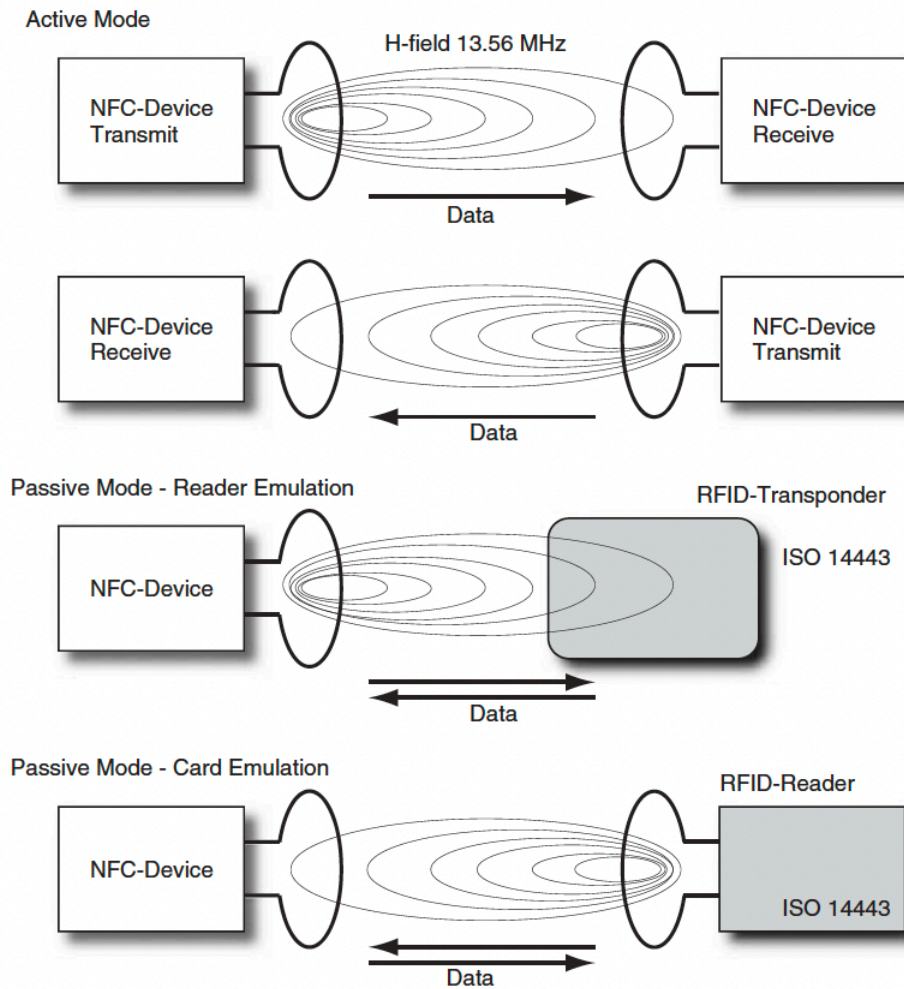


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzeller (EX1024), 58.

a) Active Mode

45. 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.

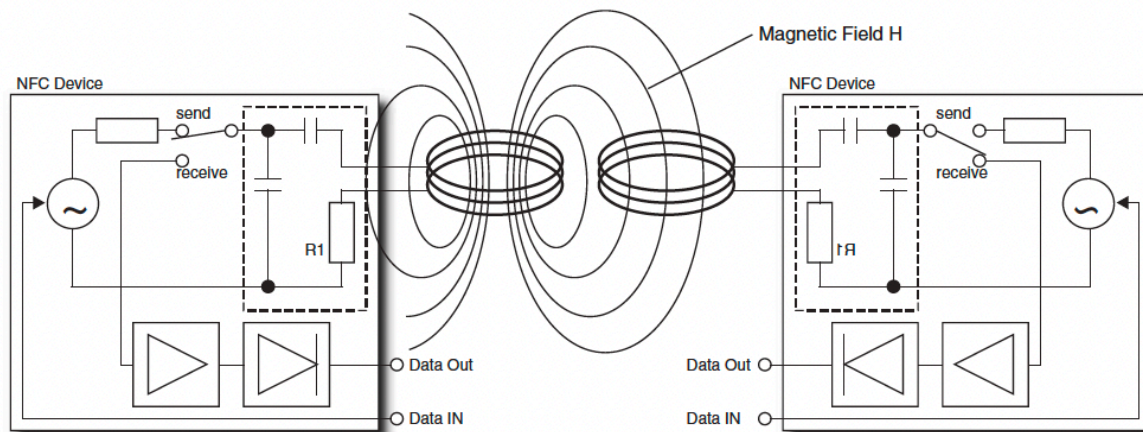


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (EX1024), 58.

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

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

b) Passive Mode

47. 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.

48. 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.

49. 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***

50. “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.

51. 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.

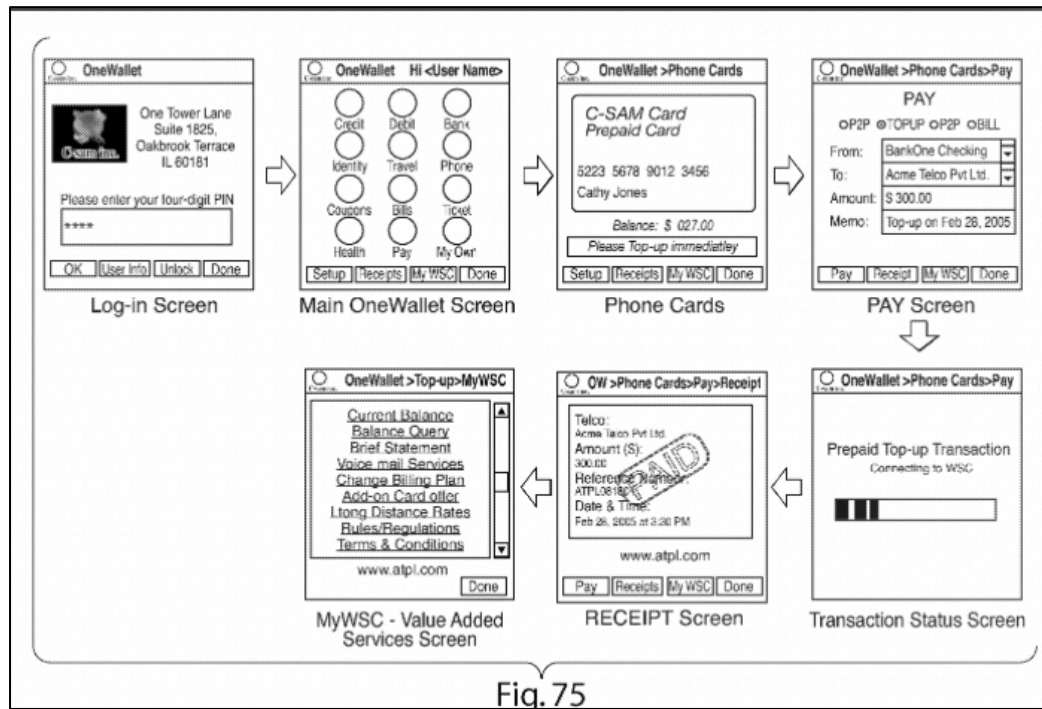
3. *Mobile Devices and Mobile Wallets*

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

53. 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.

54. 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.

55. 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.

56. 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.

57. 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.

VI. CARD EMULATION MODE

58. 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.”)

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

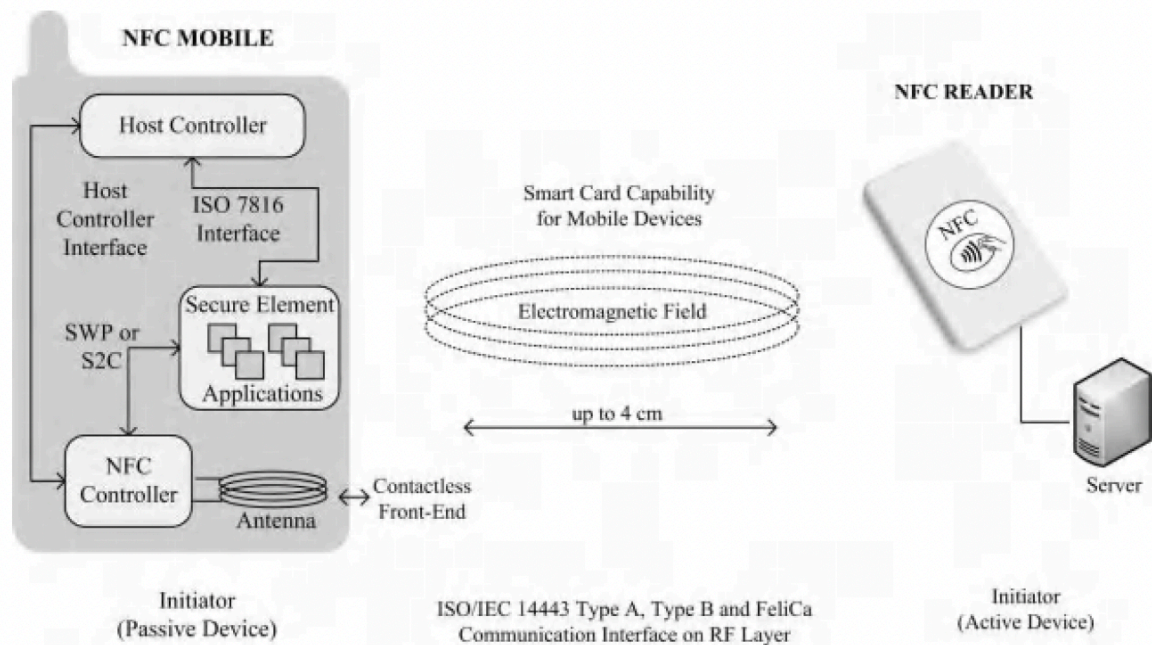


Figure 3.32 Communication architecture of card emulation operating mode.

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

60. 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

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

62. 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.

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

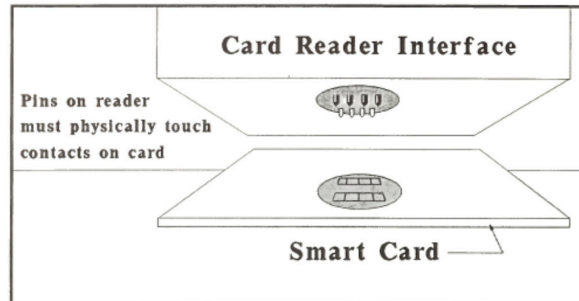


Figure 4. Contact-Type Smart Card Interface

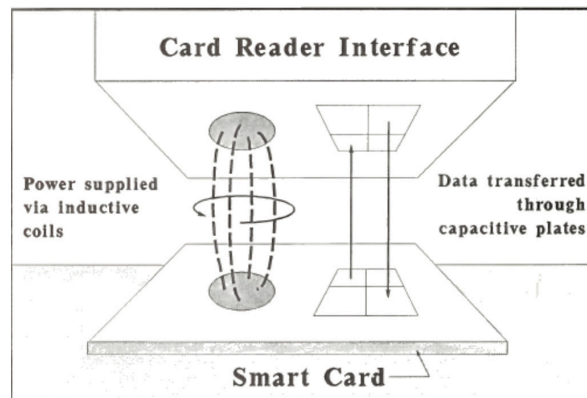
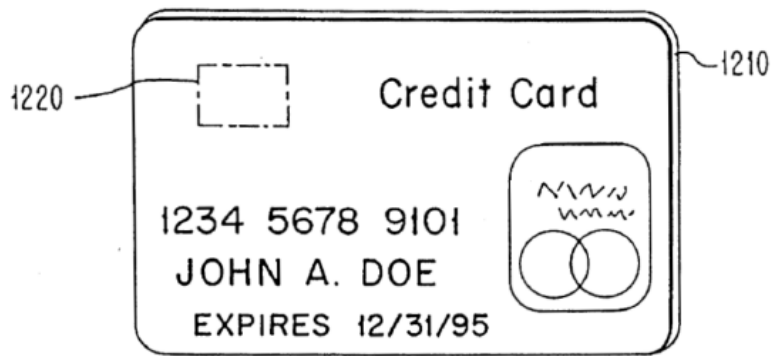


Figure 5. Non-Contact-Type Smart Card Interface

64. 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.”).

65. 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.

66. 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.

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

68. 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.

69. 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.

70. 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.

71. 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

72. 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)

73. 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.

74. 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.

75. 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].

76. 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].

77. 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*

78. 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].

79. 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].

80. 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.

81. 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].

82. 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.

VII. OVERVIEW OF THE ’538 PATENT

A. Summary of the ’538 Patent

83. 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

84. 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.

85. 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 (EX1001)*, 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

86. 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.

87. 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 (EX1001)*, 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 (EX1001)*,

1:67-2:4. To solve these problems, the “Summary of the Invention” describes “multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe” for the “purpose of emulating a standard credit card.” ’538 Patent (EX1001), 2:14-18. The “Summary of the Invention” further describes a method of performing a transaction that includes “generating a limited duration credit card number.” ’538 Patent (EX1001), 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

88. 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.

VIII. SUMMARY OF UNPATENTABILITY

Ground	Proposed Ground of Unpatentability	Exhibits
1	19, 24	Kalgi (EX1004), Khan (EX1005), and Varadarajan (EX1006)
2	20, 22	Kalgi, Khan, Varadarajan, and Hammad (EX1007)
3	21	Kalgi, Khan, Varadarajan, and Smith (EX1008)
4	25	Kalgi, Varadarajan, and Smith
5	23, 28-30	Kalgi, Khan, Varadarajan, Hammad, and Smith
6	26	Kalgi, Varadarajan, Hammad, Smith, and Bauer (EX1009)
7	27	Kalgi, Varadarajan, Hammad, Smith, and Kranzley (EX1010)

89. Above, I have reproduced the Proposed Ground 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. Kalgi

90. Kalgi teaches methods and systems for electronic purchase transactions, including transactions via a web browser. *Kalgi (EX1004)*, Abstract,

[0003], [0028]. Kalgi describes use of an electronic wallet checkout platform that supplies a consistent user experience across websites. *Kalgi (EX1004)*, [0027]-[0028]. To initiate a transaction, the user must be authorized and select a payment type. *Kalgi (EX1004)*, Abstract, [0029], [0043], [0057], [0059], Figs. 1, 5.

1. *Kalgi is Analogous*

91. In my opinion, Kalgi is analogous art to the '538 Patent. First, Kalgi Kalgi discloses conducting secure payment transactions. *Compare '538 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Kalgi (EX1004)*, Abstract, [0027], Fig. 1.

92. Second, a POSITA would have understood¹ Kalgi to be reasonably pertinent to the particular problems with which the inventor of the '538 Patent was involved because Kalgi is directed to increasing the security of payment transactions. *Compare '538 Patent (EX1001)*, 1:23-28, 1:63-2:4, 9:21-28 *with Kalgi (EX1004)*, Abstract, [0027], Fig. 1.

B. Khan

93. Khan teaches commercial transactions between a portable device and a transaction provider in a wireless environment. *Khan (EX1005)*, [0002], [0018],

¹ For brevity here and elsewhere in my analysis, I refer to what a POSITA would have known or understood in the past tense. What I mean by this stylistic shorthand, wherever I use it herein, is my corresponding analysis refers to what a POSITA would have known or understood at the time of the earliest possible priority date of the '538 Patent.

[0021], Figs. 2-4. The portable device generates credit card data, including an alias card number, cryptographic data, a counter, merchant ID, etc. *Khan (EX1005)*, [0022]-[0024], [0028]. This information is sent to a backend server that validates the credit card data. *Khan (EX1005)*, [0025], [0028], Figs. 2, 4.

1. *Khan is Analogous*

94. In my opinion, *Khan* is analogous art to the '538 Patent. First, like the '538 Patent, *Khan* discloses conducting secure payment transactions with a mobile device. *Compare '538 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Khan (EX1005)*, [0002], [0006], [0018]-[0021], Figs. 2-4.

95. Second, a POSITA would have understood *Khan* to be reasonably pertinent to the particular problems with which the inventor of the '538 Patent was involved because *Khan* is directed to increasing security of payment transactions. *Compare '538 Patent (EX1001)*, 1:23-28, 1:63-2:4, 9:21-28 *with Khan (EX1005)*, [0002], [0004]-[0005].

C. *Varadarajan*

96. *Varadarajan* generally teaches financial transactions between an application on a mobile device and a transaction provider. *Varadarajan* at 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*

97. In my opinion, Varadarajan is analogous art to the '538 Patent. First, Varadarajan is directed to conducting secure payment transactions. *Compare '538 Patent (EX1001)*, 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 (EX1001)*, 1:23-28, 1:63-2:4, 9:21-28 *with Varadarajan (EX1006)*, [0005], [0009]-[0010].

D. Hammad

98. 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.

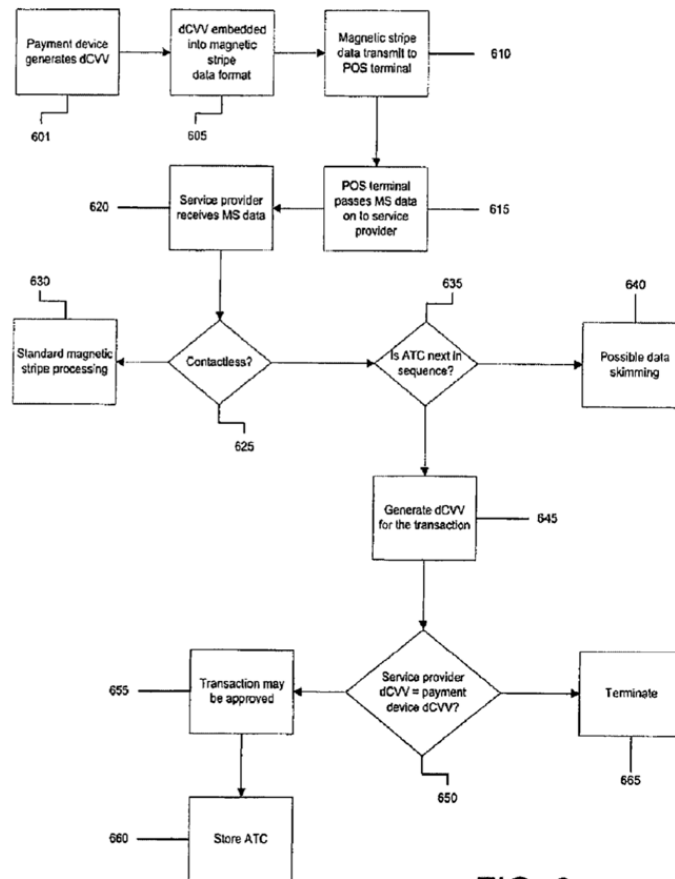


FIG. 6

Hammad (EX1006), Fig. 6.

99. 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, 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

100. 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.

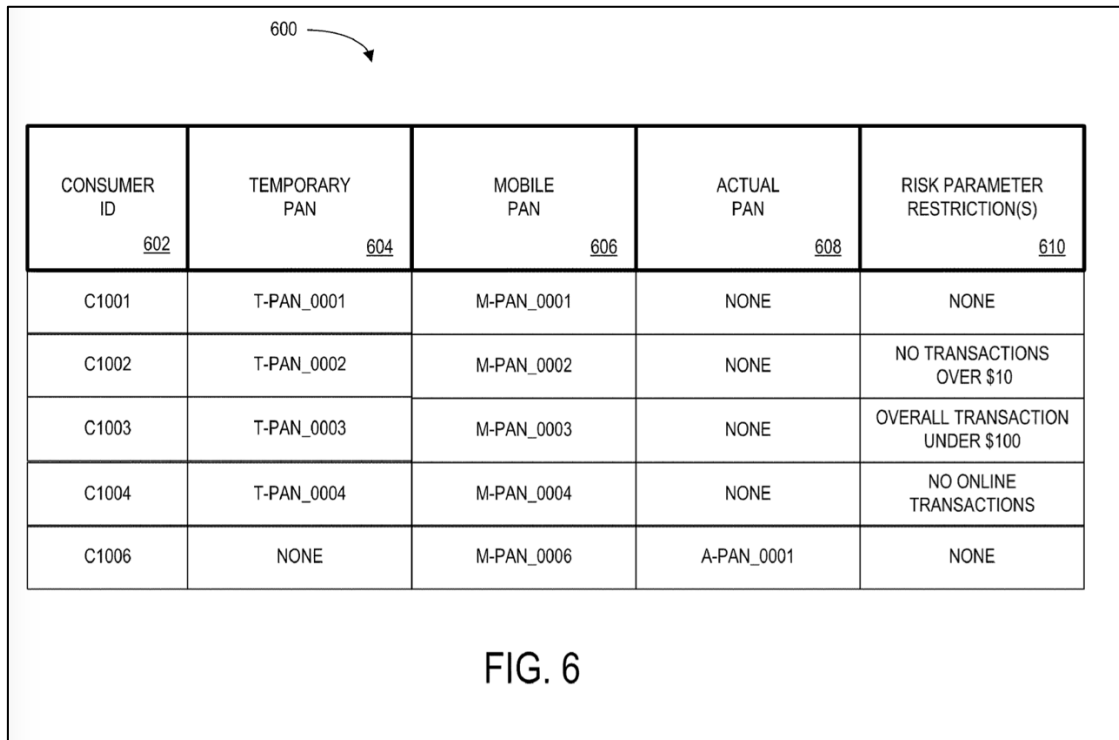
101. Hammad is also reasonably pertinent to at least one problem addressed by the '538 Patent. Like the '538 Patent, Hammad is concerned with increasing security of payment transactions. *See, e.g., Hammad (EX1007)*, 1:20-23 (“One of the primary sources of fraud, which is prevalent in the credit card 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 to 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. Smith

102. I understand Smith teaches a “mobile PAN” for a “mobile device” that “may...be used...with a near field communications enabled purchasing transaction.” *Smith* (EX1008), Abstract.

103. I understand Smith teaches a “mobile PAN” is used in place of the actual PAN. *Smith (EX1008)*, [0023] (the PPAN is associated with a “related PAN[.]”); *see also Smith (EX1008)*, [0026].



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 (EX1008), Fig. 6.

104. The mobile PAN is “stored in the mobile device 204.” *Smith (EX1008)*, [0022].

1. Smith is Analogous

105. 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 (EX1008)*, [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* (EX1008), Abstract, [0021]-[0023].

106. 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* (EX1008), [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 (EX1008), [0002], [0015], [0020].

F. Bauer

107. Bauer teaches methods and systems for using and authorizing a mobile payment account on a portable electronic device. *Bauer* (EX1009), Abstract, [0001], [0019]. Bauer describes use of an electronic wallet that includes data for payment accounts for completing a transaction. *Id.*, [0019]-[0021]. To access the wallet and conduct a transaction, the user must be authenticated, e.g., through providing a PIN. *Id.*, [0084]-[0091], Figs. 9a-b, 10a-f.

1. Bauer is Analogous

108. Bauer is analogous art to the ’538 Patent because it is from the same field of endeavor. Like the ’538 Patent, Bauer is concerned with conducting secure payment transactions. *Bauer* (EX1009) Abstract, [0001], [0019]-[0021]; *compare* ’538 patent (EX1001), Abstract, 1:23-28, Fig. 1 with *Bauer* (EX1009), Abstract, [0001], [0019]-[0021].

109. Bauer is also reasonably pertinent to at least one problem addressed by the ’538 Patent. Like the ’538 Patent, Bauer is concerned with increasing security of

payment transactions. *See, e.g., Bauer (EX1009)*, [0003]-[0006], [0009]-[0010]; *compare '538 Patent (EX1001)*, 1:23-28, 1:63-2:4, 9:21-28 *with Bauer (EX1009)*, [0003]-[0006], [0009]-[0010].

G. Kranzley

110. Kranzley generally teaches methods and system for conducting payment transactions with a mobile device over a network. *Kranzley (EX1010)*, 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 (EX1010)*, [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 (EX1010)*, [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 (EX1010)*, [0035]; [0033]-[0036].

1. Kranzley is Analogous

111. 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* (*EX1010*), Abstract, [0010], Fig. 1.

112. 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* (*EX1010*), [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

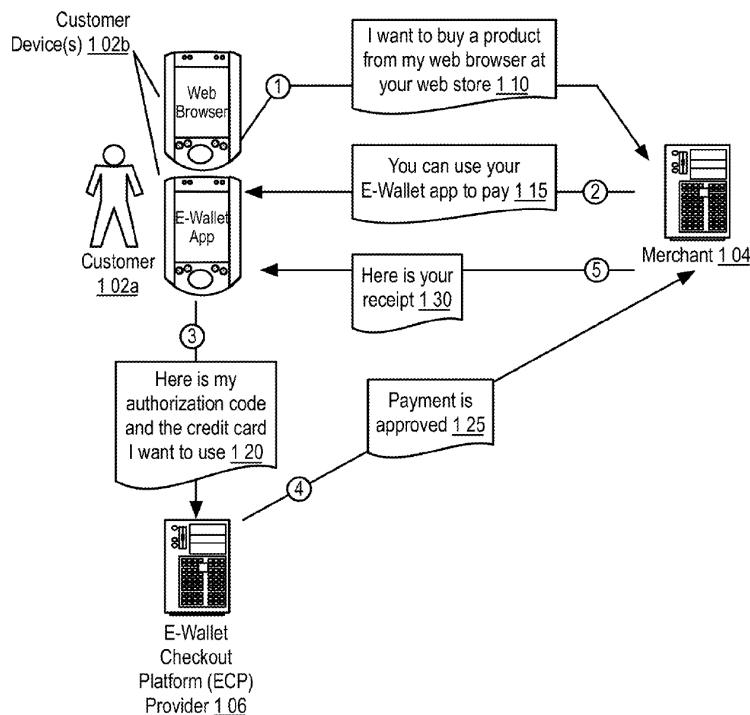
transaction request.”); *compare* '538 Patent (EX1001), 1:23-28, 1:63-2:4, 9:21-28 with *Kranzley* (EX1010), [0003], [0065].

X. GROUND 1: CLAIMS 19 AND 24 ARE OBVIOUS OVER KALGI, KHAN, AND VARADARAJAN

A. Claim 19

1. 19(pre): A method of performing an online payment transaction, the method comprising:

113. Kalgi teaches “apparatuses, methods, and systems for electronic purchase transactions,” including transactions where “a customer 102a may wish to purchase a product and/or service 110 from a merchant 104 via a web browser (e.g., at the merchant’s website).” *Kalgi* (EX1004), [0003], [0028].



Kalgi (EX1004), Fig. 1.

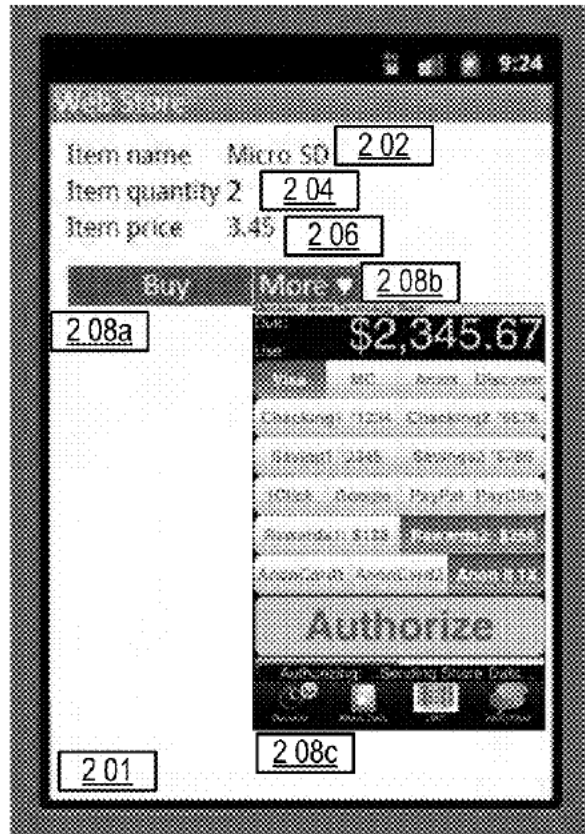
114. “For example, the customer may be shopping online for an item at the merchant’s website, via consumer device 102b.” *Kalgi (EX1004)*, [0028], [0033], [0062], [0066], [0083]. *Kalgi* teaches an electronic wallet checkout platform (EWCP) that enables the customer to “engage in a purchase transaction via a secure platform that may provide a consistent user experience across merchant websites.” *Kalgi (EX1004)*, [0027]. Thus, *Kalgi* teaches a method of performing an online payment transaction.²

2. *19(a): receiving an input signal at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface of the electronic device;*

115. *Kalgi* teaches “a customer may visit a merchant’s website using a mobile device (e.g., a cell phone, a PDA, a tablet, and/or the like).” *Kalgi (EX1004)*, [0034]; *see also*, [0027], [0028], Fig. 2. The customer’s mobile device is an electronic device.

116. *Kalgi* further teaches a “mobile EWCP application” running on the mobile device to facilitate transactions with the website. *Kalgi (EX1004)*, [0034]-[0036], Fig. 1; *see also*, [00142]-[0143], Figs. 18-19B. “The customer may wish to purchase two 204 Micro SD cards 202 at a price 206 of \$3.45 each” and “may click the ‘Buy’ button 208 a to purchase these items.” *Kalgi (EX1004)*, [0034].

² Claim language identified with *italics* and underline.



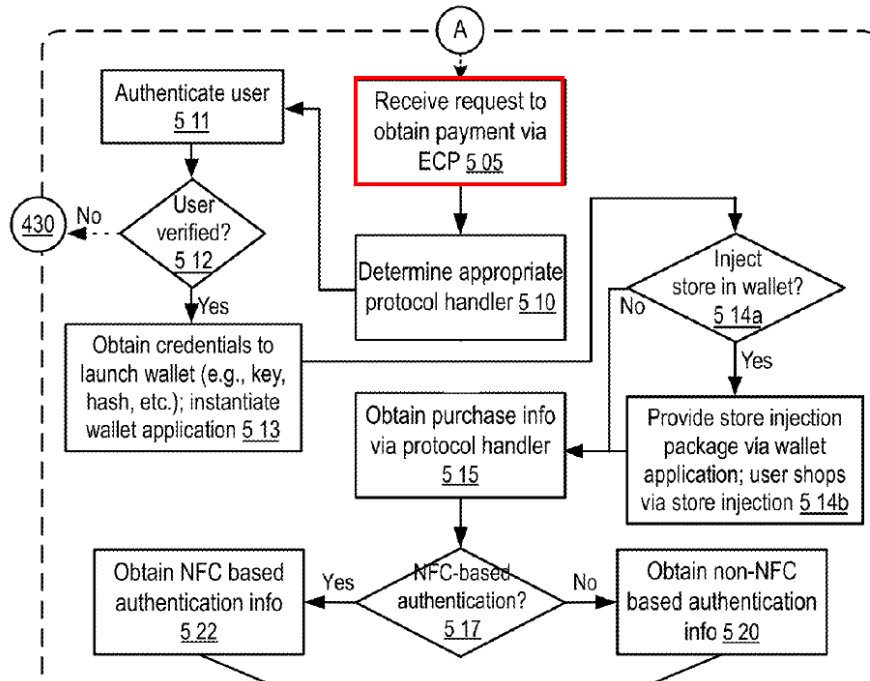
Kalgi (EX1004), Fig. 2 (excerpt).

117. After the user indicates that he or she wishes to purchase the items, the mobile EWCP application running on the mobile device “detect[s] that the merchant’s website uses an EWCP-supported protocol” using the method described with regard to Figure 5. *Kalgi (EX1004)*, [0034]; *see also*, Abstract.

118. As shown in Figure 5, “a request to obtain payment via EWCP may be received at 505.” *Kalgi (EX1004)*, [0051]; *see also* Fig. 5. “For example, an EWCP browser extension may detect that a merchant’s webpage is using an EWCP-supported protocol (e.g., by determining existence of a protocol string starting with “ewalletcheckout://”, “specialcheckout://”, “specialwallet://”, and/or the like) to

request payment from a user.” *Kalgi (EX1004)*, [0051]; *see also*, [0039]-[0040], [0047]-[0048].

FIGURE 5 **Receive a Request for Payment of an Online Payment Transaction by said Electronic Device**



Kalgi (EX1004), Fig. 5 (annotated excerpt).

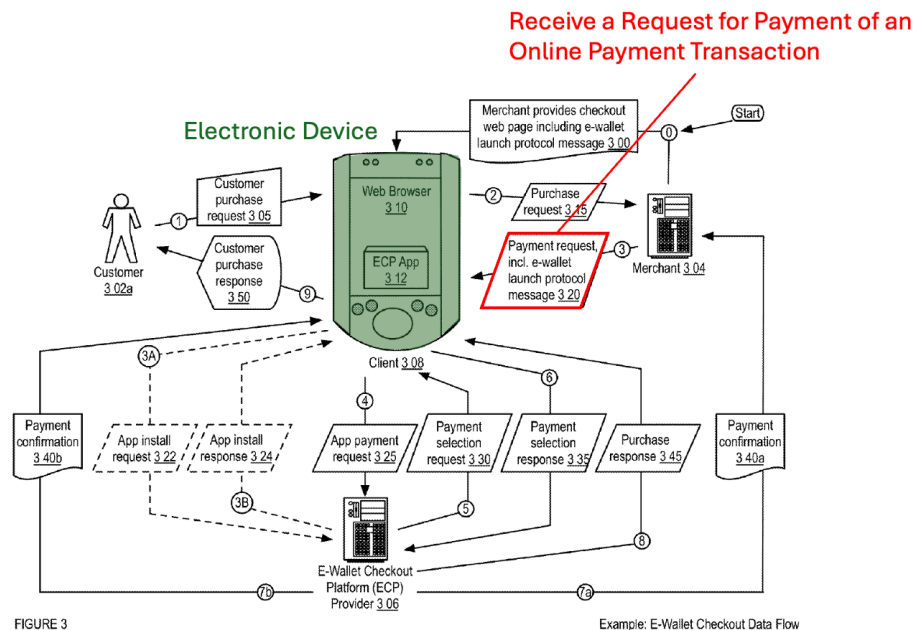


FIGURE 3

Example: E-Wallet Checkout Data Flow

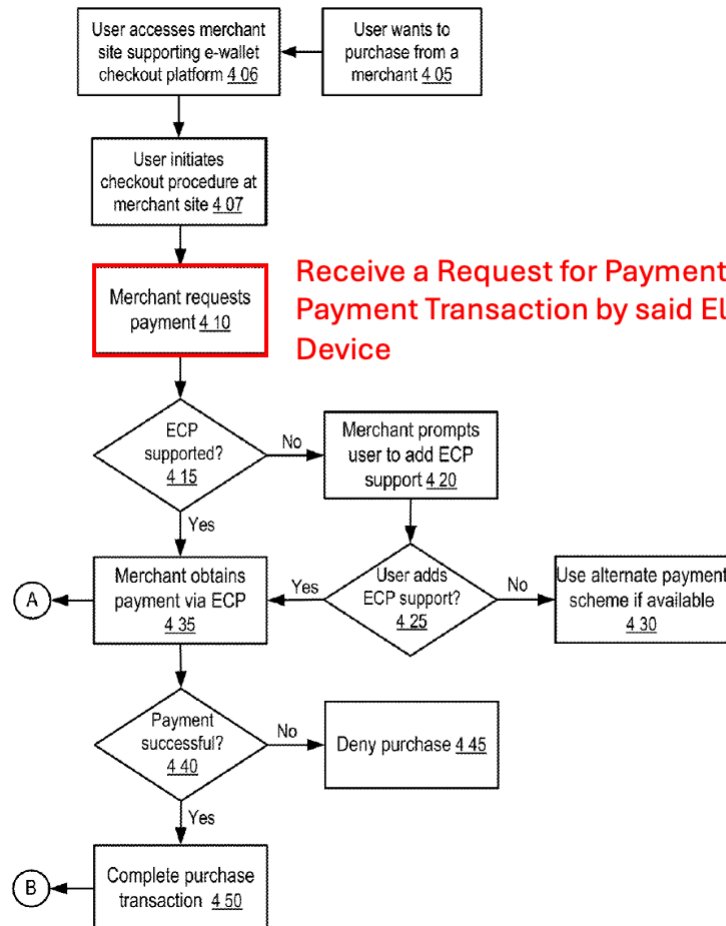
Kalgi (EX1004), Fig. 3 (annotated).

119. Thus, the mobile device receives a protocol string, which is an input signal corresponding to a request for payment of an online payment transaction by said electronic device.

120. The merchant's server may generate a payment request (including the protocol string) and send to the mobile device over a network. *Kalgi (EX1004)*, [0047], [0066], [0068]. A server is a computer that "processes and responds to the requests of remote users across a communications network," including "Wireless Networks." *Kalgi (EX1004)*, [0150]; *see also*, Figs. 1, 3, 7. Similarly, the user may communicate with a point-of-sale terminal via "Wi-Fi." *Kalgi* [0068], [0084].

121. A POSITA would have understood that mobile devices, such as *Kalgi*'s smartphone, access a merchant's website via WiFi or cellular data networks, i.e., wireless networks. *See Kalgi (EX1004)*, [0034], [0067]-[0068]. Wireless interfaces on mobile devices, e.g., cellular or smart phones, for communicating with an online merchant were well-known at the time. For example, *Kalgi* describes that its mobile device could be a smart phone, such as an iPhone or Android. *Kalgi (EX1004)*, [0149]. *Lin* depicts that an iPhone includes a wireless interface, such as a WLAN or WAN. *Lin (EX1044)*, 15:7-9, 22:21-23:30, Figs. 1, 3. Indeed, a wireless interface would be required for a user and merchant website (or PoS terminal) to communicate

wirelessly as described in Kalgi. Thus, a POSITA would have understood that Kalgi's mobile device includes a wireless interface.



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

122. Alternatively, it would have been obvious to a POSITA to configure Kalgi's mobile device to receive the protocol string via a wireless interface.

a) Khan's Teachings

123. Khan teaches a similar method of performing online payment transactions using a portable device. *Khan (EX1005)*, [0002], [0006], [0018], [0021]-[0024], [0028], Figs. 2, 4. The portable device includes one or more

interfaces, including a WIFI interface. *Khan (EX1005)*, [0018]. “Purchase information,” such as an alias of a credit card number and crypto data, are “transferred through the WIFI interface” on the portable device. *Khan (EX1005)*, [0021].

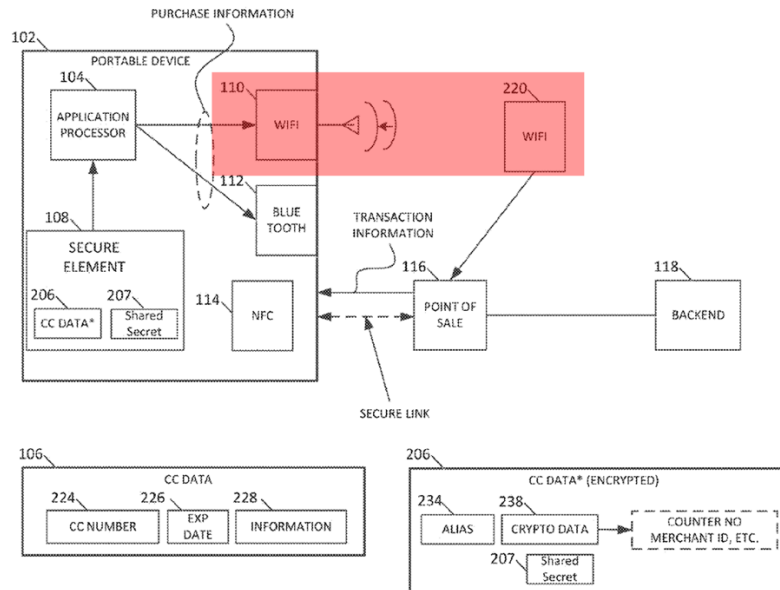


FIG. 2

Khan (EX1005), Fig. 2 (annotated). *Khan* further teaches that its portable device can make mobile payments online, which are authorized by a backend server. *Khan (EX1005)*, [0028], Fig. 4. Thus, *Khan* teaches a mobile device that communicates payment information via a wireless interface.

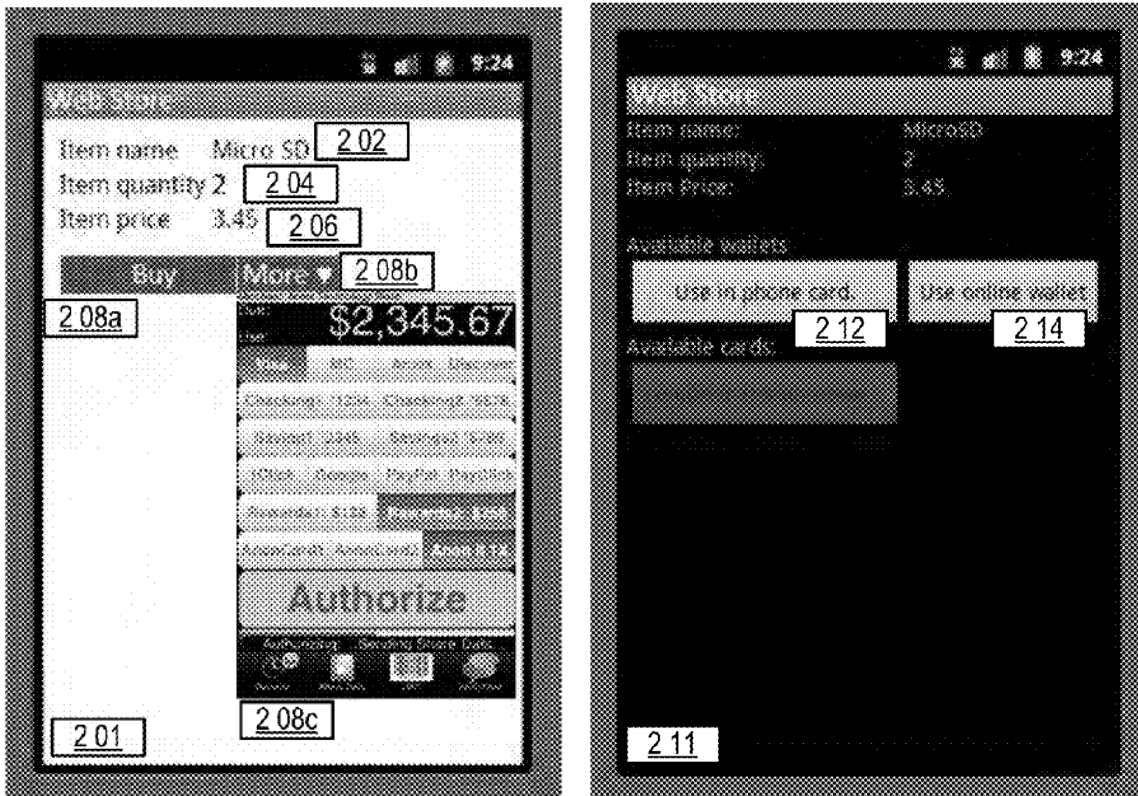
b) Motivations to Combine

124. It would have been obvious and a POSITA would have been motivated to incorporate a wireless interface, such as *Khan*’s WIFI interface, so that *Kalgi*’s mobile device receives a payment request wirelessly via a wireless interface. A

POSITA would have understood that a mobile device, such as a smartphone, would have one or more wireless interfaces to access the internet. Thus, a POSITA would have been motivated to combine prior art elements—i.e., Kalgi’s mobile device with Khan’s WIFI interface—to predictably enable Kalgi’s mobile device to communicate via wireless networks for online transactions, as Kalgi already describes. Given the ubiquity of mobile devices having wireless interfaces, there would have been a reasonable expectation of success configuring Kalgi’s mobile device to receive the request via the device’s wireless interface.

3. ***19(b): a displaying of the payment request notification at a touch-screen display user-interface of the electronic device; and,***

125. Kalgi teaches that the user provides inputs via a touch screen display user interface of the electronic device. Kalgi (EX1004), [0039], [0062], [0067], [0083], [0113]. After the payment request is received, the user is prompted “to use an EWCP electronic wallet (hereinafter “E-Wallet” or “wallet application”) to facilitate payment.” Kalgi (EX1004), [0029]. Specifically, the user is “prompted to select an available wallet,” such as illustrated on the touchscreen display of screen 211. Kalgi (EX1004), [0036], Fig. 2; *see also*, [0040] (“The payment request may prompt the customer to provide payment information to pay for the item.”). Thus, the screen 211, which prompts the user to select a displayed wallet to perform the payment transaction, serves as a payment request notification.

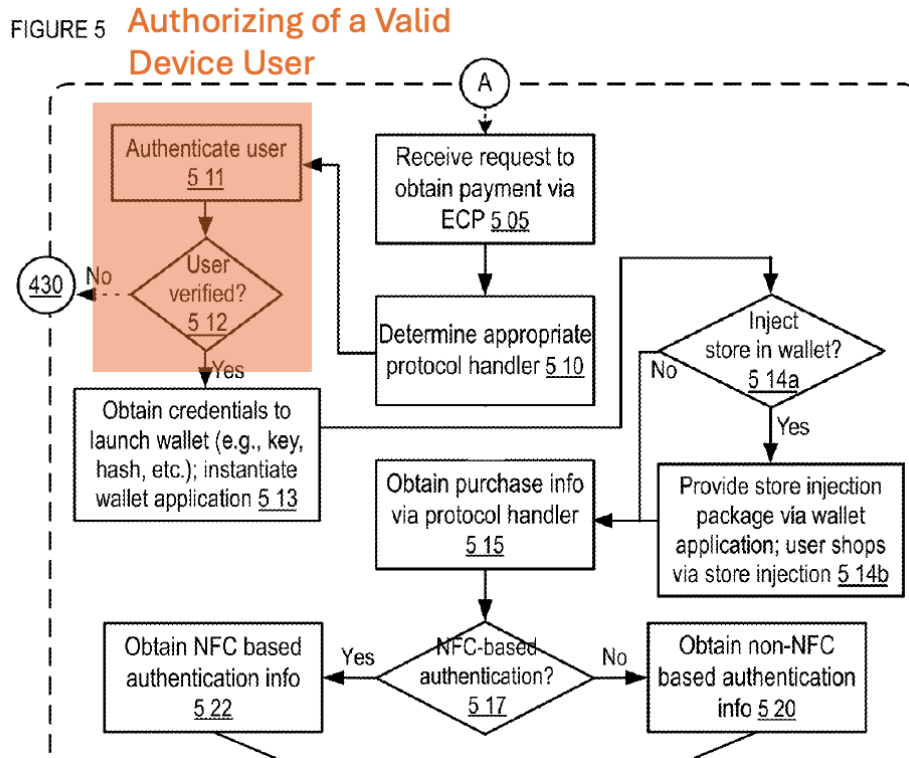


Kalgi (EX1004), Fig. 2 (excerpts).

4. ***19(c): upon an authorizing of a valid device user, displaying at least one user-selectable payment account option, and requesting a user approval of payment, via the touch-screen display user-interface;***

126. Kalgi teaches the user must be authorized as a valid device user to launch the wallet application. *Kalgi (EX1004)*, [0029] (“The customer may be asked to provide authentication and/or authorization information to use the E-Wallet.”), [0036] (“the ‘Buy’ button 208a may trigger the launch of an E-Wallet application and the application may be instantiated.”), [0051], [0054]-[0055], [0067], [0083]. “[T]he user may be required to enter login information, answer a challenge question,

submit a voice/biometric signature, provide a digital certificate, enter into a video call for verification purposes, and/or the like.” *Kalgi (EX1004)*, [0051].



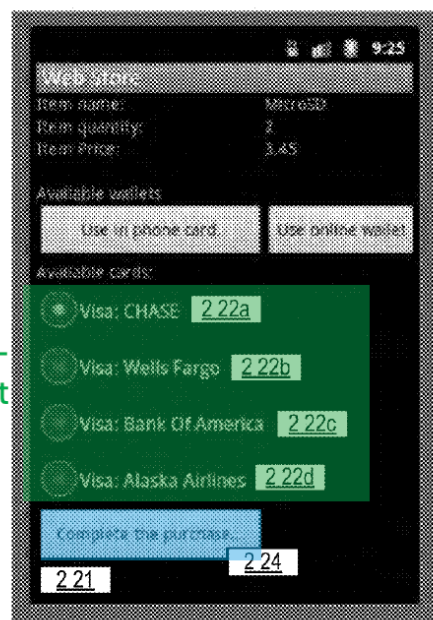
Kalgi (EX1004), Fig. 5 (annotated excerpt).

127. Figure 2 (screen 221) displays “a choice of payment methods 222a-222d (e.g., credit cards, debit cards, gift cards, and/or the like) available in the wallet selected by the customer.” *Kalgi (EX1004)*, [0037], Fig. 2; *see also*, [0035], [0036] (“[U]pon authentication and/or authorization to use the E-Wallet, the customer may be prompted to select an available wallet. In one embodiment, the customer may select a wallet stored on the mobile device 212.”). Thus, displaying the list of payment methods 222a-222d on screen 211 is displaying at least one user-selectable payment account option, via the touchscreen display user-interface.

128. “Upon selecting a payment method (e.g., 222 a), the customer may use the ‘Complete the purchase ...’ button 224 to submit payment information.” *Kalgi (EX1004)*, [0037]. Thus, *Kalgi* teaches requesting a user approval of payment (i.e., prompting the user to “Complete the purchase” via button 224), via the touchscreen display user-interface.

Displaying at Least One User-Selectable Payment Account Option

Requesting a User Approval of Payment

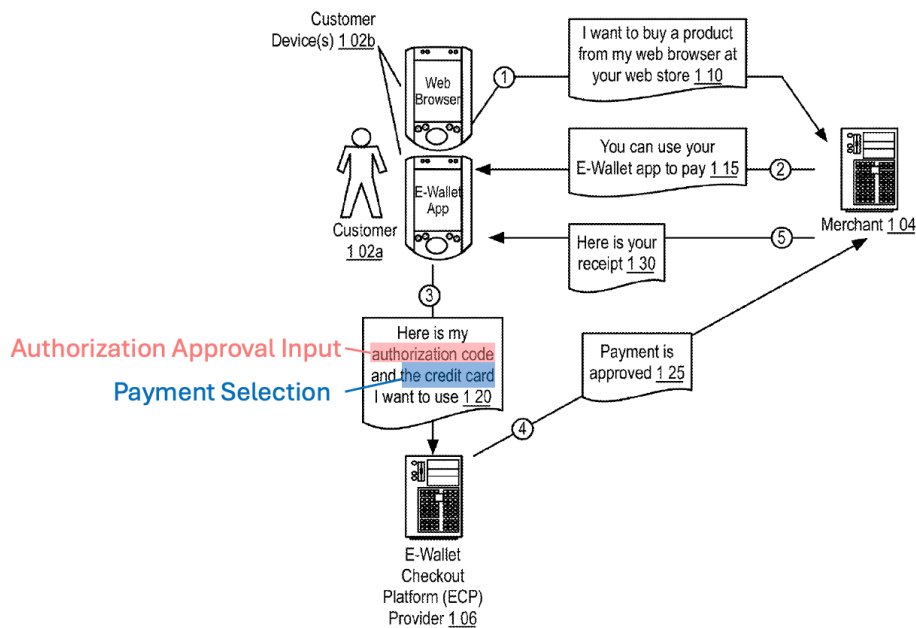


Kalgi (EX1004), Fig. 2 (annotated excerpt).

5. 19(d): receiving, from a valid device user, a payment selection and authorization approval input on the electronic device;

129. *Kalgi* teaches the valid device user “provide[s] a selection of a payment method (e.g., a specific credit card) 120” on the electronic device. *Kalgi (EX1004)*, [0029], Fig. 1; *see also*, [0057]. The “user may provide a wallet access input ... into the user wallet device” through a touchscreen interface. *Kalgi (EX1004)*, [0039], [0062], [0067], [0083]. The user must also provide “authentication and/or

authorization information” specific to the selected payment method, such as “a payment method security code, and/or the like.” *Kalgi (EX1004)*, [0029], [0043], [0059], Figs. 3, 5. Thus, *Kalgi* teaches receiving, from a valid device user, a payment selection and authorization approval input on the electronic device.



Kalgi (EX1004), Fig. 1 (annotated).

6. ***19(e): generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and***

130. *Kalgi* teaches a user providing a credit card and authorization code to complete a purchase. *Kalgi (EX1004)*, [0029], [0059], Fig. 1. *Kalgi* additionally teaches that its EWCP includes a User Purchase Checkout and Purchase Transaction Authorization component. *Kalgi (EX1004)*, [0067]-[0092], Figs. 9A-10B. In this context, a user may purchase a product from a merchant’s online site by

communicating with the merchant's PoS client or server. *Kalgi (EX1004)*, [0062], [0066], [0083], Figs. 9A-10B. When using the E-Wallet, the user provides payment information to the merchant, including an account number, account name, account address, CVV (static or dynamic), and other information, in a compatible data form. *Kalgi (EX1004)*, [0068]-[0069], [0084].

```
<?XML version = "1.0" encoding = "UTF-8"?>
<transaction_authorization_input>
  <payment_data>
    <account>
      <charge_priority>1</charge_priority>
      <charge_ratio>40%</charge_ratio>
      <account_type>debit</account_type>
      <value_exchange_symbol>USD</value_exchange_symbol>
      <account_number>123456789012345</account_number>
      <account_name>John Q. Public</account_name>
      <bill_add>987 Green St #456, Chicago, IL 94652</bill_add>
      <ship_add>987 Green St #456, Chicago, IL 94652</ship_add>
      <CVV_type>dynamic</CVV_type>
      <CVV>http://www.paynet.com/dcvv.php?sessionID=4NFU4RG94</CVV>
      <cloak_flag>ON</cloak_flag>
      <alert_rules>tar1 tar4 tar12</alert_rules>
      <mode>NFC</mode>
    </account>
    <account>
      <charge_priority>1</charge_priority>
      <charge_ratio>60%</charge_ratio>
      <account_type>rewards</account_type>
      <value_exchange_symbol>VME</value_exchange_symbol>
      <account_number>234567890123456</account_number>
      <account_name>John Q. Public</account_name>
      <bill_add>987 Green St #456, Chicago, IL 94652</bill_add>
      <ship_add>987 Green St #456, Chicago, IL 94652</ship_add>
      <CVV_type>static</CVV_type>
      <CVV>173</CVV>
```

```
<cloak_flag>ON</cloak_flag>
<alert_rules>tar1 tar4 tar12</alert_rules>
<mode>Bluetooth</mode>
</account>
<account>
  <charge_priority>2</charge_priority>
  <charge_ratio>100%</charge_ratio>
  <account_number>345678901234567</account_number>
  <account_type>credit</account_type>
  <value_exchange_symbol>USD</value_exchange_symbol>
  <account_name>John Q. Public</account_name>
  <bill_add>987 Green St #456, Chicago, IL 94652</bill_add>
  <ship_add>987 Green St #456, Chicago, IL 94652</ship_add>
  <CVV_type>static<CVV_type>
  <CVV>173</CVV>
  <cloak_flag>ON</cloak_flag>
  <alert_rules>tar1 tar4 tar12</alert_rules>
  <mode>NFC</mode>
</account>
</payment_data>
```

Kalgi (EX1004), [0069] (annotated).

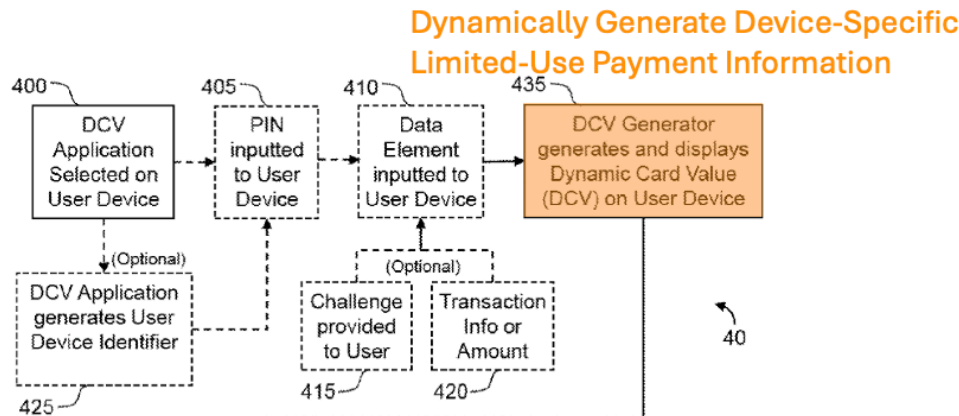
131. This information is subsequently transmitted for payment processing.

Kalgi (EX1004), [0070]-[0081], [0085]-[0092], Figs. 9A-10B.

a) *Varadarajan's Teachings*

132. Varadarajan teaches a similar mobile payment application on a mobile device. *Varadarajan (EX1006)*, [0011], [0032], [0038]-[0039], [0041]. Specifically, a “user downloads the DCV application to his mobile user device, which can be virtually any hand-held platform,” including smart phones. *Varadarajan (EX1006)*, [0026]. The DCV application generates a dynamic card value (DCV), which is used to replace a static value, such as a CVV and/or PAN. *Varadarajan (EX1006)*, [0012], [0022] (describing “both a dynamic PAN and a dynamic CVV may be generated for use in the same transaction”), [0023], [0045], [0056]. The DCV can be a 3 or 4-digit number when replacing a CVV or sixteen-digit number when replacing a PAN.

Varadarajan (EX1006), [0021], [0031]. “The DCV is configured and provided in the same form as the static DCV for which it is being substituted.” *Varadarajan (EX1006)*, [0021].



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

133. The DCV can be used in an online transaction and input to a transaction interface, such as an online shopping cart. *Varadarajan (EX1006)*, [0011], [0021], [0029]-[0030], [0042], [0045], Fig. 4.

134. The DCV is limited-use in that it expires “after a limited number of uses, which may be a single use[.]” *Varadarajan (EX1006)*, [0023], [0020], [0047].

135. Thus, Varadarajan’s DCV is at least one limited-use number that is dynamically generated at the device for using ... in place of at least a portion of said selected issuer payment information (e.g., the PAN or CVV, etc.).

b) Motivations to Combine

136. It would have been obvious and a POSITA would have been motivated to configure Kalgi's device processor to dynamically generate a DCV or PAN to be used in place of at least a portion of the selected issuer payment account information responsive to receiving a valid user transaction payment approval. A POSITA would have understood that Kalgi's device could be vulnerable to attacks where the issuer provided account information (e.g., PAN) is intercepted by an attacker and used for fraudulent transactions. Indeed, Varadarajan recognizes security vulnerabilities" associated with "card based transactions," including online transactions. *Varadarajan (EX1006)*, [0003], [0005], [0009]-[0010]. Thus, to prevent fraud, a POSITA would have been motivated to configure Kalgi to implement Varadarajan's method of dynamically generating a DCV to be used in place of a PAN or CVV to improve similar mobile payment systems in the same way for online transactions. The concept of dynamic CVVs and PANs was well-known and a POSITA would have been familiar with using such numbers in connection with payment transactions to increase security. As described in Section V.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), Hammad (assigned to Visa) describes that the generation and use of dCVVs by mobile devices 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. Substitution of Kalgi's CVV, dynamic CVV or PAN with Varadarajan's DCV is substitution of one known element for another and a POSITA would have understood that the substitution would have predictably increased the security of Kalgi's payment system and further protected the user's sensitive account information. utilizing known techniques to improve similar devices that would have predictably increased the security of Kalgi's payment system and further protected the user's account information.

137. A POSITA would have had a reasonable expectation of success in modifying Kalgi in this way because Kalgi already using dynamic CVVs in a transaction. Thus, a POSITA would have recognized that modifying Kalgi, which already describes including dynamic CVV in payment information (*Kalgi (EX1004)*, [0069]-[0070]), 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, a POSITA would realize that the electronic device of Kalgi-Khan could be modified programmatically to incorporate Varadarajan's DCV into the payment information transmitted during the payment

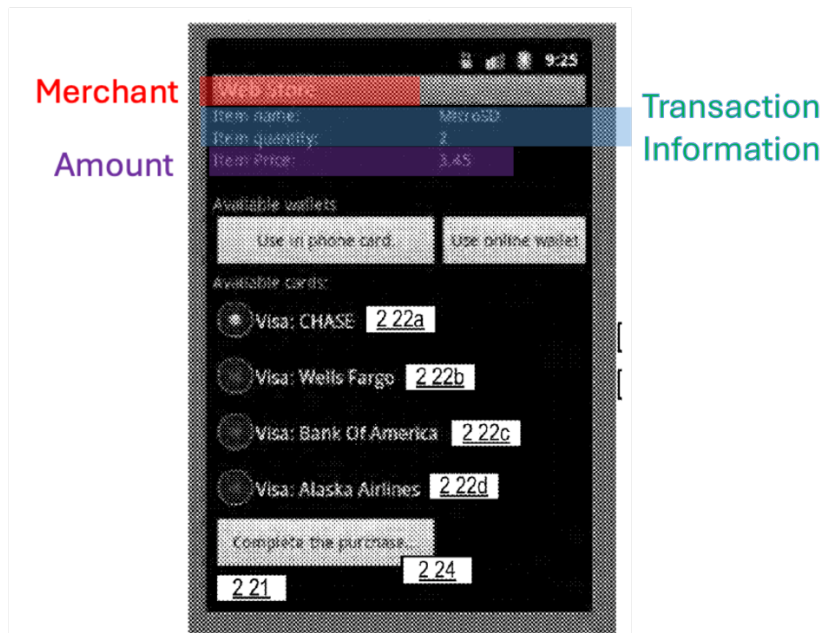
transaction. Thus, the modification would simply require including programming in Kalgi's memory for generating a dynamic card value, i.e., DCV, and using the same in place of a PAN or CVV, which would have required routine skill. As such, the modification would have been a combination of a known technique (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. 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 Kalgi's mobile device for performing a payment transaction.

7. ***19(f): combining said at least one limited-use numbers, with said selected account information, to form a complete payment information; and,***

138. As described in Claim 19(e), it would have been obvious to a POSITA to modify Kalgi's mobile device to generate a DCV for use in place of the CVV and/or PAN. *See* Claim 19(e). Kalgi teaches that the user wallet device provides payment information for the transaction, such as name, address, CVV (static and dynamic), and account number. *Kalgi*, [0069]. Thus, it would have also been obvious to combine the DCV (said at least one limited-use numbers) with selected account information in Kalgi's payment data provided by the user wallet device to form a complete payment information for the same reasons.

8. ***19(g): wherein the receiving of a user payment approval authorization through the user-interface of the electronic device, is comprising a displaying on said display at least a portion of information comprising: the payment request, the merchant, the amount, and the transaction information; and,***

139. Kalgi teaches receiving authentication and/or authorization information (a user payment approval authorization) through the user-interface of the electronic device. See Claim 19(d). Kalgi also teaches displaying the payment request, including merchant, amount, and transaction information. Kalgi (EX1004), Fig. 2.

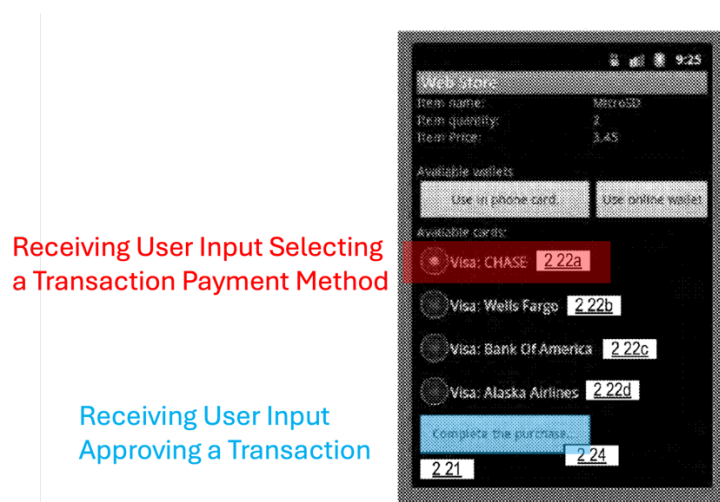


Kalgi (EX1004), Fig. 2 (annotated excerpt).

9. ***19(h): receiving a user input providing for at least one transaction authorization actions, from a set of actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method; and,***

140. As discussed above, Kalgi's mobile device receives a user input for approving a transaction and selecting a transaction payment method. See Claims

19(c)-(d). Specifically, the mobile device receives approval of a transaction when the user presses “the ‘Complete the purchase ...’ button 224 to submit payment information.” *Kalgi (EX1004)*, [0037]. The mobile device also receives a selection of the payment method. *Kalgi (EX1004)*, [0037]; *see also*, [0029], [0035], [0042]-[0043].



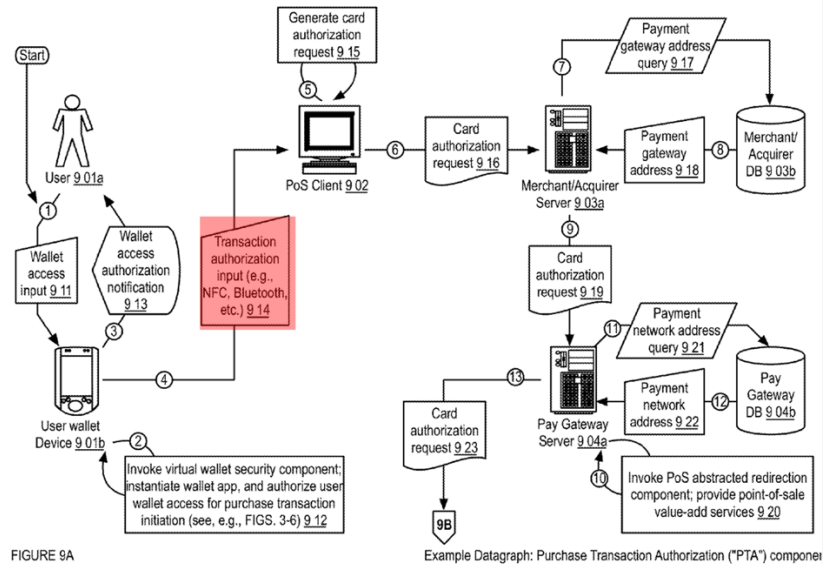
Kalgi (EX1004), Fig. 2 (annotated excerpt).

10. 19(i): on receiving said user payment approval authorization input, a transmitting by the wireless interface of the approved complete payment information for the online transaction.

141. As discussed, *Kalgi* teaches receiving user payment approval authorization input via button 224, which causes the mobile device to “to submit payment information.” *See* Claim 19(h); *Kalgi (EX1004)*, [0037], Fig. 2. Specifically, the mobile device transmits “a payment selection response 335 to the

142. For the reasons discussed above, it would have been obvious to a POSITA to enable Kalgi's mobile device to communicate via a wireless interface. *See* Claim 19(a); *Kalgi (EX1004)*, [0067]-[0068], [0083]-[0084]. For the same reasons, it would have been obvious to enable Kalgi's mobile device to transmit the payment selection response including the approved complete payment information for the online transaction to the EWCP provider the wireless interface. *Kalgi (EX1004)*, [0067]-[0068], [0083]-[0084]; *see also* Claims 19(e)-(f).

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



Kalgi (EX1004), Fig. 9A (annotated), Fig. 10A.

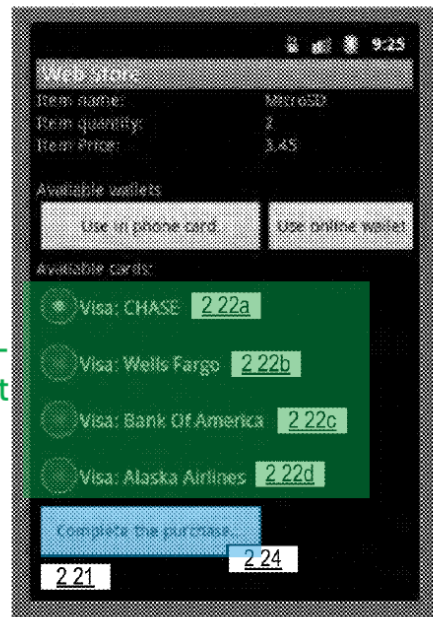
B. Claim 24

- 1. 24:** *The method of claim 19, wherein the user selecting of a payment method at an electronic device comprises receiving a user touch input selection, via the user interface, of a displayed payment method option, on the device touch-screen display interface.*

143. As discussed above, Kalgi teaches that the user provides inputs via a touch screen display user interface of the electronic device. Kalgi (EX1004), [0039], [0062], [0067], [0083], [0113]; *see also*, Claim 19(b). Fig. 2 also depicts a screen shown on the touchscreen display where a user selects a payment method via a touch input selection. *See* Claim 19(c); Kalgi (EX1004), [0037].

Displaying at Least One User-
Selectable Payment Account
Option

Requesting a User
Approval of Payment



Kalgi (EX1004), Fig. 2 (annotated excerpt).

XI. GROUND 2: CLAIMS 20 AND 22 ARE OBVIOUS OVER KALGI, KHAN, VARADARAJAN, AND HAMMAD

A. Claim 20

1. 20(a): The method of claim 19, further comprising:

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

a) Varadarajan's Teachings

144. 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].

b) *Hammad’s Teachings*

145. Hammad teaches dynamically generating a dCVV (*cryptogram number*) using an application on a mobile device for use in a wireless mobile payment transaction, e.g., over a wireless local area network. *Hammad (EX1007)*, 2:65-3:11, 3:51-4:6. The DCV 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.” *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 cryptographically combining this information with multiple encryption keys, including a master derivation key, resulting in a 3-digit dCVV. *Hammad (EX1007)*, 4:61-6:34, Figs. 1-3. The master derivation key is provided by the service provider. *Hammad (EX1007)*, 5:38-57, Fig. 2.

146. The dCVV is embedded into the payment data, which is transmitted to the point of sale terminal and then to the service provider, e.g., “payment processing organization or an issuer of the portable consumer device.” *Hammad (EX1007)*, 2:18-20, 4:61-6:34, 6:40-42, 6:49-7:27, 7:29-32, 7:43-46, 7:55-62, Figs. 4-5. The service provider uses the dCVV to determine the authenticity of the payment. *Hammad (EX1007)*, 7:29-8:50, Fig. 6. A POSITA would have understood that Hammad’s dCVV, like Varadarajan’s DCV, is a cryptogram.

147. Thus, Hammad teaches generating a dCVV from an application transaction counter (“ATC”) (device transaction sequence counter count); user information, such as telephone number, birthday, home address; an account number

(payment account number); a service code; and expiration date, among other information, that is combined with a master derivation key (information and secrets known to a payment processing authority). *Hammad (EX1007)*, 4:21-44, 4:52-56, 4:63-5:5, 5:34-6:3 Figs. 1-2.

c) Motivation to Combine

148. A POSITA would have understood that a dCVV, as generated by Hammad, is a cryptogram number used in place of a card validation value (e.g., CVV) originated from the payment issuing authority generated by cryptographically combining the recited elements, among other information. As discussed in Section V.C.2, the use of dynamic card verification values was prevalent long before 2012. A POSITA would have found it obvious and been motivated to use Hammad's dCVV generation process for the same reasons recited in Claim 19(e) for using Varadarajan's DCV. Hammad is a natural extension of Varadarajan, which teaches generating a DCV from data elements. *Varadarajan (EX1006)*, [0055]. Hammad extends this teaching by including at least three or four dynamic data elements and static data elements, including an account number, to the generate a dynamic CVV to increase security. 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 recognized that including more data elements in generating a DCV would decrease the likelihood that, even if the payment data were intercepted, that it could be used in a fraudulent manner. Therefore, a POSITA would have been motivated to include more data elements in generating a DCV for the CVV in the combination, as taught by Hammad. 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 transactions if the information were intercepted. Given Hammad's teachings regarding how to generate such a dynamic verification value, a POSITA would have had a reasonable expectation of success. A POSITA would have further recognized that modifications to Kalgi-Khan-Varadarajan would be minimal as it would simply require additional inputs to Varadarajan's DCV generator. This modification is applying known techniques (e.g., using various data elements to generate a card verification value cryptogram to replace a static value) to improve similar devices (e.g., mobile devices used in payment transactions) in the same way to yield the predictable result of increasing security of the transaction.

2. ***20(b): wherein further, said dynamically generating said card validation value number results in a one-time limited-use payment information, on incrementing the device transaction sequence counter count on each transaction payment, and said device combining said current transaction sequence count at the instant of generating said cryptogram number.***

149. Hammad teaches the dCVV is generated for “each transaction” (a one-time limited-use payment information). *Hammad (EX1007)*, 2:65-67, 4:21-31, 4:61-65. The ATC is “incremented with each transaction.” *Hammad (EX1007)*, 4:25-26; *see also*, 1:50-51. The user device combines the ATC with other dynamic and static data elements at the time of generating the dCVV. *Hammad (EX1007)*, 4:63-6:34. A POSITA would have understood the resulting dCVV, combined with other payment data, is payment information limited to one use and generated from combining the current ATC with other data elements.

B. Claim 22

1. ***22(a): The method of claim 19, further comprising:

generating a limited-use security code number for use in place of a card issuer card security code, by cryptographically combining information from at least one of a set of information comprising: a device transaction sequence counter; a device account number; a payment account information, device secrets; payment processing authority secrets; and***

150. As discussed in Claims 20(a), Hammad teaches generating a limited-use dCVV (limited-use security code number) by cryptographically combining at least one of an ATC (a device transaction sequence counter), account number (a

payment account information), and PIN verification data or master derivation key (payment processing authority secrets).

151. Varadarajan teaches that a DCV can be configured as a “Card Security Code (CSC).” *Varadarajan (EX1006)*, Abstract, [0002]-[0003], [0013]. A POSITA would have understood that a DCV/dCVV, when configured as a CSC, is used in place of a card issuer card security code. *See also* Claim 20(a).

2. 22(b): displaying the limited-use security code number on the user-interface of the device display.

152. Varadarajan teaches that the DCV can be displayed on the user device for subsequent entry. *Varadarajan (EX1006)*, [0032] (“The DCV may be displayed to the user ... to be keyed in ... to the transaction interface.”), [0045], [0056], Fig. 4 (steps 435, 450). A POSITA would have found it obvious to implement the same in Kalgi to enable a user to perform the online transaction by entering the required information on a user interface. Without such information, the transaction could not be completed, which would not be acceptable. A POSITA would have had a reasonable expectation of success in implementing the same as Kalgi already teaches a user interface for displaying and entering information, such as a card security code. *Kalgi (EX1004)*, [0059], [0062], [0106], Fig. 2. The combination, therefore, is simply a combination known methods to yield the predictable result of enabling a user to securely conduct an online transaction.

**XII. GROUND 3: CLAIM 21 IS OBVIOUS OVER KALGI, KHAN,
VARADARAJAN, AND SMITH**

A. Claim 21

1. 21(a): The method of claim 19, wherein at least a portion of said limited-use number comprises a static device account number,

and wherein the static device account number is of a limited scope of valid use to a specific device,

153. As discussed in Claim 19(e), Varadarajan teaches generating a DCV (*limited-use number*) for a PAN and CVV. In the case of a DCV being generated for a portion of the “static PAN,” Varadarajan teaches that the DCV may replace a portion of the PAN, e.g., the last ten digits, referred to as a “dynamic partial PAN.” *Varadarajan*, [0012]-[0013], [0021], [0030]-[0031]. A POSITA would understand that at least a portion of a dynamic PAN, therefore, includes parts of a static PAN.

a) Smith’s Teachings

154. 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 (EX1008)*, [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 (EX1008)*, [0014]-[0016], [0026].

155. This “temporary PAN is mapped to a **mobile PAN (e.g., such as a PayPass® PAN, or PPAN).**” *Smith (EX1008)*, [0026] (emphasis added). The PPAN (device account number) is “assigned to the mobile device 104.” *Smith (EX1008)*, [0016]. The PPAN is “stored in the mobile device 204.” *Smith (EX1008)*, [0022]. The PPAN is, therefore, a device account number.

156. Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith (EX1008)*, [0026], [0040]. The PPAN (device account number) is then associated with a “related PAN[.]” *Smith (EX1008)*, [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 (EX1008)*, [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 (EX1008), Fig. 6.

157. The issuer can “implement dual account number structures” so that “multiple NFC-enabled handsets may be managed for a single account.” *Smith (EX1008)*, [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 (EX1008)*,’s PPAN is a distinct account number for a payment account on a particular “mobile device” (a specific device).

158. 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 (EX1008)*, [0026] (“an instantly-issued payment

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

159. Smith teaches the expiration date associated with the account may be updated without updating the PPAN. *Smith (EX1008)*, [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 and mobile device, it is a static device account number for a specific device. A POSITA would further understand the PPAN is of limited scope of valid use in that it is only able to be used by the mobile device 104 within the expiration period. Thus, Smith’s PPAN is a static device account number [] of a limited scope of valid use to a specific device.

b) Motivation to Combine

160. A POSITA would have found it obvious and been motivated to use Smith’s PPAN in place of Kalgi’s account number. A POSITA would have appreciated that storing a PPAN would be safer than storing the actual account number on Kalgi’s device.

161. A POSITA would have been motivated to use Smith’s PPAN in place of Kalgi’s account number so that Kalgi’s mobile device would not be required to store the account number, which is a sensitive financial number. 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 Kalgi'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 (EX1043)*, [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 (EX1043)*, [0007], [0014], [0074], Fig. 6.

162. A POSITA would have had a reasonable expectation of success in implementing Smith's PPAN in Kalgi's payment application without undue experimentation because Kalgi already teaches use of account number and a POSITA would have been familiar with using PAN-alternatives. In the combination, Smith's PPAN would perform the same function—provide an account number that can be used for a payment transaction. *Smith (EX1008)*, [0021]-[0022]. A POSITA would have understood that using Smith's PPAN in place of Kalgi's account number would be combining prior art elements according to known methods to yield the predictable result of increased security. Indeed, as discussed in Section V.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). 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 (EX1005)*, [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 (EX1005)*, [0005]. A POSITA would have been motivated to apply Kalgi and Smith’s teachings and appreciated the compatibility of their teachings because both discuss payment systems that rely on similar functionalities.

163. A POSITA would have substituted Smith’s PPAN for Kalgi’s account numbers when making payment transactions, as taught by Smith. *Smith (EX1008)*, [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 (EX1008)*, [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 for another and a POSITA would have understood to predictably increase the security of Kalgi’s payment system and protected the user’s sensitive account information. A POSITA

would have recognized that modifying Kalgi's system according to the teachings of Smith required only basic software modifications and routine skill as it a simple substitution of one known element for another. 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 Kalgi 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, Kranzley, Grigg*. Thus, such a modification to Kalgi's system would have been straightforward.

164. A POSITA would have further found it obvious and been motivated to use the PPAN to generate a dynamic partial account number, as taught by Varadarajan. *See Claim 19(e)*. Thus, in combination, Kalgi-Khan-Varadarajan-Smith would generate a dynamic CVV and dynamic partial PPAN (DCV + portion of the PPAN), which is of limited scope of valid use to the user's specific device.

2. ***21(b): and wherein further a payment processing authority provides said device account number unique for the specific electronic device, in place of payment issuer information, in performing payment transactions by the electronic device, and further comprising:***

165. Smith teaches that the PPAN (device account number unique for the specific electronic device) is provided to the mobile device in place of an account number (payment issuer information). *Smith (EX1008)*, [0015]-[0018], [0026], [0029] Figs. 1-4, 6. Specifically, after a user requests an account, the issuer provides a temporary PAN to an OTA provisioning service. *Smith (EX1008)*, [0015]. The OTA provisioning service forwards the temporary PAN to a PAN mapping/account generation service, which assigns the PPAN to a mobile device and maps the PPAN to the temporary PAN, and subsequently to the real PAN. *Smith (EX1008)*, [0016], [0019], Figs. 1, 6. The OTA and PAN mapping/account generation services, which generate and provide the PPAN to the mobile device, are operated on behalf of a payment network, such as MasterCard. The PPAN is used in payment transactions by the mobile device. (*EX1008*), [0022]-[0023]. A POSITA would have understood, therefore, that the OTA and PAN mapping/account generation service are a payment processing authority that provides the device account number for the specific mobile device in place of the temporary and actual PAN for use in transactions.

3. 21(c): performing a payment transaction by the electronic device including the dynamically generated limited-use number;

166. Varadarajan teaches performing a payment transaction using a DCV. Specifically, Varadarajan teaches sending a DCV and other transaction information to an issuer/authenticating server. *Varadarajan (EX1006)*, [0027], [0045]; *see also* Claim 19(e). The issuer/authenticating server independently regenerates the DCV to authenticate the transaction. *Varadarajan (EX1006)*, [0027], [0043], [0045], [0056], Fig. 4. A POSITA would have found it obvious to perform a transaction using Varadarajan's DCV for same reasons discussed in Claim 19(e).

4. 21(d): combining the dynamically-generated number and the static device account number within a device-generated complete payment information; and

167. A POSITA would have found it obvious to combine the DCV, i.e., dynamic PAN and/or CVV, (dynamically-generated number) and Smith's PPAN (static device account number) in the payment data (device-generated complete payment information) sent to the merchant and financial institution in Kalgi. *See also* Claims 19(e)-(f).

5. 21(e): conveying said device-generated complete payment information, in place of a selected payment issuer information, when the device is performing payment transactions; and

168. A POSITA would have found it obvious to convey the DCV(s), PPAN, and other payment data (device-generated complete payment information) in place

of selected payment issuer information (e.g., CVV and/or PPAN) when the device is performing payment transactions. *See also* Claims 19(e), 21(a).

6. ***21(f): wherein a using of said static device account number without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage.***

169. In the proposed combination, if an invalid DCV is sent with the PPAN, the financial institution authenticating the transaction would not be able to regenerate the DCV. *Varadarajan (EX1006)*, [0027], [0043], [0045], [0056], Fig. 4. In that case, the transaction would not be authenticated because it would indicate that device is not able to conduct the requested transaction. *Varadarajan (EX1006)*, [0027], [0043], [0045], [0056], Fig. 4. A POSITA would understand, therefore, that using Smith's PPAN without a valid DCV would be denied as invalid and outside the scope of use for the mobile device.

XIII. GROUND 4: CLAIM 25 IS OBVIOUS OVER KALGI, VARADARAJAN, AND SMITH

A. Claim 25

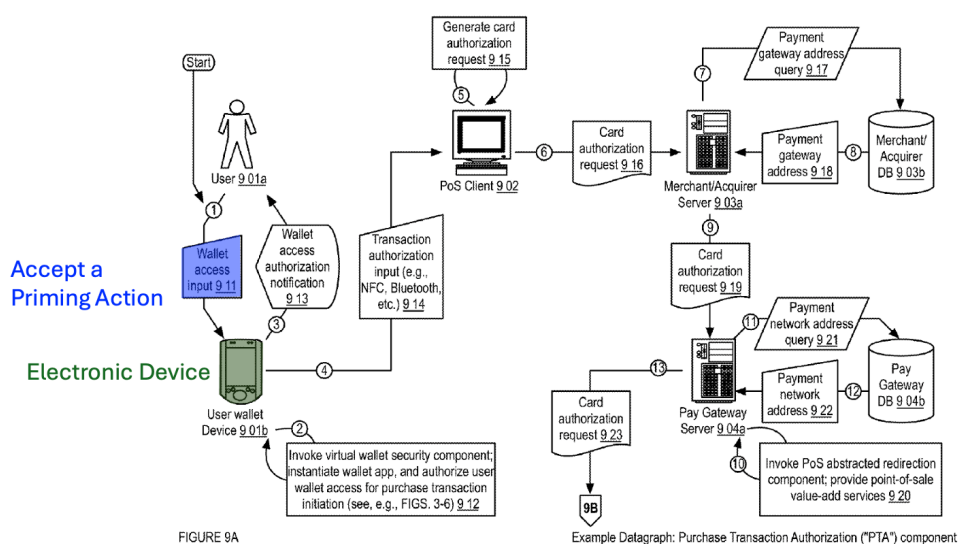
1. ***25(pre): A non-transitory, computer-readable medium storing computer executable instructions that when executed by one or more processors, cause the one or more processors to:***

170. To the extent the preamble is limiting, Kalgi teaches a user device, such as a mobile device, that executes "an E-Wallet application" (computer executable instructions) that causes the device to perform e-wallet functions. *Kalgi (EX1004)*,

[0048]; *see also*, Abstract, [0033] (“The user device may have executing thereon a wallet application, including features such as those as described herein.”), Figs. 1 (illustrating E-Wallet application on mobile device 102(b)), 2 (depicting wallet application interface). Kalgi further describes an “e-wallet checkout apparatus, comprising: a processor; and a memory disposed in communication with the processor and storing processor-issuable instructions to: ... receive a merchant payment request, ... instantiate, via the processor, a wallet application ..., obtain a payment method selection via the wallet application, provide a transaction execution request for a transaction ..., receive a purchase response ...; and output purchase response information” *Kalgi (EX1004)*, [0259]-[0268]; *see also*, [0198]-[0205], [0229]-[0236]. Therefore, that the E-Wallet application is stored on the mobile device’s non-transitory, computer readable medium as computer executable instructions that when executed by the device’s processor, cause it to perform the functions recited below.

2. 25(a): accept a priming action of the electronic device by an identified valid device user, identified from the device inputs;

171. Kalgi’s user device (the electronic device) accepts “a wallet access input” from the user. *Kalgi (EX1004)*, [0067], [0083], Fig. 9A.



Kalgi (EX1004), Fig. 9A (annotated).

172. The wallet access input is “a single tap (e.g., a one-tap mobile app purchasing embodiment) of a touchscreen interface, keyboard entry, card swipe, activating a RFID/NFC equipped hardware device (e.g., electronic card having multiple accounts, smartphone, tablet, etc.) within the user device, ... single/multi-touch gestures on a touch-sensitive interface, touching user interface elements on a touch-sensitive display[.]” *Kalgi (EX1004)*, [0067]. “[T]he user wallet device may authenticate the user based on the user’s wallet access input, instantiate a wallet application (see, e.g., FIGS. 13-19B) upon authenticating the user, and provide virtual wallet features for the user via the wallet application.” *Kalgi (EX1004)*, [0067]; *see also*, [0029], [0054]-[0055], [0083], Fig. 5.

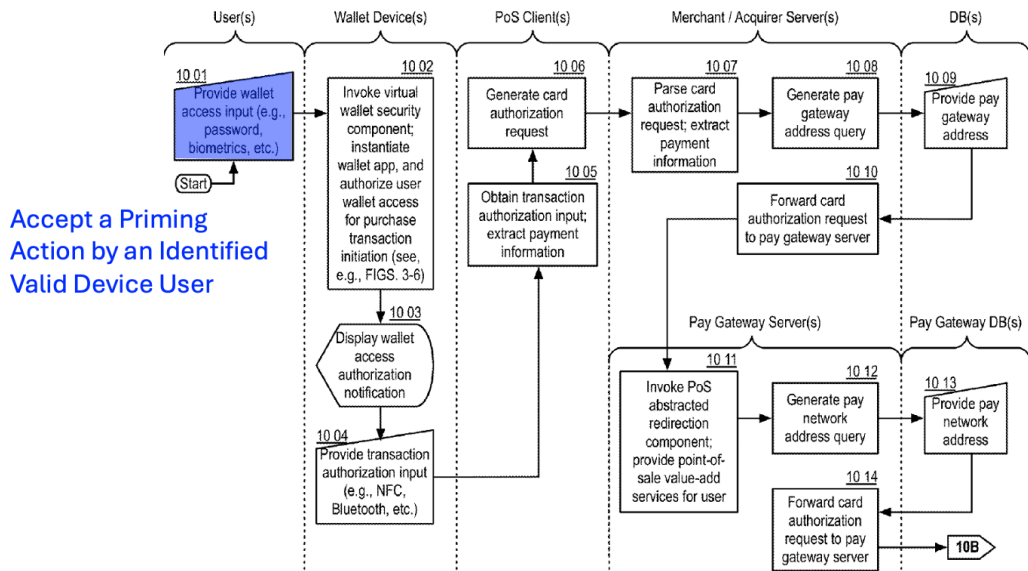


FIGURE 10A

Example Logic Flow: Purchase Transaction Authorization ("PTA") component

Kalgi (EX1004), Fig. 10A (annotated).

173. To perform the authentication, “the user may be required to enter login information, answer a challenge question, submit a voice/biometric signature, provide a digital certificate, enter into a video call for verification purposes, and/or the like.” *Kalgi (EX1004)*, [0051], [0067], [0083], [0145].

174. This mapping is consistent with the '538 Patent's description that bringing a device within range of a reader or a key input may form part of the priming operation. '538 *Patent (EX1001)*, 11:67-12:3, 13:65-14:1.

3. ***25(b): enable the electronic device for imminent performance of a payment operation responsive to the priming action of said valid user;***

175. *Kalgi* teaches that after accepting the wallet access input of the authenticated user (*said valid user*), the device “instantiate[s] a wallet application

(see, e.g., FIGS. 13-19B) upon authenticating the user, and provide[s] virtual wallet features for the user via the wallet application.” *Kalgi (EX1004)*, [0067]-[0068], [0083]-[0084]. “For example, the user wallet device may utilize the components described above in the description with respect to FIGS. 3-6 to provide e-wallet checkout services for the user via the wallet application.” *Kalgi (EX1004)*, [0067].

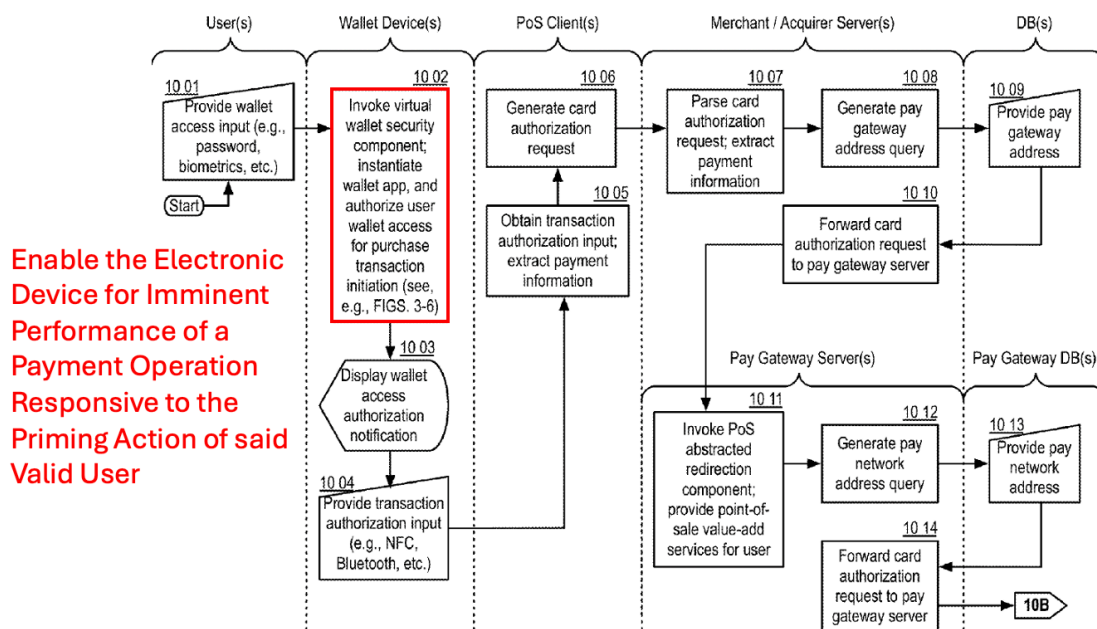


FIGURE 10A

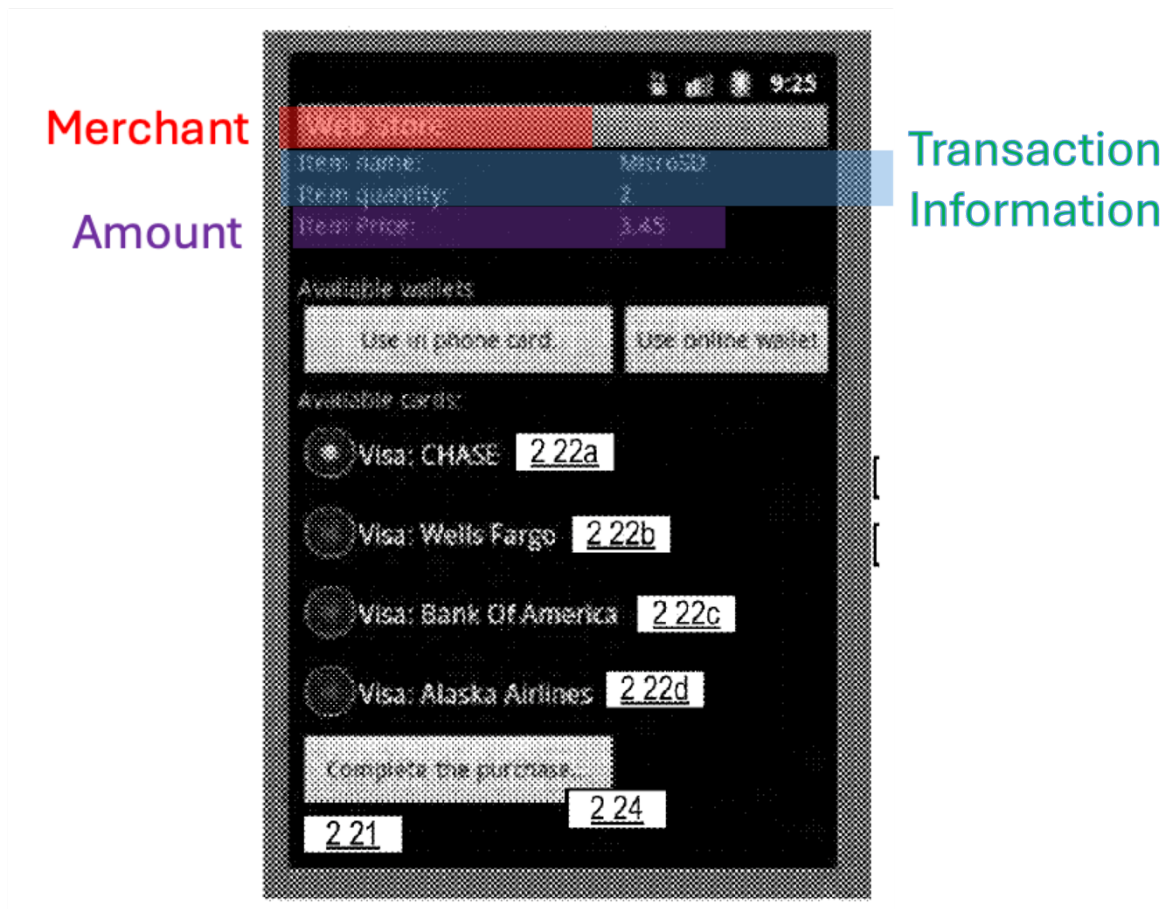
Example Logic Flow: Purchase Transaction Authorization ("PTA") component

Kalgi (EX1004), Fig. 10A (annotated), Fig. 9A.

176. By instantiating the wallet application and providing the wallet application features, the electronic device is enabled for imminent performance of a payment operation responsive to the wallet input of a valid user.

4. ***25(c): display a summary of online purchase information including the merchant information and the purchase amount; and,***

177. As shown in Figure 2, Kalgi's e-wallet application causes the processor to display a summary of online purchase information including the merchant information and purchase amount.



Kalgi (EX1004), Fig. 2 (annotated excerpt).

5. ***25(d): display at least one selectable issuer payment account methods on a display; and,***

178. See Claim 19(c).

6. 25(e): receive a payment selection and approval authorization from said valid device user via a human input sensing at the device; and

179. See Claim 19(d). A POSITA would understand that Kalgi's touchscreen interface performs human input sensing at the device. In particular, a POSITA would understand a capacitive touchscreen detects the touch of, for example, a the user's finger based on electrical properties of the human body. See, e.g., U.S. Patent No. 7,653,883 to Hotelling (EX1045), 4:6-18, 6:34-51, 8:15-34, 9:61-10:16, 25:29-36, 26:29-46, Figs. 3, 5, 23.

7. 25(f): responsive to receiving a valid user transaction payment approval, generate a device-specific limited-use payment information for use in place of at least a portion of said selected issuer payment account information on the device,

180. As discussed in Claim 19(c), Kalgi teaches that a user wallet device includes payment information, including an account number, account name, account address, CVV (including a dynamic CVV), and other information, in a compatible data form that is provided to a PoS client. *Kalgi (EX1004)*, [0068]-[0069], [0084]. As discussed in Claim 21(a), a DCV can be generated and used as part of a PPAN. See Claim 21(a); see also Claim 19(e). Because the PPAN is device-specific, a POSITA would understand a dynamic partial PPAN is device-specific limited-use payment information that is used in place of the PPAN.

181. Additionally, or alternatively, Varadarajan's 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.” *Varadarajan (EX1006)*, [0029]; *see also*, [0053] (“By including a device identifier in the DCV generator, where the included device identifier is unique to each user device accessing a joint account, **each transaction and DCV is further identifiable to the user device conducting a transaction** or requesting a DCV.”); Claim 19(e).

182. Thus, Varadarajan’s DCV, e.g., dynamic PPAN and/or CVV, is device-specific limited-use payment information that is dynamically generated for use in place of at least a portion of said selected issuer payment account information (e.g., the PAN, CVV, etc.) on the device.

8. ***25(g): form a complete combined device payment information from a dynamically generated portion and a statically generated portions stored in a memory of the device,***

183. As discussed above, Kalgi teaches device payment information for a credit card including, e.g., account number, account name, billing address, and CVV values. *Kalgi (EX1004)*, [0069]-[0070]. In addition, Kalgi teaches that the user wallet is stored on the mobile device, such as in memory. *Kalgi (EX1004)*, [0036]; *see also*, [0067]-[0069]. The user wallet includes issuer provided payment information, such as PAN and CVV, that is provided to the PoS client. *Kalgi (EX1004)*, [0069]. As discussed above, it would have been obvious to replace at least

of portion of the issuer provided payment information, such as the CVV, with Varadarajan's DCV. *See* Claim 25(f); *Kalgi (EX1004)*, [0069], [0083].

184. Thus, it would have been obvious to further configure Kalgi's electronic device to form a complete combined payment information from Varadarajan's DCV (e.g., CVV) (a dynamically generated portion) and (mobile wallet) account number, account name, billing address, etc. (a statically generated portions stored in a memory of the device) for the same reasons. *See* Claims 19(e), 21(a).

9. ***25(h): wherein the communication interface is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction; and***

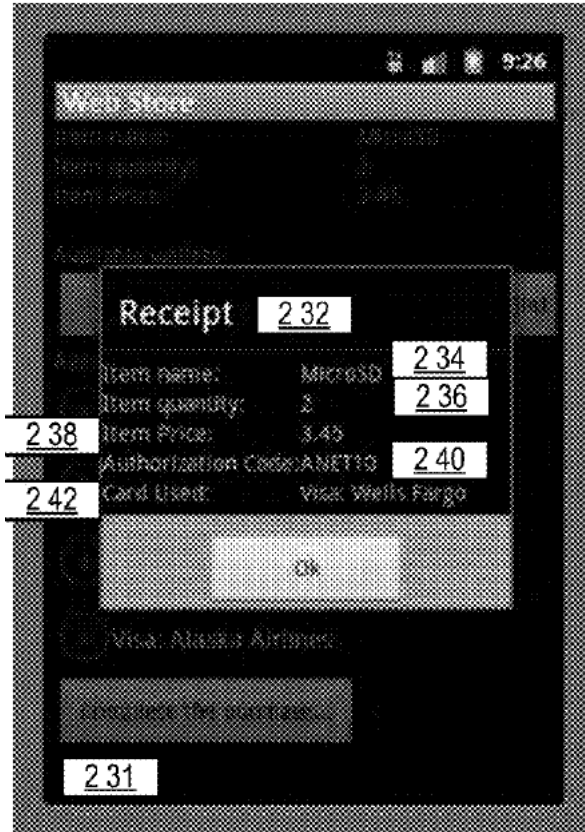
185. Kalgi teaches that the user wallet device can provide payment information to the merchant PoS client using various communication technologies, including Wi-Fi, Bluetooth, NFC. *Kalgi (EX1004)*, [0068], [0084]; *see also* Claim 19(a). The payment information is "formatted according to a data formatting protocol appropriate to the communication mechanism employed in the communication between the user wallet device and the PoS client." *Kalgi* at [0069], [0084]. A POSITA would have understood that Kalgi's device, e.g., a cellular phone, includes interfaces for communicating with the PoS client using these technologies. Otherwise, the device could not communicate with a merchant website over Wi-Fi, for example, if it did not include a Wi-Fi interface. Mobile devices were known to

include wireless interfaces, such as wi-fi or cellular interfaces, that would allow the device to exchange information with a merchant served during a transaction. *See Khan (EX1005)*, [0018], [0022], Fig. 2; *Lin*, 15:7-9, 22:21-23:30, Figs. 1, 3. Thus, the combination also teaches that the communication mechanism (communication interface) is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction.

10. 25(i): wherein further the processor is operable to receive an approval and a denial confirmation from an online payment facility of the complete device payment information, and cause the display to visually convey a status of the online purchase transaction.

186. The processor of Kalgi's device is further operable to receive a receipt from the EWCP provider or payment/issuer servers (an online payment facility). *Kalgi (EX1004)*, [0030], [0033], [0038], [0081]-[0082], [0092]; *see also*, [0259]-[0268] ("... receive a purchase response to the transaction execution request; and output purchase response information derived from the received purchase response."). Because the receipt is only sent when the transaction is approved, it qualifies as an approval confirmation. *Kalgi (EX1004)*, [0038].

187. As shown in Figure 2, the receipt 232 is displayed on screen 231 to visually convey the status of the online purchase transaction.



Kalgi (EX1004), Fig. 2 (annotated excerpt); *see also*, Figs. 9B, 10B.

188. *Kalgi* also teaches “[i]f the payment was unsuccessful, the purchase may be denied.” *Kalgi (EX1004)*, [0050]. “For example, the user may be directed to a webpage that informs the user that the payment was unsuccessful[.]” *Kalgi (EX1004)*, [0050]; *see also*, Figs. 4, 10B (“Display ... transaction declined notice for user”). The approval or denial are only sent once the payment information is received and processed by EWCP provider or one or more payment processing facilities. *Kalgi (EX1004)*, [0044], [0072]-[0082], [0086]-[0092], Figs. 9A-9B, 10A-B.

189. Thus, Kalgi's processor is also operable to receive a denial confirmation from an online payment facility of the complete device payment information, and cause the display to visually convey a status of the online purchase transaction.

XIV. GROUND 5: CLAIMS 28-30 ARE OBVIOUS OVER KALGI, KHAN, VARADARAJAN, HAMMAD AND SMITH

A. Claim 23

1. **23(a): The method of claim 19, wherein a payment processing authority verifying and authorizing a transmitted limited-use number based on a time of use, and cryptographically combining a transaction sequence count information; a device account number; a user account information; a payment issuer information; a payment processing authority secrets; a transaction information; and,**

190. As discussed in Claims 20(a) and 21, it would have been obvious to generate a DCV/dCVV (limited-use number) by cryptographically combining an ATC (transaction sequence count information), PPAN (device account number), information relating to a user, such as telephone number or home address (user account information), expiration date or service code (payment issuer information), PIN verification data or master derivation key (payment processing authority secrets), and payment amount (transaction information).

191. Hammad further teaches that the dCVV may be generated using time as one of the dynamic data elements. *Hammad (EX1007)*, 3:9-11, 4:37-40, 4:61-5:5, 6:49-57, 7:4-14, Figs. 4-5. The service provider can use the time of day (time of use)

to determine whether it is within a certain range in authenticating the transaction.

Hammad (EX1007), 8:28-36.

192. A POSITA would have found it obvious, and been motivated, to implement Hammad's time of use check in authorizing a transaction or use the time of day in generating the dCVV. A POSITA would have recognized that using the time of day provides an additional layer of security to the authorization process. Using a temporal element in authenticating a transaction to prevent replay attacks was known long before the '538 Patent. For example, I wrote papers on timestamps for a similar purpose (i.e., preventing replay attacks) as early as 1993. *See* EX1046, *A Note on the Use of Timestamps as Nonces*. Using timestamps as a security measure to prevent replay attacks in credit card transactions was also known as early as 1997. *See* U.S. Publication No. 2002/0174075 to Mirlas (EX1047), Abstract, [0038]-[0039], [0124] (describing a payment message sent for an online transaction that includes payment info and timestamp "to prevent replay attack, among other information), Figs. 1-2; U.S. Patent No. 5,903,721 ("Sixtus") (EX1048) at Abstract 8:57-66 ("The time stamp is an additional security feature ... which is preferred since it changes with every transaction request and makes it more difficult to spoof (trick) the system."). Sixtus cites my paper titled "Requirements for Network Payment: The NetCheque Perspective," on its face (although he misspells my last name). Implementing this feature in Kalgi would have predictably yielded the result of

increased security by limiting the time for which a generated DCV/dCVV could be used. This modification would not change the operation of the combination or require any additional hardware; rather, it would require only minor programmatic changes.

2. ***23(b): further comprising: receiving an authorization of said transaction, responsive to verifying a valid limited-use number appearing in a transaction information in place of the payment issuer information; and***

193. Kalgi teaches a provider sending and displaying a receipt or payment confirmation message to a customer confirming the purchase transaction (authorization of said transaction). Kalgi (EX1004), [0038], [0044]-[0046], [0050], [0060]-[0061], [0064], [0081]-[0082], [0092], Figs. 2 (element 231), 3, 6, 8, 9B, 10B (“Display purchase receipt ... declined notice for user”). Varadarajan and Hammad teach a financial institution verifying the limited-use DCV/dCVV, and other payment information, used in the payment transaction. Varadarajan (EX1006), [0045], [0056], Fig. 4; Hammad (EX1007), 7:55-8:44, Fig. 6.

194. A POSITA would have understood that in the combination, Kalgi’s receipt/payment confirmation would only be received by the mobile device if the DCV/dCVV generated and sent by the mobile device in place of the payment issuer account information, and other payment information, was verified by the service provider.

3. ***23(c): a rejecting by the payment processing authority, on a detecting as invalid at least one verification test, from a set of tests comprising:***

a mis-matching of the transacted limited-use number, and the authority cryptographically-combined number;

a transactional use of a device account number outside of its limited scope of valid payment reader facility use;

a transactional use outside of a valid time window;

a transactional re-use of a number limited to a one-time use; and,

a transactional use of an expired number outside of a limited time-of-use.

195. Kalgi teaches that if the payment was unsuccessful, the purchase may be denied by the provider and the user notified of the same in the display. *Kalgi (EX1004)*, [0050], Figs. 4, 10B (“Display ... transaction declined notice for user”).

196. Varadarajan teaches the authenticating server independently generates a DCV to determine if the inputted DCV matches. *Varadarajan (EX1006)*, [0033], [0045], [0056], Fig. 4. Varadarajan further teaches the server determines whether the DCV is expired, based on number of uses or time. *Varadarajan (EX1006)*, [0045], [0047], [0056], Fig. 4.

197. Hammad teaches that if the service provider generated dCVV (*authority cryptographically-combined number*) does not match (*mis-matching*) the dCVV provided by the mobile device (*transacted limited-use number*), the transaction is terminated. *Hammad (EX1007)*, 8:47-50, Fig. 6. Hammad also teaches

that if a dCVV is being used outside of a time window (valid time window), “the transaction may be declined.” *Hammad (EX1007)*, 8:38-36. As discussed, it would have been obvious to implement such a time window check to increase security. *See* Claim 23(a).

B. Claim 28

1. ***28(a): The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further causes the one or more processors to perform:***

a combining of a static device-specific payment account information, a device generated information, and other user and account information stored on the device which is uniquely identifying the specific user, specific selected account, and the specific device; and,

198. Hammad teaches a user device maintaining and combining static data elements, such as a telephone number, account number, home address, expiration date, birthday, etc. (user and account information), with dynamic data elements to generate a dCVV (device generated information). *See* Claim 19(e); *Hammad (EX1007)*, 4:21-60.

199. Smith teaches assigning and storing a PPAN (static device-specific account information) on a user’s device. *See* Claim 21(a); *Smith (EX1008)*, [0016], [0021]-[0022].

200. Varadarajan teaches using a “unique device identifier ... generated from unique data collected from the user device” (device generated information) to

generate a DCV. [0049]. By including the device identifier in this process, “each transaction and DCV is further identifiable to the user device conducting a transaction or requesting a DCV.” *Varadarajan (EX1006)*, [0053].

201. Thus, a POSITA would have understood, or found it obvious, to store this information in the user device while performing a transaction. It would have been obvious to modify Kalgi with the teachings of Hammad, Smith, and Varadarajan to combine this information in generating a DCV/dCVV for the same reasons discussed above in Claims 19, 20, 21(a), 21(e), and 25(f). When combined in this way, the stored information *uniquely identif[ies] the specific user, specific selected account, and the specific device.*

2. ***28(b): a generating of a limited-use payment information by the one or more device processors cryptographically generating at least one one-time limited-use cryptogram numbers; and,***

202. See Claims 19(e), 20(a).

3. ***28(c): wherein the one or more device processors are further operable to combine said limited-use static device account information and said one-time use cryptogram number(s) to produce the complete combined device payment information; and,***

203. See Claims 19(f), 20(a), 21(d), 25(g).

4. *28(d): wherein the one or more device processors are further operable to transmit said complete payment information in place of said user-selected payment account information in a device payment transaction; and,*

204. *See Claim 19(i), 25(g)-(h).*

5. *28(e): wherein the one or more device processors are further operable to display at least a portion of said user-specific selected account information associated with said complete device payment information used during said transaction, via a user interface disposed of the device.*

205. *See Claims 19(c), 25(d).*

C. Claim 29

1. *29(a): The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more processors to dynamically generate a one-time limited-use cryptogram number, via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority, and selected from a set of information known and stored at both said payment authorities, and on said device, including:*

a transaction sequence counter,

a device account number,

...

a payment processing authority secret,

a user information,

a payment account information,

...

a payment amount, transactional information; and,

206. Varadarajan, Hammad, and Smith render obvious cryptographically combining various pieces of information stored on a device to generate a DCV/dCVV (one-time limited-use cryptogram number). See Claim 28(a); see also Claims 19(f), 20(a), 21(d). Hammad teaches a user device maintaining (store) and combining data elements, such as a telephone number, account number, home address, expiration date, birthday, etc. (payment account information and user information); an ATC (transaction sequence counter); information relating to the

consumer's portable consumer device; current transaction amount (payment amount, transactional information); and master derivation key (payment processing authority secret) to generate a dCVV. *See* Claim 19(e); *Hammad (EX1007)*, 4:21-60, 5:38-57.

207. Varadarajan teaches using a “unique device identifier ... generated from unique data collected from the user device” (information unique to the device and device secret), which is known the provisioning and authenticating servers, to generate a DCV. *Varadarajan (EX1006)*, [0049]-[0050]; *see also* Claim 28(a). Varadarajan also teaches using the payment amount to generate a DCV. *Varadarajan (EX1006)*, [0055].

208. Smith teaches assigning and storing a PPAN (device account number) on a user's device. *See* Claim 21(a); *Smith (EX1008)*, [0016], [0021]-[0022].

209. Thus, a POSITA would understand, or found it obvious, to store this information in the user device before generating a DCV/dCVV. It would have been obvious to modify Kalgi with the teachings of Hammad, Smith, and Varadarajan to combine this information in generating a DCV/dCVV for the same reasons discussed above in Claims 19(e), 20, 21(a), 21(e), 22(b), and 25(f).

210. Further, 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 issuer system. *Smith (EX1008)*, [0012], [0016], [0038]-[0040], Fig. 6.

211. Varadarajan teaches that the service provider 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. *Varadarajan (EX1006)*, [0045]; *see also*, [0033], [0056]. A POSITA would understand that the user account information used to generate the DCV key that is used to generate the DCV generator would have also been stored at the authenticating and/or provisioning server in order to verify the same. *Varadarajan (EX1006)*, [0043], [0045]. Thus, a POSITA would understand this information is stored at the authenticating server to independently generate a DCV.

212. Alternatively, it would have been obvious to store this information the payment processing authority and/or payment issuer. For example, Hammad teaches that the payment processing authority and issuer both “validate cryptogram” (i.e., dCVV). *Hammad '089 Provisional (EX1011)*, p. 78. Some payment processing entities perform the functions of payment processor and issuer. *Hammad '089 Provisional (EX1011)*, [0025]. Thus, a POSITA would understand that in order to validate the cryptogram (i.e., dCVV), each authority would need to store the information from which the dCVV was generated, as described above.

2. ***29(b): wherein said one or more processors uses said one-time limited-use cryptogram number in place of at least a portion of an issuer's static payment information, in a payment transaction using said payment account; and,***

213. As discussed, a DCV/dCVV is used in place of an issuer's CVV or account number (*static payment information*) in a payment transaction using the selected payment account. *See* Claims 19(e), 20(a).

3. ***29(c): wherein said payment authorities are operable to recognize from the transactional payment information, the correct set of user, device and account specific information to be cryptographically combined into an authority computed cryptogram, for comparing with device transmitted limited-use payment information; and,***

214. As discussed in Claim 23(b)-(c), the authority verifying the DCV/dCVV re-generates the DCV/dCVV in the same way and using the same information as the user device. The authority-generated DCV/dCVV are compared with the user-device generated DCV/dCVV. *See* Claim 23(b)-(c); *see also* Claims 21(f), 23(f). A POSITA would understand that in order to re-generate a DCV/dCVV, the verifying authorities would need to recognize what information needs to be used to perform such a re-generation. *See also* Claim 29(a).

4. ***29(d): wherein said payment processing authorities are operable to deny as invalid a transaction including a cryptogram not matching an authority computed cryptogram; and,***

215. *See* Claims 23(c), 25(i).

5. ***29(e): wherein said payment authorities are operable to approve as valid a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,***

216. See Claims 23(b), 25(i).

6. ***29(f): wherein said device is operable to receive an approval and a denial status of said transaction, from said payment authorities, and visually convey said transaction status in the user-interface on the display disposed of the device.***

217. The proposed combination teaches or render this limitation obvious.

See Claims 23(b)-(c), 25(i).

D. Claim 30

1. *30(a): The electronic device of claim 25, further comprising a processor and a non-transitory, computer-readable medium storing computer executable instructions that when executed by the one or more processors, cause the one or more device processors to dynamically generate a one-time limited-use cryptogram number by a cryptographic combination, of at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic device, and selected from a set of information including:*

a transaction sequence counter;

a user payment account number;

a device payment account number;

a device secret; device keys;

a payment issuer original account information;

a payment issuer device account information;

a payment processing authority secret;

a transaction information;

and a user private information; and,

218. As discussed in Claim 29 (a), it would have been obvious to generate a DCV/dCVV (one-time limited-use cryptogram number) by cryptographically combining information, including at least one of: account number, home address, expiration data, birthday, etc. (user payment account number and user private information), ATC (transaction sequence counter), current transaction amount (transaction information), device identifier (device secret), master derivation key

(payment processing authority secret), and PPAN (device payment account number)

that is unique to the device. See Claim 29(a); see also Claim 20(a), 23(a). Further, as discussed in Claims 29(a), this information would be known to the user device, payment processing authority, and payment issuer authority.

2. ***30(b): wherein said cryptogram is operable to be used in place of at least a portion of an issuer's static payment information, in a payment transaction for said selected payment account; and,***

219. See Claim 29(b).

3. ***30(c): wherein said payment processing authority is operable to deny as invalid, a transaction including a cryptogram not matching a payment processing authority computed cryptogram; and,***

220. See Claim 29(d).

4. ***30(d): wherein said payment processing authority is operable to approve as valid, a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,***

221. See Claim 29(e).

5. ***30(e): wherein said user device is operable to receive an approval and a denial status of said transaction information validation, and visually convey said transaction status in the user-interface on the display disposed of the device; and,***

222. The proposed combination teaches or renders obvious this limitation.

See Claims 23(b)-(c), 25(i), 29(f).

6. *30(f): wherein said user device is operable to emulate the behavior of an issuer account payment transaction, when said complete device payment information is used in electronic payment facilities.*

223. A POSITA would understand that when a user device is used as described in Claims 25 and 30, the device emulates the behavior of a payment transaction involving an issuer account, i.e., credit card, when the payment information is received and processed by the payment authorities.

XV. GROUND 6: CLAIM 26 IS OBVIOUS OVER KALGI, VARADARAJAN, HAMMAD, SMITH AND BAUER

A. Claim 26

1. *26(a). The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more processors to:*
- receive the priming action of a user via the device human input sensors;*

224. Kalgi teaches that user device accepts a “wallet access input” via the device human input sensors (e.g., NFC hardware, touchscreen interface, voice, etc.) as part of a priming action. *See* Claim 25(a).

2. ***26(b): identify an authorized valid device user through a human to device inputs, selected from at least one security challenge, of a set of human to device input challenges comprising:***

a correct passcode touch entry sequence,

a correct touch gesture,

...

a biometric recognition of a valid user,

...

***a security question which a valid user could answer correctly,
and***

225. As described in Claim 25(a), Kalgi teaches authenticating a user by requiring at least one security challenge, including entry at a touchscreen (human device input) of login information (a correct passcode touch entry sequence), answering a challenge question (a security question which a valid user could answer correctly), single/multitouch gestures on a touchscreen interface (a correct touch gesture), submitting voice/biometric signature (a biometric recognition of a valid user), among other authorization measures. *Kalgi (EX1004)*, [0051], [0067], [0083], [0145].

3. ***26(c): receiving a correct user response input, from a security challenge presented on the device display; and***

226. Kalgi teaches the “user wallet device ... authenticate[s] the user based on the user’s wallet access input,” and if the user is verified, “the client may obtain

security credentials ... from the client's memory, to launch the wallet application, and may instantiate the wallet application.” *Kalgi (EX1004)*, [0051], [0067]-[0068], [0083]-[0084], [0145]; *see also* Claim 26(b).

4. 26(d): responsive to receiving an incorrect user response input, offer a reduced number of additional challenge attempts before failing the user authorization at the device, and denying the payment authorization.

227. *Kalgi* teaches that if the authentication information is not valid (incorrect user respond input), the user is informed that login information was incorrect. *Kalgi (EX1004)*, [0055]. *Kalgi* also teaches that “if the number of failed authorization attempts exceeds a threshold,” e.g., when the payment options has insufficient funds, the server may “abort the authorization process, and provide an ‘authorization fail’ message to the ... user device[.]” *Kalgi (EX1004)*, [0078], [0090]. A POSITA would have found it obvious to apply *Kalgi*’s threshold attempts to the user authentication process. Using a threshold of authentication attempts at a user device was commonplace at the time. *See* U.S. Patent No. 8,127,999 to Diamond (EX1049), 22:15-53 (describing authentication of a mobile device user to interact in a payment transaction by allowing the user a maximum of three tries to enter a valid personal identification number (PIN).”), Fig. 13. A POSITA would have been motivated to implement such a process in *Kalgi*’s device to increase device security and prevent unauthorized users from making purchases if they had access to the mobile device. This modification would have been using known

techniques to improve a device in a known way and a POSITA would have had a reasonable expectation of success in making this modification to yield the predictable result of increased security.

228. To the extent that Patent Owner argues that such a modification would not have been obvious, it would have been obvious in view of Bauer.

a) Bauer's Teachings

229. Bauer teaches a process for conducting a payment transaction using a mobile device that stores a wallet application for one or more accounts, such as a credit. *Bauer (EX1009)*, [0073]-[0074], [0087]. A user provides input to activate a payment feature with the wallet application. *Bauer (EX1009)*, [0086]. If required, the mobile device prompts the user for entry of a PIN and compares the entered PIN to a pre-defined PIN. *Bauer (EX1009)*, [0087], [0090]. If the entered PIN is incorrect, the mobile device updates a count of the incorrect PIN entry attempts and if a PIN is entered incorrectly a defined number of times, lock the PIN, which “effectively prohibits the payment feature for the mobile payment account[.]” *Bauer (EX1009)*, [0087], [0090]. A POSITA would understand that through this process a user is offered a reduced number of additional challenge attempts before failing user authorization and denying payment authorization.

b) Motivations to Combine

230. It would have been obvious and a POSITA would have been motivated to configure an electronic device to offer a pre-defined number of security challenge attempts before failing user authorization, as taught by Bauer. This modification would have predictably reduced the possibility that an unauthorized person would gain access to the mobile device wallet. Therefore, a POSITA would have been motivated to improve similar devices and methods in the same way. There would have been a reasonable expectation of success because Bauer's methodology was commonplace at the time and would have required minimal software changes to Kalgi's device as it constitutes a combination of known elements that yield a predictable result of preventing an unauthorized user from accessing a payment application. Indeed, given Kalgi already requires the entry of a PIN, the modification would simply require putting a cap on the number of attempts before a payment authorization request could be sent; such a cap on accessing a payment application was a well-known function of mobile devices at the time. *See* U.S. Patent No. 8,127,999 (EX1049), 22:15-53 (describing authentication of a mobile device user to interact in a payment transaction by allowing the user a maximum of three tries to enter a valid personal identification number (PIN).”), Fig. 13.

**XVI. GROUND 7: CLAIM 27 IS OBVIOUS OVER KALGI,
VARADARAJAN, HAMMAD, SMITH, AND KRANZLEY**

A. Claim 27

- 1. 27(pre): The non-transitory, computer-readable medium of claim 25, wherein the one or more processors include a cryptographic processor, and wherein the executable instructions further cause the one or more processors to:***

231. Kalgi teaches “instantiating, via a processor, a wallet application.” *Kalgi (EX1004)*, [0198], [0229], [0259]-[0261]. Hammad’s “portable consumer device” includes a microprocessor and performs various encryptions techniques, including generating encryption keys and encrypting static and dynamic data elements to generate a dCVV. *Hammad (EX1007)*, 3:51-54, 5:2-6:34, Figs. 1-3. Hammad also teaches that its system can be implemented using hardware or a combination of hardware and software. *Hammad (EX1007)*, 9:31-38. A POSITA would understand Hammad’s processor is a cryptographic processor because it performs cryptographic functions, including multi-level encryption. *See ’538 Patent (EX1001)*, 1:42-47.

232. Alternatively, it would have been obvious to modify Kalgi based on the teachings of Khan.

a) Khan’s Teachings

233. Khan discloses a mobile device having a secure element (“SE”) (cryptographic processor) for use in generating dynamic payment data for

conducting payment transactions, including online. *Khan (EX1005)*, [0018], [0021], [0022]-[0025], [0028], Figs. 2, 4. Specifically, Khan discloses a portable device with an SE configured to store and process credit card information. *Khan (EX1005)*, [0018], Fig. 2. In conducting an online or in-store transaction, the SE generates an “alias” of the credit card number and encrypts the alias and “crypto data,” which is a digitally-signed combination of the alias, a counter value, a merchant identifier, or any other important value, using a shared key. *Khan (EX1005)*, [0023]-[0024], [0028], Figs. 2, 4. This information is sent to a backend server that validates the combination of alias and crypto data using a shared secret key. *Khan (EX1005)*, [0025], [0028]. A POSITA would have understood that Khan’s SE is a cryptographic processor because it is a hardware component isolated from an application processor and that stores encryption keys and secrets and performs cryptographic functions. See U.S. Patent No. 8,646,059 to von Behren (EX1050) at 4:38-55 (describing “contactless payment devices” such as “smart phones; mobile phones” that include a “secure element” that includes “crypto processors”), Figs. 1-2.

b) Motivation to Combine

234. It would have been obvious to configure Kalgi’s processor in combination to include a secure element for cryptographically combining payment data, as taught by Khan. A POSITA would have understood that a general purpose processor accessing payment data could be compromised. A POSITA would have

been motivated to include a secure element to handle and process the payment data and perform the cryptographic functions of Varadarajan and Hammad in order to prevent this risk. Indeed, Khan expressly recognizes how the secure element reduces that risk. *Khan*, [0004], [0018], [0024]. As the use of an SE in mobile devices for this purpose was well-known around this time, a POSITA would have had a reasonable expectation success in modifying Kalgi's device to include the same for performing cryptographic functions recited by Claim 27. *See* U.S. Patent No. 8,646,059 (EX1050), 4:38-55 (describing "contactless payment devices" such as "smart phones; mobile phones" that include a "secure element" that includes "crypto processors"), Figs. 1-2; EX1051, *SmartCard Alliance*, at 19 (describing a "secure element" as "a secure microprocessor (a smart card chip) that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing payment applications"). This combination of known elements to achieve recognized benefits would have yielded the predictable result of more secure payment transactions.

2. 27(a): cryptographically compute a dynamically generated one-time-use cryptogram number,

235. *See* Claim 20(a)-(b).

3. ***27(b): and combine said dynamically generated portion with a static device-specific account number known to a payment processing authority and limited in use to the device use in place of an issuer payment method; and,***

236. See Claims 19(f), 21(a)-(e), 29(a).

4. ***27(c): wherein further said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count, a payment account information, a user information, and information stored in the device and specific to the device and which is not communicated in the transaction; and,***

237. See Claims 20(a), 28(a). As discussed in Claim 25(f), Varadarajan teaches using a DCV generator to generate the DCV using a DCV key. *Varadarajan (EX1006)*, [0015], [0034] [0050]. The DCV generator is stored in the device and is specific to the device because it is generated from, and uses, a device identifier in generating a DCV. *Varadarajan (EX1006)*, [0049], [0053]. Further, the device identifier is stored in and specific to the device and does not pass in the transaction. *Varadarajan (EX1006)*, [0049]. A POSITA would have found it obvious to use a device identifier, as information “relat[ing] to a consumer’s portable consumer device,” as an additional data element in generating a DCV/dCVV, as taught by Hammad, in the proposed combination. See Claim 20(a).

5. ***27(d): wherein said transaction sequence counter, said information and said secrets are known to both said device, and to said payment processing authority; and,***

238. See Claims 20(a), 28(a), 29(a).

6. ***27(e): wherein further said static device-specific device account number is known to a payment issuer, and has a device-specific expiration date of limited duration of validity; and,***

239. See Claim 21(a)-(c).

a) Kranzley's Teachings

240. Kranzley teaches a system for conducting payment transactions using a mobile device having a payment application installed thereon. *Kranzley (EX1010)*, Abstract, [0016], [0019], [0021], [0038]. The payment application can store a virtual payment account number ("VPAN"), which is different than, but associated with, a PAN, and can be used in a transaction. *Kranzley (EX1010)*, [0036], Fig. 5. The VPAN "may have its own virtual expiry date." *Kranzley (EX1010)*, [0036], [0064], [0068], Fig. 5. The VPAN is used, along with expiry date and dynamic data (used in place of a CVV), in the transaction and sent to the issuer, which will deny or allow the transaction based on the VPAN (and associated PAN) and expiry date. *Kranzley (EX1010)*, [0023]-[0027], [0035], [0037]-[0049], Fig. 6.

b) Motivations to Combine

241. A POSITA would have found it obvious and been motivated to use an expiration date with Smith's PPAN in the combination, as taught by Kranzley. As noted by Kranzley, the expiry date is sent to a payment processor and used to conduct an initial authorization check on the VPAN. *Kranzley (EX1010)*, [0056], [0068], Fig. 3. The use of expiration dates in this manner was well-known long before the '538

Patent. A POSITA would have been motivated to use this information to improve similar mobile wallet systems in the same way. A POSITA would have had a reasonable expectation of success implementing this modification because the combination already contemplates including the expiration date in the combined payment information sent to the payment processing authority. *See Hammad (EX1007)*, 7:1-3, 7:25-28, Figs. 4-5. As such, this modification would be combining prior art elements according to known methods that would yield predictable results of ensuring a valid (i.e., not expired) account number is being used.

7. ***27(f): wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram,***

242. As discussed in Claim 20(a), the DCV/dCVV is generated from at least the account number (static device-specific device account number), expiration date (device account expiration date), telephone number, home address, etc. (user information), service code (payment account information), and DCV/dCVV (dynamically generated cryptogram). In the combination, it would have been obvious to use the PPAN and expiration date as an additional data element. *Hammad (EX1007)*, 4:52-56. Hammad further teaches the information used to generate a DCV/dCVV is part of the payment data sent to a payment processing authority. *Hammad (EX1007)*, 4:61-6:34, 6:49-7:54, Figs. 1, 4-5; *see also Kranzley (EX1010)*,

[0023]-[0027], [0035], [0037]-[0049], Fig. 6. A POSITA would have had a reasonable expectation of success implementing this modification for the same reasons recited in Claims 19(e), 20(a), 27(f).

8. ***27(g): and transmitting said complete device payment information when said issuer payment account method is selected.***

243. See Claim 21(e), 25(d)-(e), (h).

XVI. CONCLUSION

244. 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.