

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

CARDWARE INC.
Patent Owner

Case No. IPR2025-01145
U.S. Patent No. 10,339,520

**DECLARATION OF DR. CLIFFORD NEUMAN
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 10,339,520**

TABLE OF CONTENTS

I.	INTRODUCTION.....	17
A.	EDUCATIONAL BACKGROUND AND PROFESSIONAL EXPERIENCE	17
II.	MATERIALS CONSIDERED	20
III.	OVERVIEW AND LEGAL STANDARDS.....	21
A.	PERSON OF ORDINARY SKILL IN THE ART	22
B.	OBVIOUSNESS	23
C.	CLAIM CONSTRUCTION	28
D.	PRINTED SUBJECT MATTER	28
IV.	LEVEL OF A PERSON OF ORDINARY SKILL	29
V.	OVERVIEW OF THE '520 PATENT.....	30
A.	SUMMARY OF THE '520 PATENT	30
B.	FIELD OF ENDEAVOR	31
C.	PROBLEM PURPORTEDLY SOLVED BY THE INVENTORS OF THE '520 PATENT	32
D.	THE PROSECUTION HISTORY OF THE '520 PATENT.....	33
VI.	BACKGROUND OF TECHNOLOGY	34
A.	THE EVOLUTION OF PAYMENT CARDS.....	35
1.	<i>Magnetic Stripe Cards</i>	<i>35</i>
2.	<i>Smart/Chip Cards</i>	<i>38</i>
3.	<i>Europay, MasterCard, and Visa (EMV) Standard.....</i>	<i>39</i>
B.	CONTACTLESS PAYMENTS	39
1.	<i>Near Field Communications.....</i>	<i>39</i>
2.	<i>Active Mode</i>	<i>41</i>
3.	<i>Passive Mode.....</i>	<i>43</i>
C.	CONTACTLESS EMV PAYMENT CARDS	44
1.	<i>Mobile Devices and Mobile Wallets</i>	<i>45</i>
2.	<i>Card Emulation Mode</i>	<i>48</i>
3.	<i>Contactless ATMs</i>	<i>50</i>

D.	PAYMENT CREDENTIAL SECURITY FEATURES	54
1.	<i>Alternatives to a Payment Account Number (PAN)</i>	55
2.	<i>Alternatives to Static Card Verification Values</i>	58
VII.	SUMMARY OF UNPATENTABILITY	60
VIII.	SUMMARY OF THE PRIOR ART	61
A.	TOOMER.....	61
1.	<i>Toomer is Analogous</i>	62
B.	GRIGG	62
1.	<i>Grigg is Analogous</i>	63
C.	HAMMAD	63
1.	<i>Hammad is Analogous</i>	64
D.	MULLEN '449.....	66
1.	<i>Mullen '449 is Analogous</i>	67
E.	CASEY.....	67
1.	<i>Casey is Analogous</i>	68
F.	LIN.....	68
1.	<i>Lin is Analogous</i>	69
G.	MULLEN '760.....	71
1.	<i>Mullen '760 is Analogous</i>	72
H.	GRIFFIN.....	72
1.	<i>Griffin is Analogous</i>	73
IX.	GROUND 1: CLAIMS 10-13 ARE OBVIOUS OVER TOOMER, GRIGG, AND HAMMAD	74
A.	CLAIM 10	74
1.	<i>10(pre): A method of storing and generating payment information in an electronic device, the method comprising:</i>	<i>74</i>
2.	<i>10(a): accepting a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information;</i>	<i>75</i>

a)	Toomer's Teachings.....	75
b)	Grigg's Teachings.....	78
c)	Motivation to Combine	79
3.	<i>10(b): wherein the electronic device comprises device-specific and user-specific information; and, ...</i>	<i>82</i>
4.	<i>10(c): wherein the issuer provided payment information is communicated wirelessly; and, ...</i>	<i>83</i>
5.	<i>10(d): receiving wirelessly a static device account number payment information for storage on the electronic device;</i>	<i>84</i>
a)	Toomer's Teachings.....	84
b)	Grigg's Teachings.....	85
c)	Motivation to Combine	89
6.	<i>10(e): and wherein.....</i>	<i>94</i>
	<i>at least a portion of the payment information is a limited-use number for limited use by the device, in place of a issuer provided payment information; and, ...</i>	<i>94</i>
7.	<i>10(f): dynamically generating a one-time limited-use number based on at least one of a set of information including: user-identifying information; ... time; merchant; sequence count; payment information; account information; amount; ...; and</i>	<i>95</i>
a)	Toomer's Teachings.....	95
b)	Hammad's Teachings.....	96
c)	Motivation to Combine	97
8.	<i>10(g): using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.</i>	<i>100</i>
B.	CLAIM 11	102
1.	<i>11. The method of claim 10, wherein the electronic device is configured to accept the user input by at least one of a</i>	

	<i>means comprising: a touch sensor array; a touch screen; a keypad; buttons;</i>	<i>102</i>
C.	CLAIM 12	103
1.	<i>12. The method of claim 10, wherein the device-specific information comprises at least one of a set including: device identifiers; device secrets; devices keys; device usage sequence counters; and device account numbers.</i>	<i>103</i>
D.	CLAIM 13	103
1.	<i>13. The method of claim 10, wherein the user-specific information comprises at least one of a set comprising: ... user information; bank accounts; payment information; device account numbers; ... currency amount</i>	<i>103</i>
X.	GROUND 2: CLAIMS 14-17 ARE OBVIOUS OVER TOOMER, GRIGG, HAMMAD, MULLEN '449, AND LIN	104
A.	CLAIM 14	104
1.	<i>14. The method of claim 10, further comprising rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name.</i>	<i>104</i>
a)	Toomer's Teachings.....	104
b)	Mullen '449's Teachings	105
c)	Motivation to Combine	106
B.	CLAIM 15	107
1.	<i>15. The method of claim 14, further comprising accepting a user selection of a payment method type for use in a transaction responsive to a user selection from a list of payment method images rendered the display and using a touch screen interface for the user selection.</i>	<i>107</i>
a)	Toomer's Teachings.....	107
b)	Mullen '449's Teachings	108

c)	Motivation to Combine	108
C.	CLAIM 16	109
1.	<i>16. The method of claim 15, wherein the user selection is a default payment method to be used in transactions.....</i>	<i>109</i>
a)	Toomer's Teachings.....	109
b)	Lin's Teachings.....	109
c)	Motivation to Combine	110
D.	CLAIM 17	111
1.	<i>17. The method of claim 15, wherein the issuer provided payment information is selected from at least one of a set comprising: account number; card number; device account number; ... an account type;</i>	<i>111</i>
XI.	GROUND 3: CLAIMS 1, 4-6, 8-9 ARE OBVIOUS OVER TOOMER, CASEY, GRIGG, AND HAMMAD.....	112
A.	CLAIM 1	112
1.	<i>1(pre): An electronic device comprising:</i>	<i>112</i>
2.	<i>1(a): a near-field communication (NFC) unit;</i>	<i>112</i>
3.	<i>1(b): a touch sensor array;.....</i>	<i>113</i>
4.	<i>1(c): a display;.....</i>	<i>114</i>
5.	<i>1(d): a motion rate detection array;</i>	<i>115</i>
a)	Toomer's Teachings.....	115
b)	Casey's Teachings	115
c)	Motivation to Combine	118
6.	<i>1(e): a memory for storing a user data and a currency amount;</i>	<i>120</i>
7.	<i>1(f): a processor operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory;</i>	<i>121</i>
8.	<i>1(g) a computer readable medium having instructions stored thereon that, responsive to execution by the electronic device, cause the electronic device to perform operations comprising:</i>	<i>122</i>

9.	<i>1(h)-(n):</i>	123
B.	CLAIM 4	124
1.	<i>4. The electronic device of claim 1, wherein the user input comprises one or more of:</i>	124
	<i>an introduction of a transaction-specific identifier;</i>	124
	<i>a confirmation or a denial of an indicated transaction;</i>	
	<i>and</i>	124
	<i>a lock/unlock command determining operation of the electronic device according to an input sequence or a gesture across the plurality of touch sensors.</i>	124
	a) Casey's Teachings	124
	b) Motivation to Combine	125
C.	CLAIM 5	126
1.	<i>5. The electronic device of claim 1, further comprising a sequence counter which generates a sequential parameter when the processor initiates a transaction, wherein the sequential parameter is combined with any of a user information, a transaction identifier, a user secret, and a credit card authority secret and the processor is operable to generate a limited-duration credit card number therefrom.</i>	126
D.	CLAIM 6	128
1.	<i>6. The electronic device of claim 1, wherein the limited-use number has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions.</i>	128
E.	CLAIM 8	128
1.	<i>8. The electronic device of claim 1, wherein the payment transaction comprises a cryptographic hash of the transaction unit, wherein the cryptographic hash is processed and stored in said memory.</i>	128
	a) Hammad's Teachings	128
	b) Motivation to Combine	129
F.	CLAIM 9	129

1. 9. *The electronic device of claim 1, further comprising a USB connector for connection to a standard computing device.* 129

XII. GROUND 4: CLAIM 7 IS OBVIOUS OVER TOOMER, GRIGG, HAMMAD, CASEY, AND LIN.....130

A. CLAIM 7: 130

1. 7. *The electronic device of claim 1, wherein the display enables information to be displayed regarding the limited-use number, the time, a passcode, a sequence code, a currency amount, and other credit card transaction information of the user; a merchant, a bank or a credit card authority.* 130
- a) Toomer and Grigg’s Teachings.....130
- b) Lin’s Teachings.....131
- c) Motivation to Combine 132

XIII. GROUND 5: CLAIMS 1-2 ARE OBVIOUS OVER TOOMER, GRIGG, HAMMAD, AND MULLEN ’760 134

A. CLAIM 1 134

1. 1(*pre*)-(c), (e)-(n): 134
2. 1(d): *a motion rate detection array;* 134
- a) Toomer’s Teachings.....134
- b) Mullen 760’s Teachings.....134
- c) Motivation to Combine 136

B. CLAIM 2 137

1. 2. *The electronic device of claim 1, wherein the motion rate detection array comprises a set of motion rate detection units, wherein the set comprises: a plurality of inductor coils and companion magnetic-field pickup coils; an optical sensor array; and a plurality of accelerometers, and wherein a detected proximity between the electronic device and a second electronic device is determined from at least one of the set of motion rate detection units.* 137
- a) Mullen 760’s Teachings.....138

b)	Motivation to Combine	142
XIV.	GROUND 6: CLAIM 3 IS OBVIOUS OVER TOOMER, GRIGG, HAMMAD, MULLEN '760, AND GRIFFIN	143
A.	CLAIM 3	143
1.	3. <i>The electronic device of claim 2, wherein the plurality of accelerometers generate an indication of the detected proximity in response to a contact between said electronic device and said second electronic device.</i>	<i>143</i>
a)	Griffin's Teachings	144
b)	Motivation to Combine	145
XV.	CONCLUSION.....	145

CLAIM LISTING

1 (pre). An electronic device comprising:

1(a): a near-field communication (NFC) unit;

1(b): a touch sensor array;

1(c): a display;

1(d): a motion rate detection array;

1(e): a memory for storing a user data and a currency amount;

1(f): a processor operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory;

1(g): a computer readable medium having instructions stored thereon that, responsive to execution by the electronic device, cause the electronic device to perform operations comprising:

1(h): accepting a user input of issued payments information input at a touch screen display of the electronic device, wherein the information comprising an issuer provided payment information;

1(i): wherein the memory comprises device-specific and user-specific information; and,

1(j): wherein the user provided payment information is communicated wirelessly; and,

1(k): wirelessly receiving a static device account number payment information for storage on the electronic device; and

1(l): wherein at least a portion of the payment information is a limited-use number for limited-use by the device, in place of a issuer provided payment information; and,

1(m): dynamically-generating a one-time limited-use numbers based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information; and

1(n): using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.

2. The electronic device of claim 1, wherein the motion rate detection array comprises a set of motion rate detection units, wherein the set comprises: a plurality of inductor coils and companion magnetic-field pickup coils; an optical sensor array; and a plurality of accelerometers, and wherein a detected proximity between the electronic device and a second electronic device is determined from at least one of the set of motion rate detection units.

3. The electronic device of claim 2, wherein the plurality of accelerometers generate an indication of the detected proximity in response to a contact between said electronic device and said second electronic device.

4. The electronic device of claim 1, wherein the user input comprises one or more of:

an introduction of a transaction-specific identifier;

a confirmation or a denial of an indicated transaction; and

a lock/unlock command determining operation of the electronic device according to an input sequence or a gesture across the plurality of touch sensors.

5. The electronic device of claim 1, further comprising a sequence counter which generates a sequential parameter when the processor initiates a transaction, wherein the sequential parameter is combined with any of a user information, a transaction identifier, a user secret, and a credit card authority secret and the processor is operable to generate a limited-duration credit card number therefrom.

6. The electronic device of claim 1, wherein the limited-use number has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions.

7. The electronic device of claim 1, wherein the display enables information to be displayed regarding the limited-use number, the time, a passcode, a sequence

code, a currency amount, and other credit card transaction information of the user, a merchant, a bank or a credit card authority.

8. The electronic device of claim 1, wherein the payment transaction comprises a cryptographic hash of the transaction unit, wherein the cryptographic hash is processed and stored in said memory.

9. The electronic device of claim 1, further comprising a USB connector for connection to a standard computing device.

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

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

10(b): wherein the electronic device comprises device-specific and user-specific information; and,

10(c): wherein the issuer provided payment information is communicated wirelessly; and,

10(d): receiving wirelessly a static device account number payment information for storage on the electronic device; and wherein

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

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

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

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

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

13. The method of claim 10, wherein the user-specific information comprises at least one of a set comprising: an email address; a username; a password; a PIN; a passcode; gestures; user information; bank accounts; payment information; device account numbers; merchant accounts; online accounts; currency amount; currency

type; cryptocurrency address; cryptocurrency keys; private/public keys; signature information; and user secrets.

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

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

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

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

cryptocurrency address; cryptocurrency key; cryptocurrency network; and card-type information.

I, Dr. Clifford Neuman declare the following:

I. INTRODUCTION

1. I have been retained by counsel for Petitioners as a technical expert in the above-captioned case. Specifically, I have been asked to render certain opinions regarding the IPR petition with respect to U.S. Patent No. 10,339,520 (the “’520 Patent”). I understand that the Challenged Claims are 1-17 in the Petition, 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. 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. 10,339,520 (“520 Patent”) (EX1001) and the ‘520 Patent’s prosecution history (“520 File History”) (EX1002). My opinions support Apple Inc.’s petition for *Inter Partes* Review, which challenges claims 1-17 of the 520 Patent (“Challenged Claims”). In developing my opinions relating to the ‘520 Patent, I have considered the materials cited or discussed herein, including those listed below.

Exhibit	Description
1001	U.S. Patent No. 11,176,520 (the “’520 Patent”)
1002	File History of the ’520 Patent (“the ’520 File History”)
1004	U.S. Pub. No. 2009/0210308 (“Toomer”)
1005	U.S. Pub. No. 2014/0006276 (“Grigg”)
1006	U.S. Patent No. 7,740,168 (“Hammad”)
1007	U.S. Pub. No. 2012/0290449 (“Mullen ’449”)
1008	U.S. Pub. No. 2010/0082481 (“Lin”)
1009	U.S. Patent No. 8,255,323 (“the ’323 Patent” or “Casey”)
1010	WIPO Publication No. 2009/082760 (“Mullen ’760”)
1011	U.S. Pub. No. 2011/0070826 (“Griffin”)

11. I have considered these materials from the viewpoint of a POSITA as of the priority date of the ’520 Patent. For the purposes of this declaration, I apply the priority date of the ’520 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 ’520 Patent, unless expressly stated otherwise. To the extent that I use any verb tense in this declaration that is present tense (e.g., “a POSITA would understand” instead of “a POSITA would have understood”), such verb tense should be understood to be my opinion as of the ’520 Patent’s priority date (again, unless expressly stated otherwise). I merely use the present verb tense for ease of reading.

III. OVERVIEW AND LEGAL STANDARDS

12. In formulating my opinions, I have been instructed to apply certain legal standards. I am not a lawyer. I do not offer any testimony regarding what the law is. Instead, the following sections summarize the law as I have been instructed to apply it in formulating and rendering my opinions found later in this declaration.

I understand that, in an *inter partes* review (“IPR”) proceeding, patent claims may be deemed unpatentable if it is shown that they are anticipated or rendered obvious in view of the prior art. I understand that prior art in an IPR review is limited to patents or printed publications that predate the priority date of the patent at issue. I understand that questions of claim clarity (definiteness) and enablement cannot be considered as a ground for considering the patentability of a claim in these proceedings.

A. Person of Ordinary Skill in the Art

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

14. I understand that a person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors above. The hypothetical person is presumed to have the same level of

skill as the typical practitioner of the art and is presumed to have knowledge of all prior art in the relevant field. I understand that the inventor's actual knowledge or lack of knowledge of prior art reference is irrelevant to the obviousness determination.

B. Obviousness

15. I understand that a claim may be invalid under 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been "obvious" to a POSITA in view of a single or combination of prior art references at the time the claimed invention was made. I further understand that a POSITA is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent-in-suit and all analogous prior art. I understand that obviousness in an IPR review proceeding is evaluated using a preponderance of the evidence standard, which means that the claims must be more likely obvious than nonobvious.

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

obviousness analysis must focus on the state of the art at the time of the invention to avoid impermissibly using hindsight to invalidate a patent.

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

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

range of documents a POSITA would have consulted to address the type of problems described in the Challenged Claims.

19. I have been informed that to establish that a claimed invention was obvious based on a combination of prior art elements, an articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I have been informed that the prior art, either as a single reference or a combination of multiple items of prior art, renders a patent claim obvious when there was an apparent reason for a POSITA, at the time of the invention, to combine or modify the prior art. Rationales for combining or modifying the prior art include, but are not limited to, any of the following: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that

would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

20. I have also been informed that where there is a motivation to combine, claims may be rejected as obvious provided a POSITA would have had a reasonable expectation of success regarding the proposed combination. I have also been informed that common sense may be considered. Common sense teaches that familiar items may have obvious uses beyond their primary purposes. I have been informed that if the combination was obvious to try (regardless of whether it was actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than non-obvious innovation.

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

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

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

24. I have been further informed that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be based on prior art features.

The establishment of a nexus is a question of fact. While I understand that Patent Owner here has not offered any secondary considerations at this time, I will supplement my opinions should Patent Owner raise secondary considerations during the course of this proceeding.

C. Claim Construction

25. I understand that the claim terms in an IPR proceeding are construed according to their plain and ordinary meaning as understood in light of the claim language, the patent's description, and the prosecution history viewed from the perspective of a POSITA. I further understand that where a patent defines claim language, the definition of the patent controls, even if there are other definitions that might be understood by those working in the art. I have applied these principles when interpreting the Challenged Claims and in rendering the opinions provided in this declaration.

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

D. Printed Subject Matter

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

IV. LEVEL OF A PERSON OF ORDINARY SKILL

28. Based on my review and analysis of the '520 Patent, the prior art cited herein, and the ordinary skill factors described in this section, a POSITA in the field of the '520 Patent at the time of the earliest possible priority date, March 15, 2013, would have been knowledgeable 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 a similar technical field, and one or two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless and online technologies. Additional industry experience or technical training may offset less formal education, while advanced degrees or additional formal education may offset lesser levels of industry experience. When I refer to the understanding of a POSITA, I am referring to the understanding of such a person as of March 15, 2013.

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

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

V. OVERVIEW OF THE '520 PATENT

A. Summary of the '520 Patent

31. The '520 Patent generally describes emulating a standard credit card with a device “capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe ... for the purpose of emulating a standard credit card” for use in financial transactions. *'520 Patent (EX1001)*, Abstract; 2:14-24. The '520 Patent also describes “allow[ing] user control of said device for the purpose of authorizing or controlling use of said device in the application of credit, debit and cash transactions.” *'520 Patent (EX1001)*, 2:20-24. The invention also describes “generating a limited-duration credit card number when performing a transaction.” *'520 Patent (EX1001)*, 2:24-29. This limited-duration number “is limited in scope to a predetermined number of authorized transactions.” *'520 Patent (EX1001)*, 2:26-29. The electronic device is capable of using near field communications (“NFC”) to conduct a transaction using the limited-duration number. *'520 Patent (EX1001)*, 2:32-62.

32. “The credit card device comprises a realtime clock that is able to produce a cryptographically protected timestamp for each interaction.” *'520 Patent (EX1001)*, 10:7-9. “The power source is able to activate the processor unit such that

a unique number may be generated by the credit card device and verified by the credit authority according to the timestamp and the transmitted user information.”

'520 Patent (EX1001), 10:9-13. “The limited duration credit card number is able to be produced at the time the credit card device is performing a transaction, and is able to be generated according to the user’s private information, a bank information, information regarding the facility performing the transaction, and the time of day.”

'520 Patent (EX1001), 10:13-18. Further, the “limited-duration credit card number is able to be limited to only one transaction, a finite number of transactions, or may be limited to a specified period of time—e.g., 2 minutes, 10 minutes, 3 hours—after which time that particular limited-duration number would become invalid.” *'520 Patent (EX1001)*, 10:18-23. In some cases, the disclosed credit card device is used to conduct transactions with an automated teller machine (ATM). *'520 Patent (EX1001)*, 11:16-26, 12:44-53, 14:59-60.

B. Field of Endeavor

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

34. The *'520 Patent* expressly defines the field of invention, and notes that embodiments “generally relate to electronic or smart credit card devices and, more

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

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

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

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

37. The *'520 Patent* notes that a concern with “credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise” and therefore they “have security limitations.” *'520 Patent (EX1001)*, 1:63-67. The *'520 Patent* also noted that “cards employing smart integrated circuit chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still

predominantly supports conventional plastic credit cards.” *’520 Patent (EX1001)*, 1:67-2:4. To solve these problems, the “Summary of the Invention” describes “multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe” for the “purpose of emulating a standard credit card.” *’520 Patent (EX1001)*, 2:14-18. The “Summary of the Invention” further describes a method of performing a transaction that includes “generating a limited duration credit card number, which is limited in scope of use to a predetermined number of authorized transactions.” *’520 Patent (EX1001)*, 2:25-29. Thus, a POSITA would understand that the *’520 Patent* is directed to solving the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

D. The Prosecution History of the *’520 Patent*

38. I have reviewed the prosecution history for the *’520 Patent*. Notably, there were no substantive rejections based on prior art at any point during the review of the application that issued as the *’520 Patent*. *See generally ’520 File History (EX1002)*. The only rejection that was made was based on statutory double patenting. *’520 File History (EX1002)*, 69. The applicant responded to the rejection by amending independent claim 1 and adding new claims 10-24. *’520 File History (EX1002)*, 107-121. No further rejections were issued and a Notice of Allowance then issued. In the Notice of Allowance, the examiner noted that available prior art

reference, Sebastian et al. (US 2013/0297509) taught a mobile payment using a dynamic code. *'520 File History (EX1002)*, Notice of Allowability. However, the Examiner noted none of the prior art teaches the limitations required by the claims of the application that issued as the *'520 Patent. '520 File History (EX1002)*, Notice of Allowability. A corrected Notice of Allowance was later filed indicating an Examiner's Amendment provided an amendment to claim 2 and 3 indicating the detected proximity was "between the electronic device and a second electronic device." *'520 File History (EX1002)*, Corrected Notice of Allowance. Other minor amendments were made to claims 4 and 8 for clarity. *'520 File History (EX1002)*. The Examiner's reasons for allowance remained the same as the original reason for allowance. Nothing in the file history indicates the art set forth in the petition was located or analyzed by the Examiner.

VI. BACKGROUND OF TECHNOLOGY

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

processors (including Mastercard and Visa) years before the earliest filing date of the '520 Patent.

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

41. The evolution of electronic payment systems can be traced back several decades, marked by key technological milestones that have transformed how financial transactions are processed. Early developments in this field centered on introducing magnetic stripe technology for payment card transactions. Before the late 1960s, credit card transactions primarily consisted of “a tiny printing press to record raised letters and numbers from a card onto a form made of pressure-sensitive paper with carbon copies.” *IBM (EX1020)*, 1. However, this process was “insecure, slow, and prone to errors” therefore a need for magnetic stripe cards arose. *IBM (EX1020)*, 1.

A. The Evolution of Payment Cards

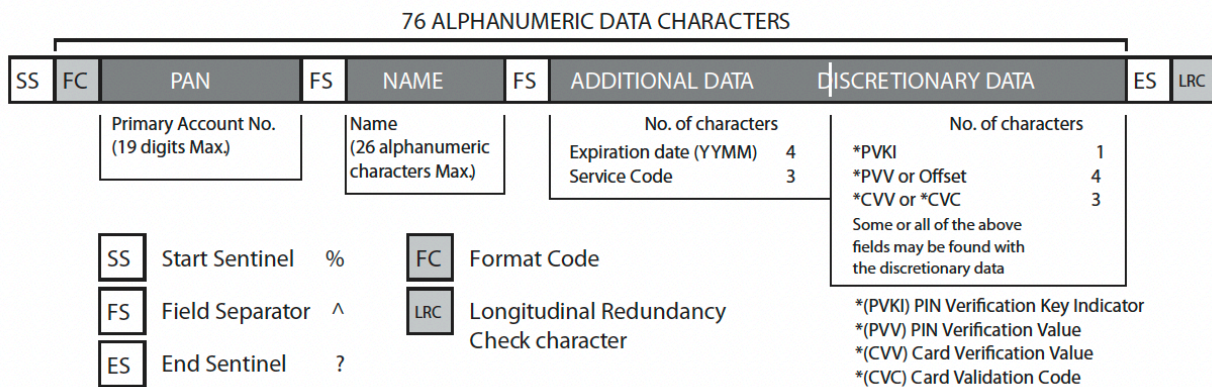
1. Magnetic Stripe Cards

42. In the 1960s, “[t]he process of attaching a magnetic stripe to a plastic card was invented by IBM [.]” *Coskun (EX1021)*, 59. “A magnetic stripe card is one that contains a digital storage space where the data are loaded during the manufacturing phase. The stripe is made up of tiny magnetic particles in a resin. It

is traditionally a read-only item. It is read by physical contact by swiping the card past a device with a magnetic reading head.” *Coskun (EX1021)*, 6.

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

Card Data Format - Track 1

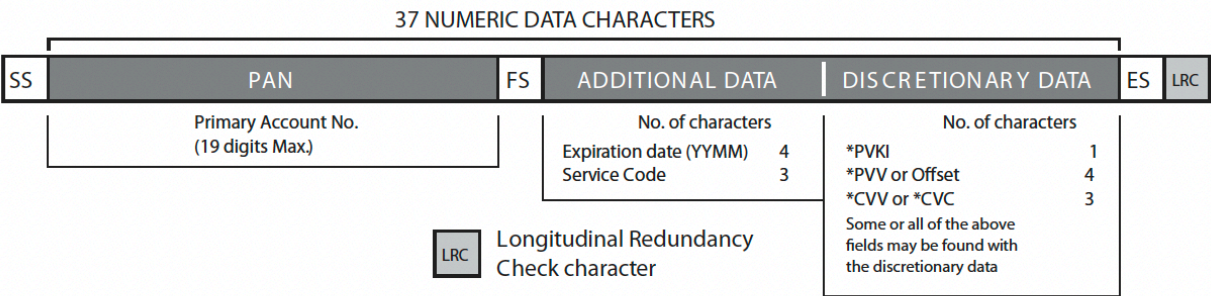


MagTek (EX1022), 1. On a card’s track:

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

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

Card Data Format - Track 2



Magtek (EX1022), 1.

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

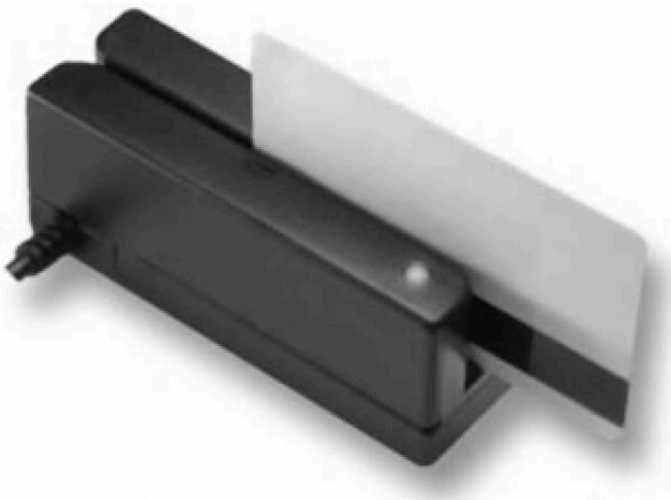


Figure 2.15 Magnetic stripe card.

Coskun (EX1021), Figure 2.15.

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

2. *Smart/Chip Cards*

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

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

for smart cards in order to use them in payments both as a debit and a credit card.”

Coskun (EX1021), 60.

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

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

B. Contactless Payments

1. *Near Field Communications*

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

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

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

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

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

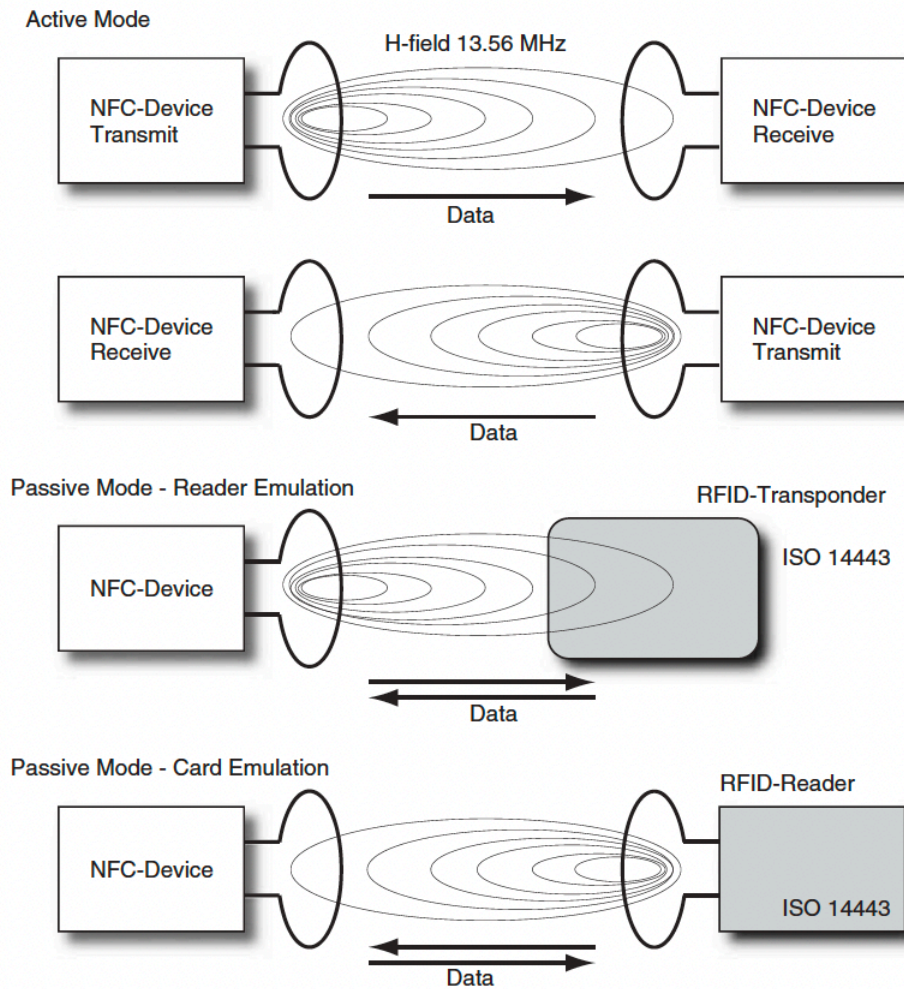


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzeller (EX1024), 58.

2. *Active Mode*

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

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

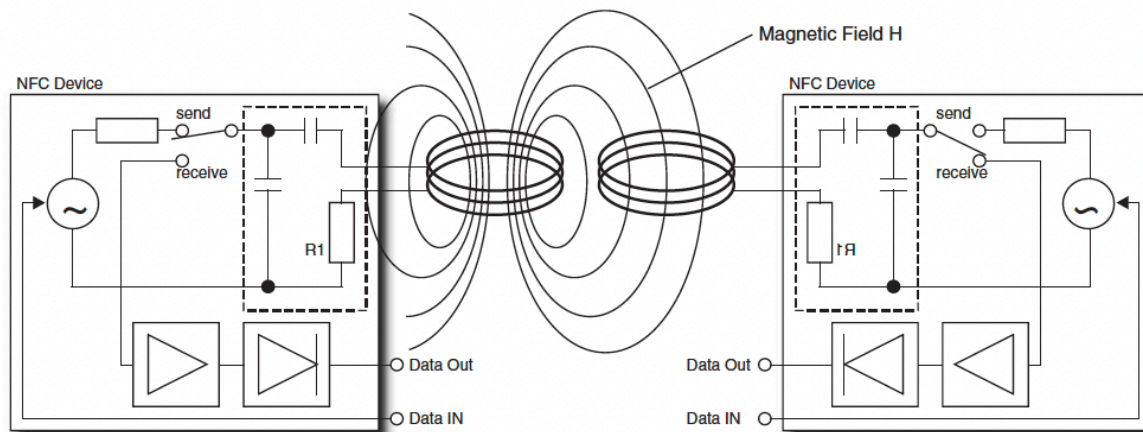


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (EX1024), 58.

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

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

3. *Passive Mode*

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

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

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

C. Contactless EMV Payment Cards

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

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

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

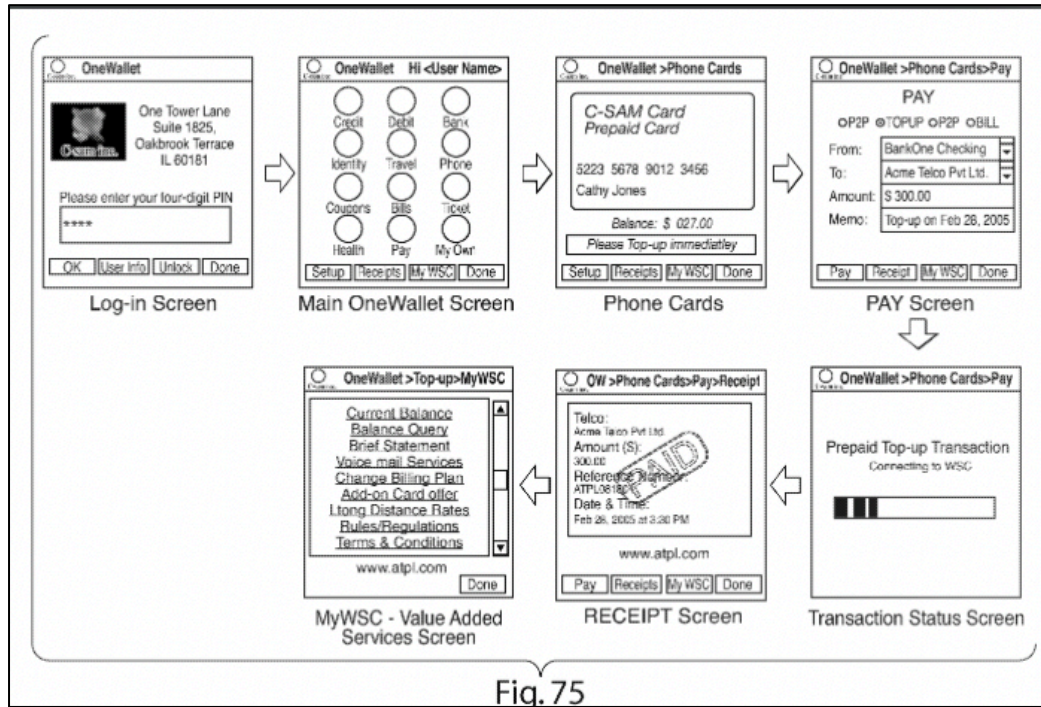
1. Mobile Devices and Mobile Wallets

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

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

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

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



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

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

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



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

Coskun (EX1021), 347.

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

65. By 2012 the use of mobile phones with mobile wallets was well known. For example, MasterCard PayPass Wallet was released. *PayPass (EX1025)*, 1. (“integrate PayPass Wallet into its mobile application.”). MasterCard also released a list of 42 “Approved Mobile Devices”—including phones from Google, Intel, LG,

Asus, HTC, Nokia, BlackBerry, Samsung, Zony, and ZTE—all of which supported at least one mobile payment wallet. *MasterCard Mobile Partner (EX1028)*, 1.

2. Card Emulation Mode

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

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

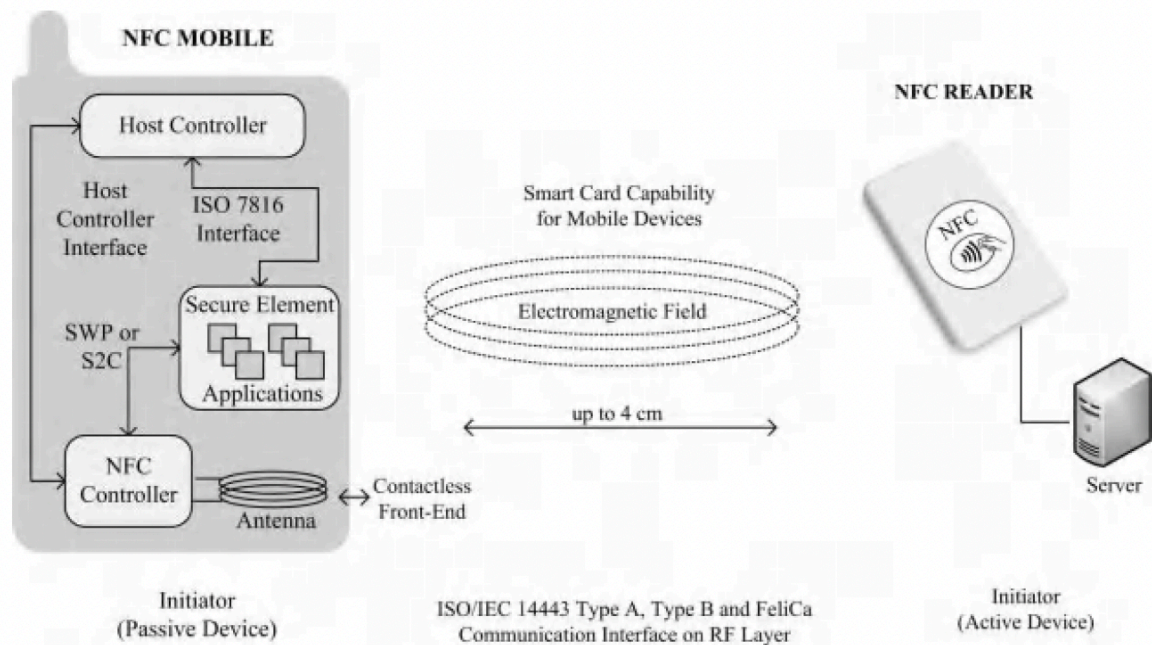


Figure 3.32 Communication architecture of card emulation operating mode.

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

68. In the instance where a phone does not include a secure element, the mobile phone still needs a way to provide a secure and trusted environment for applications. Often, the mobile phone will have a remote-SE located outside of the mobile phone's hardware. As an example, "the NFC mobile device has the ability to use a SE for the transaction that is not physically located in the mobile device. This may be done by creating a data connection to a remote SE for which is used for the payment transaction. In step 757, while the phone is being placed into card emulation mode, the connection to the remote SE that will be used for emulation is attempting to connect. As illustrated in step 758 there is a chance that the connection is already

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

3. *Contactless ATMs*

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

70. In 1988, the National Institute of Standards and Technology issued NIST Special Publication 500-157, entitled “Smart Card Technology: New Methods for Access Control” (“*Smart Card Tech.*”) (EX1035). It discusses uses of magnetic stripe cards and explains the advantages of using smart cards, both contact and contactless, in their place, including in ATMs:

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

Smart Card Tech. (EX1035), 1.

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

Smart Card Tech. (EX1035), 3.

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

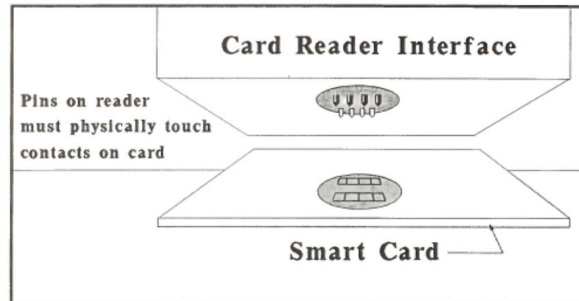


Figure 4. Contact-Type Smart Card Interface

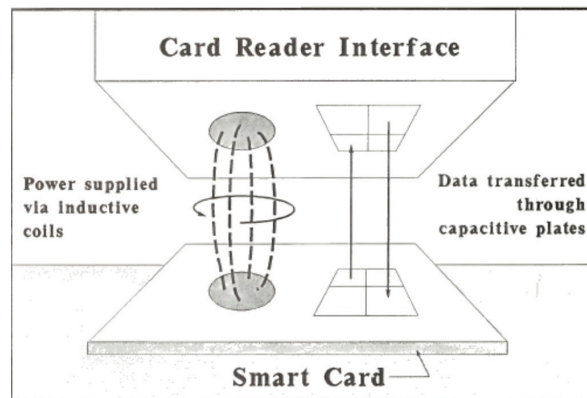
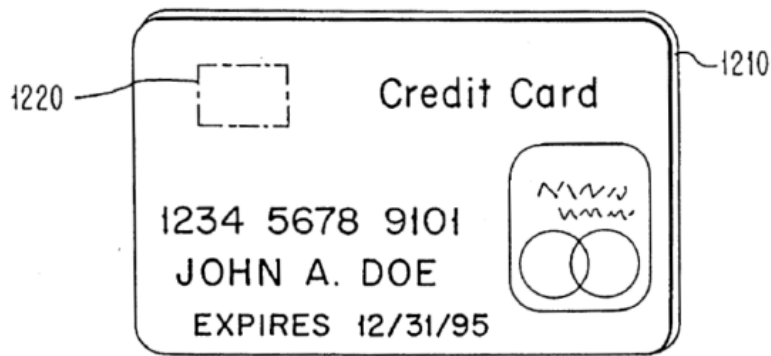


Figure 5. Non-Contact-Type Smart Card Interface

72. On September 9, 1994, Moskowitz et al., assignors to IBM, filed an application that issued as U.S. Patent 5,528,222 on June 18, 1996, entitled “Radio Frequency Circuit and Memory in Thin Flexible Package” (EX1036). It discloses a Radio Frequency Identification (RFID) tag that could be used with an ATM or credit card:



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

73. Not surprisingly, the financial community began to devise uses for contactless cards. In 1995, the Federal Reserve Bank for New York began publishing “Current Issues in Economics and Finance.” The very first article in the first issue was entitled “The Electronic Purse,” by Wenninger et al. (*EX1037*). It describes the choice between contact and contactless cards as a design choice:

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

Wenninger (EX1037), 2.

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

An electronic purse system might work as follows. A bank issues stored value cards to its customers, who then transfer value from their accounts to the cards at an ATM, a personal

computer, or a specially equipped telephone. The electronic purse card might also function as an ATM card or a credit card. When making purchases, customers pass their cards through a vendor's point of sale terminal.

Wenninger (EX1037), 1.

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

76. On April 24, 1995, Kenneth et al. filed an application that issued as U.S. Patent 5,594,233 on January 14, 1997, entitled "Multiple Standard Smart Card Reader" (EX1038). It discloses a card reader that could read all three of magnetic stripe cards, contact smart cards and contactless smart cards, specifically to used at an ATM:

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

Kenneth (EX1038), 1:4-8.

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

Kenneth (EX1038), 1:18-25.

77. Additionally, on April 1, 2003, Douglass, assignor to Diebold, a well-known manufacturer of ATMs, filed a provisional application which, through a

subsequent regular application, became U.S. Patent No. 7,004,385 on February 28, 2006, entitled “Currency Dispensing ATM with RFID Card Reader” (EX1039).

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

Douglass (EX1039), 2:31-42.

78. Additional examples of contactless transactions between a mobile device and an ATM can be found in U.S. Pub. No. 2007/0265984 (Sanantha) (EX1040) and U.S. Pub. No. 2012/0197691 (Grigg) (EX1041). *Sanantha*, [0035]-[0036]; *Grigg*, [0108] (“The external apparatus may generally be a contactless transaction terminal such as a contactless payment terminal, an automated teller machine (ATM), or the like.”), Figs. 1, 7.

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

D. Payment Credential Security Features

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

1. Alternatives to a Payment Account Number (PAN)

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

82. Using these limited-use numbers or tokens in place of the PAN was well-known long before the Critical Date. In fact, in August of 2011, PCI SSC adopted tokenization guidelines. *PCI SSC (EX1031)*, 5. Tokenization replaces “sensitive PAN values with non-sensitive token values.” *PCI SSC (EX1031)*, 5. Non-sensitive means that the number does “not require any security or protection” because “the token has no value to an attacker.” *PCI SSC (EX1031)*, 5. These limited-use tokens are either “single-use or multi-use.” *PCI SSC (EX1031)*, 5. A token can consist of numeric characters, alphabetic characters, or a combination thereof. *PCI SSC (EX1031)*, 5. Using tokens “instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment[.]” *PCI SSC (EX1031)*, 3. PCI SSC also teaches that “[o]ne of the primary goals of tokenization solution should be to replace sensitive PAN values with non-sensitive token values.” *PCI SSC (EX1031)*, 5.

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

500

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

FIG. 5

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

84. As an additional example, Grigg teaches a “mobile wallet account number” that “is a distinct number that is different from any traditional financial institution account number or any other account number associated with a payment device...[that] may be utilized for a transaction for a product.” *Grigg (EX1041)*, [0011]. Grigg teaches that the mobile wallet on the user device 204 will be assigned a “mobile wallet account number” to be used by the user device 204 in place of a traditional account number such as a credit card number (PAN). *Grigg (EX1041)*, [0006], [0047], [0051]. Grigg notes that the payment device or devices are for example, “credit cards” or a “payment device account number (such as a traditional bank account number) [.]” *Grigg (EX1041)*, [0002], [0006]. Grigg notes that each payment device has a “different mobile wallet account number[.]” *Grigg (EX1041)*, [0011], [0003] (“[A] mobile wallet is typically associated with the individual’s mobile device[.]”). In Grigg, the financial institution application “provide[s] the user 202 via the user device 204 the assigned mobile wallet account number.” *Grigg (EX1041)*, [0053]. This mobile wallet number “may be permanently associated with the mobile wallet” *Grigg (EX1041)*, [0051]. “[A] user 202 may use his/her user device 204 as a mobile wallet” to make payments at a point-of-transaction (POT) or online. *Grigg (EX1041)*, [0043].

85. It was well known in the art that replacing a PAN with a different number increases security. For example, an article titled “Security in Mobile

Payments” by Vizzarri et al. (“Vizzarri”) teaches different techniques to guarantee security in m-payment systems. Classical methods are end-to-end encryption and tokenization. With tokenization an encrypted or random value, called token, replaces the card number (PAN) or the magnetic stripe track data in an electronic transaction. The token then becomes the reference number representing the card number, so all tokens can be referenced back to the original card number.” *Vizzarri (EX1032)*, 5.

2. *Alternatives to Static Card Verification Values*

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

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

“can separate the dynamic CVV from credit/debit card data, validate the credit/debit card data, and then merge the CVV with the credit/debit card data once the dynamic CVV is authenticated to produce the transaction authorization.” *Ashfield (EX1033)*, [0005].

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

TABLE 4

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

Yeager (EX1029), Table 4.

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

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

VII. SUMMARY OF UNPATENTABILITY

Ground	Claims	References
1	10-13	Toomer (EX1004), Grigg (EX1005), and Hammad (EX1006)
2	14-17	Toomer, Grigg, Hammad, Mullen ’449 (EX1007), and Lin (EX1008)
3	1, 4-6, 8-9	Toomer, Grigg, Hammad, and Casey (EX1009)
4	7	Toomer, Grigg, Hammad, Casey, and Lin
5	1-2	Toomer, Grigg, Hammad, and Mullen ’760 (EX1010)
6	3	Toomer, Grigg, Hammad, Mullen ’760 , and Griffin (EX1011)

91. 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.

VIII. SUMMARY OF THE PRIOR ART

A. Toomer

92. Toomer describes an “electronic device that can be used to initiate or otherwise participate in a financial transaction.” *Toomer (EX1004)*, [0023]. The electronic device, specifically mobile device 324, is adapted to store and execute a mobile wallet application. *Toomer (EX1004)*, [0024], [0052]. The mobile wallet application stores and maintains electronic payment credentials, that is, information related to financial accounts of a user of the mobile device 324. *Toomer (EX1004)*, [0052], [0063]. The user is able to select her preferred payment credential (e.g., credit card) from those stored in the mobile wallet, and complete a financial transaction at a point-of-sale (“POS”) device. *Toomer (EX1004)*, [0063]. The mobile device 324 communicates with the POS device using wireless technology, such as a near field communications (“NFC”) connection. *Toomer (EX1004)*, [0051]. Thus, the “mobile device 324 may be used in addition to or instead of a card or other token representing an account.” *Toomer (EX1004)*, [0051]; Fig. 4 (illustrating details of a system for processing financial transactions using mobile device 324). A more detailed discussion of Toomer is included below in my analysis of specific claims and claim limitations.

1. Toomer is Analogous

93. In my opinion, Toomer is analogous to the claimed invention of the '520 Patent because it is from the same field of endeavor. First, Toomer, like the '520 Patent, discloses conducting secure payment transactions. *Compare '520 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Toomer (EX1004)*, Abstract, [0001], [0004]-[0008], Fig. 7. Second, *Toomer* is reasonably pertinent to the particular problem with which the inventor of the '520 Patent was involved because it is directed to increasing security of payment transactions. *Compare '520 Patent (EX1001)*, 1:23-28, 1:63–2:4, 9:9-15 *with Toomer (EX1004)*, Abstract, [0004], [0024], [0038].

B. Grigg

94. Grigg generally 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 (EX1005)*, [0011]. 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 (EX1005)*, [0002], [0006]. Grigg notes that each payment device has a “different mobile wallet account number[.]” *Grigg (EX1005)*, [0011], [0003] (“[A] mobile wallet is typically associated with the individual’s mobile device[.]”). In Grigg

(EX1005), the financial institution application “provide[s] the user 202 via the user device 204 the assigned mobile wallet account number.” *Grigg (EX1005)*, [0053]. This mobile wallet number “may be permanently associated with the mobile wallet” *Grigg (EX1005)*, [0051]. A more detailed discussion of Grigg is included below in my analysis of specific claims and claim limitations.

1. *Grigg is Analogous*

95. In my opinion, Grigg is analogous art to the ’520 Patent. First, Grigg is directed to conducting secure payment transactions and, therefore, Grigg is in the same field of endeavor that is expressly defined in the ’520 Patent. *Compare ‘520 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Grigg (EX1005)*, Abstract, [0005]-[0006], Fig. 1. Second, a POSITA would have understood Grigg to be reasonably pertinent to the particular problems with which the inventor of the ’520 Patent was involved because Grigg is directed to increasing security of payment transactions. *Compare ‘520 Patent (EX1001)*, 1:23-28, 1:63-2:4, 9:21-28 *with Grigg (EX1005)*, [0003]-[0004].

C. *Hammad*

96. Hammad generally teaches methods and system for generating verification values on a portable consumer device for use in payment transaction. *Hammad (EX1006)*, 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* (EX1006), 4:21-6:42.

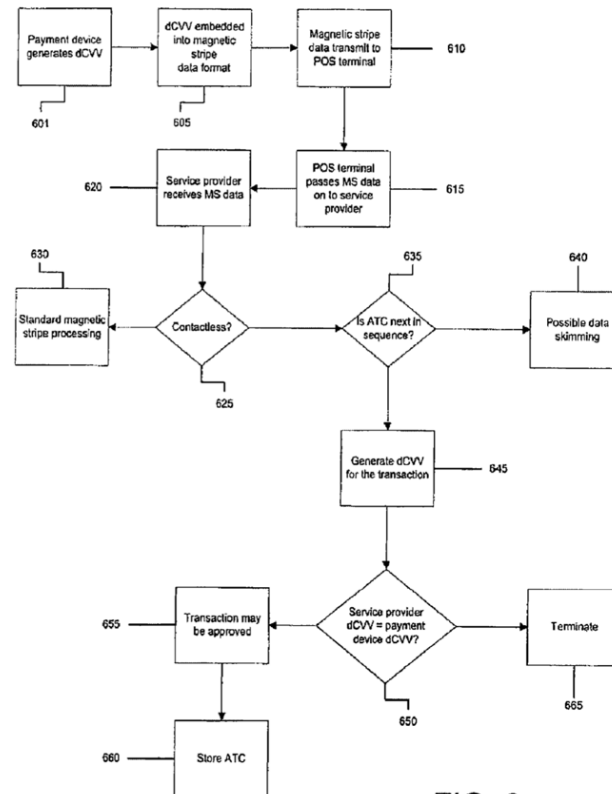


FIG. 6

Hammad (EX1006), Fig. 6.

1. *Hammad* is Analogous

97. *Hammad* is analogous art to the '520 Patent because it is from the same field of endeavor. Like the '520 Patent, *Hammad* relate to conducting secure payment transactions. *See, e.g., Hammad* (EX1006), 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* ’520 Patent (EX1001), Abstract, 1:23-28, Fig. 1 *with Hammad* (EX1006), Abstract, 2:12-20, Fig. 6.

98. Hammad is also reasonably pertinent to at least one problem addressed by the ’520 Patent. Like the ’520 Patent, Hammad is concerned with increasing security of payment transactions. *See, e.g., Hammad* (EX1006), 1:20-23 (“One of the primary sources of fraud, which is prevalent in the credit card industry is skimming. Skimming refers to the electronic copying of a card's magnetic stripe data to create counterfeit cards.”), 1:45-65 (“To address the above problems, a dCVV or a dynamic card verification value can be used. The dCVV can be generated using an algorithm which uses at least a counter and input data such as an account number, expiration date, and other information. The counter can increase by one each time a transaction is conducted. The dCVV can be independently generated by either a portable consumer device or POS terminal at the front end of a transaction and can be sent to a back end computer. The counter may be sent from the merchant to the back end computer so that it knows the current counter value associated with the portable consumer device. In other cases, the counter may simply be present at the back end computer. In the latter case, the counter increments every time the back end computer sees a transaction. The back end computer, using a similar algorithm to

the one that generated the dCVV at the front end, the counter value, and input data, can independently generate a second dCVV. If the received dCVV and the generated dCVV match, the transaction can be considered authentic. If the dCVVs do not match, this may indicate that the transaction is fraudulent.”); *compare* ’520 Patent (EX1001), 1:23-28, 1:63-2:4, 9:9-15 with *Hammad* (EX1006), 1:20-23; 1:45-65.

D. Mullen ’449

99. Mullen ’449 describes a system and method to “generate a mobile wallet of virtual cards” on a mobile device, such as a cell phone, for use in payment transactions. *Mullen* ’449 (EX1007), Abstract, [0003], [0021], [0053]. The mobile device is configured to store information from physical payment cards by communicating with the cards via a contactless communication channel, for example, RFID technology. *Mullen* ’449 (EX1007), [0003]-[0004], [0009]. The virtual cards are also rendered onto a display of the mobile device, the rendering including each card’s particular card and cardholder information. *Mullen* ’449 (EX1007), [0009], [0010], Fig. 11. “In so doing, [each] virtual card may be created within the mobile device that is both visibly and functionally equivalent to its physical counterpart. *Mullen* ’449 (EX1007), [0009]. Thus, a user of a mobile device may convert her entire physical wallet or purse “into a virtual equivalent [] that resides electronically within the mobile device.” *Mullen* ’449.

1. Mullen '449 is Analogous

100. It is my opinion that Mullen '449 is analogous to the claimed invention of the '520 Patent because it is from the same field of endeavor. Mullen '449, like the '520 Patent, discloses conducting secure payment transactions. *Compare '520 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Mullen '449 (EX1007)*, [0003]-[0005]. Second, Mullen '449 is also reasonably pertinent to certain problems addressed by the '520 Patent such as increasing security of payment transactions. *Compare '520 Patent (EX1001)*, 1:23-28, 1:63-2:4, 9:9-15 *with Mullen '449 (EX1007)*, [0008], [0091].

E. Casey

101. Casey describes “[m]ethods and devices for confirming payment transactions” using an electronic device 10 that may be a cellular telephone. *Casey (EX1009)*, Abstract, 3:38, Fig. 1. A user of the electronic device 10 is able to access and select a payment instrument through a touch screen on the electronic device 10, the payment instrument being a digital representation, e.g., of a credit card, stored on an electronic wallet. *Casey (EX1009)*, 3:10-14, 8:34-44. A payment transaction may be confirmed on the electronic device 10 by dragging a graphical element 180 such as a slide bar 182 to a confirmation position 188 on the touch screen 54. *Casey (EX1009)*, 13:39-51; Fig. 5. Alternatively, the electronic device 10 may include a motion sensing device 62 to sense movement of the device in a direction that

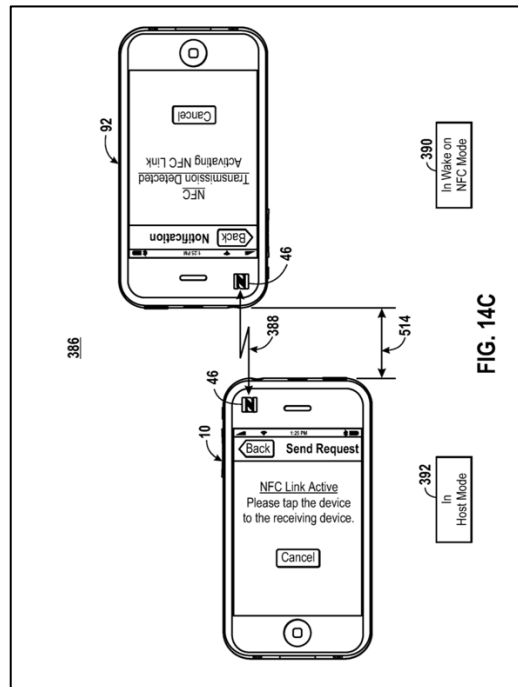
corresponds to confirming (or declining) a transaction. *Casey (EX1009)*, 18:19-67, Figs. 12-13.

1. Casey is Analogous

102. Casey is analogous to the claimed invention of the '520 Patent because it is from the same field of endeavor. Casey, like the '520 Patent, discloses conducting secure payment transactions. *Compare '520 Patent (EX1001)*, Abstract, 1:26-28, Fig. 1 *with Casey (EX1009)*, Abstract, 1:6-9, 3:10-19. Casey is also reasonably pertinent to the particular problem with which the inventor of the '520 Patent was involved because it is directed to increasing security of payment transactions. *Compare '520 Patent (EX1001)*, 1:26-28, 1:63–2:4, 9:9-15 *with Casey (EX1009)*, 3:35-37, 10:35-46, 17:15-38.

F. Lin

103. I understand Lin teaches “the establishment of an NFC connection 388 between two devices, namely the payee device 10 and the payor device 92, by way of the tap operation 386 [.]” *Lin (EX1008)*, 68:10-13.



Lin (EX1008), Fig. 14C.

104. Once “active device 10 is placed within an acceptable distance 514 (e.g., 2-4 cm) from the payor device 92” the devices establish an “NFC connection 388...through which the payment request may be transmitted.” *Lin (EX1008)*, 68:13-25.

1. *Lin is Analogous*

105. *Lin* is analogous art to the '520 Patent because it is from the same field of endeavor because both *Lin* and the '520 Patent are directed towards conducting secure payment transactions. *See, e.g., Lin (EX1008)* at Abstract (“...one or more external financial servers 100 configured to process and determine whether the payment may be authorized.”), 33:2-7 (“Regardless of the type of connection established between the device 10 and the financial servers 100, it should be

understood that one or more of the data encryption techniques and security protocols...may be further utilized in order to facilitate the secure transmission of the transaction data 98 to the financial servers 100.”), 98:7-10 (The smart card server 874 may perform a one or more verification and/or authorization processes...wherein the payor’s smart card account 872 is verified for validity and sufficiency of funds, for example.”). *Compare* ’520 Patent (EX1001), Abstract, 1:23-28, Fig. 1 *with* Lin (EX1008), Abstract, 68:13-25, Fig. 14C.

106. Lin is also reasonably pertinent to at least one problem addressed by the ’520 Patent. Like the ’520 Patent, Lin is concerned with increasing security of payment transactions. *See, e.g.,* Lin (EX1008), 26:26–27:7 (“The security features 74 may be stored in the storage device 54 and may include one or more cryptographic protocols, such as a secure sockets layer (SSL) protocol or a transport layer security (TLS) protocol, for establishing secure communications between the device 10 and an external device. The security features 74 may also include one or more encryption applications for encrypting information sent from the device 10.”); *see also* Lin (EX1008) at 27:8–28:15; *compare* ’520 Patent (EX1001), 1:23-28, 1:63-2:4, 9:9-15 *with* Lin (EX1008), 26:26-28-15.

G. Mullen '760

107. Mullen '760 describes electronic credit cards that generate dynamic information for use in a financial transaction. *Mullen '760 (EX1010)*, [0002]-[0007], [0016], [0198]-[0200].

A credit card is provided that may include a credit card number, where at least a portion of the credit card number changes periodically. A magnetic emulator and/or magnetic stripe encoder may be provided to communicate at least a portion of the information needed to complete a credit card transaction to a credit card reader. A magnetic stripe emulator may communicate data serially and may comprise a coil having a soft-magnetic material as well as a permanent magnet. Dynamic magnetic information may be utilized to provide a variety of credit, debit, gift, and loyalty cards.

Mullen '760 (EX1010), Abstract.

108. The dynamic information may be a dynamic credit card number, verification code, or security number. *Mullen '760 (EX1010)*, [0023], [0033]-[0034], [0231]-[0232], [0261]-[0262]. The “dynamic credit card number may, for example, change based on time or use. A portion of a dynamic credit card number may be static. Accordingly, for example, the credit card number may change but particular digits of the dynamic credit card number may remain constant. For example, a dynamic credit card number may be provided such that the beginning one or more digits (e.g., first six digits) are static.” *Mullen '760 (EX1010)*, [0003]-[0004]. The

magnetic emulator “include one or more wires that are able to produce an electromagnetic field that is operable to be read by, for example, a magnetic stripe reader.” *Mullen '760 (EX1010)*, [0007]. The “emulator may be utilized, for example, to communicate a dynamic credit card number or a portion of a dynamic credit card number to a credit card reader.” *Mullen '760 (EX1010)*, [0214], [0295], [0305]. A remote server verifies the payment information, including the dynamic information. *Mullen '760 (EX1010)*, [0231]-[0232], [0261]-[0262], [0292].

1. Mullen '760 is Analogous

109. Mullen '760 is analogous to the claimed invention of the '520 Patent because it is from the same field of endeavor. Mullen '760, like the '520 Patent (EX1001), relates to secure payment transactions. *Compare '520 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Mullen '760 (EX1010)*, Abstract, [0002]-[0005], [0016], [0021]-[0034], Figs. 1, 6-7.

110. Mullen '760 is also reasonably pertinent to the particular problem with which the inventor of the '520 Patent was involved because it is directed to increasing security of payment transactions. *Compare '520 Patent (EX1001)*, 1:23-28, 1:63-2:4, 9:9-15 *with Mullen '760 (EX1010)*, [0210], [0299].

H. Griffin

111. Griffin describes “mobile wireless communications devices and related methods that use Near Field Communications (NFC).” *Griffin (EX1011)*, [0001].

The use of NFC “enable[s] communication between electronic devices, including mobile wireless communications devices.” *Griffin (EX1011)*, [0003], Fig. 1. The short range communications include “payment.” *Griffin (EX1011)*, [0001], [0003]. When an NFC connection is established between two devices, data, such as security codes, IDs or PINs, are exchanged. *Griffin (EX1011)*, [0023], [0039]. This device-to-device communication allows a user to “share data content with another communications device in an easy and secure manner.” *Griffin (EX1011)*, [0037].

1. Griffin is Analogous

112. Griffin is analogous to the claimed invention of the ’520 Patent because it is from the same field of endeavor. Griffin, like the ’520 Patent, relates to secure payment transactions. *Compare ’520 Patent (EX1001)*, Abstract, 1:23-28, Fig. 1 *with Griffin (EX1011)*, Abstract, [0001], [0003] (describing NFC transactions between electronic devices (e.g., mobile wireless devices) including for “payment”), [0037].

113. Griffin is also reasonably pertinent to the particular problem with which the inventor of the ’520 Patent was involved because it is directed to secure transactions involving two devices. *Compare ’520 Patent (EX1001)*, 1:23-28, 1:63–2:4, 9:9-15 *with Griffin (EX1011)*, [0003], [0037] (“the device-to-device communication allows a user of a portable wireless communications device 20 as

illustrated to share media or data content with another communications device 22 in an easy and secure manner”).

IX. GROUND 1: CLAIMS 10-13 ARE OBVIOUS OVER TOOMER, GRIGG, AND HAMMAD

A. Claim 10

1. 10(pre): A method of storing and generating payment information in an electronic device, the method comprising:

114. Toomer describes methods and systems for “authorizing financial transactions initiated by or otherwise involving the use of a contactless or mobile device.” *Toomer (EX1004)*, [0019], [0038]. Toomer describes its systems as “electronic device that can be used to initiate or otherwise participate in a financial transaction.” *Toomer (EX1004)*, [0023]. The electronic device, specifically mobile device 324, is adapted to store and execute a mobile wallet application. *Toomer (EX1004)*, [0024], [0052]. The mobile device of Toomer is described as “any small, likely handheld, electronic device that can be used to initiate or otherwise participate in a financial transaction,” which “can include, but is not limited to, a cellular telephone, a Personal Digital Assistant (PDA), a smart card or other contactless device, etc.” *Toomer (EX1004)*, [0023]. The mobile wallet application of Toomer stores and maintains electronic payment credentials, that is, information related to financial accounts of a user of the mobile device 324. *Toomer (EX1004)*, [0052], [0063]. The user is able to select her preferred payment credential (e.g., credit card)

from those stored in the mobile wallet, and complete a financial transaction at a point-of-sale (“POS”) device. *Toomer (EX1004)*, [0063]. The mobile device 324 communicates with the POS device using wireless technology, such as a near field communications (“NFC”) connection. *Toomer (EX1004)*, [0051]. When communicating, the mobile wallet application “may **store or generate** a unique identifier for use by other systems in identifying one or more accounts associated with the mobile wallet.” *Toomer (EX1004)*, [0038], [0059]. Thus, the “mobile device 324 may be used in addition to or instead of a card or other token representing an account.” *Toomer (EX1004)*, [0051], Fig. 4 (illustrating details of a system for processing financial transactions using mobile device 324). Toomer’s mobile device, therefore, performs a method of storing and generating payment information in an electronic device.

2. ***10(a): accepting a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information;***

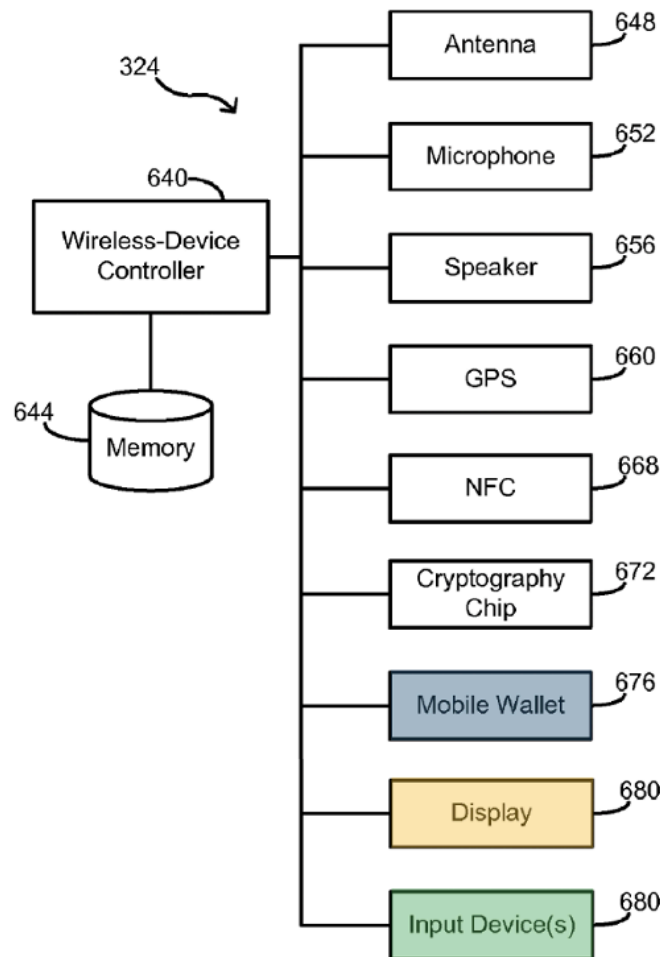
a) *Toomer’s Teachings*

115. As mentioned in Claim 10(pre), Toomer’s mobile wallet application 676 “can be adapted to store payment vehicle information, i.e., an electronic payment credential and/or other information identifying one or more financial accounts such as credit accounts, debit accounts, demand deposit accounts, stored value accounts, etc.” *Toomer (EX1004)*, [0063]. The described “payment vehicle” is

simply payment information, such as a “credit, debit, stored-value” or other account.

Toomer (EX1004), [0027]. “[T]he **mobile wallet 676** can allow storage of multiple payment vehicles and can provide a user interface that can be displayed on a **screen or display device 680** and through which the user can select a specific payment vehicle by manipulating a keypad, wheel, **touch screen**, or other input device **682**.”

Toomer (EX1004), [0063], Fig. 6. Toomer teaches that “accounts represented by information stored in such electronic devices” may be “manually entered by a user of the device.” *Toomer (EX1004)*, [0003].



Toomer (EX1004), Fig. 6 (contains a typographical error, as “Input Device(s)” should have reference number “682”).

116. Toomer describes a system for “securely authorizing a financial transaction utilizing an electronic payment credential.” *Toomer (EX1004)*, [0038]. A “payment credential” includes “information representing an account[,],” such as a bank name, account number, account type, etc[,],” that can be maintained in the device and/or accessible by a mobile wallet.” *Toomer (EX1004)*, [0038], [0053] (“The credential of other information regarding the selected account can identify the account to be used in supporting transactions, for example, including an indication of the financial institution 316 where that account is maintained, an account number, etc. Such identifications may conveniently be made with numerical strings similar to card numbers that have portions that identify a financial institution and portions that identify specific accounts. Additional information may include ownership details of the account, current balance levels for the account, and the like.”).

117. A POSITA would have understood that in order for account information, such as an account number, to be maintained by Toomer’s mobile device, it would first need to be input to the device. Toomer recognizes that “accounts represented by information stored in such electronic devices” may be “manually entered by a user of the device.” *Toomer (EX1004)*, [0003]. Based on Toomer’s teaching that a user selects a payment vehicle using a touch screen, a

POSITA would have found it obvious to also configure the touchscreen to accept the account information to be stored thereon. Thus, Toomer teaches or renders obvious that its mobile wallet application allows a user to use a touch screen display of the electronic device to input and select a payment vehicle, the payment vehicle information comprising issuer provided payment information.

b) Grigg's Teachings

118. Similar to Toomer, Grigg teaches a user device having a mobile wallet application thereon. *Grigg (EX1005)*, [0005], [0070], Fig. 2. A “user device” can be “any mobile communication device, such as a ... a cell phone or mobile phone” or a “smartphone.” *Grigg (EX1005)*, [0070], [0062] describing a “smartphone” as “means that a user 202 may use to perform a transaction with a[] merchant”). A POSITA would have understood that most smartphones in 2012 when Grigg was filed, such as iPhones and Android devices, included a touchscreen. *See e.g., Lin (EX1008)* (describing iPhone with touchscreen for use in a financial transaction). The mobile wallet application on the user device stores a “mobile wallet account number” and payment device account numbers in memory on the device. *Grigg (EX1005)*, [0029], [0073] (“the user application 222 may store the mobile wallet account number in the memory device 216”), Fig. 2.

119. The mobile wallet application allows a user to “manually input [] payment devices into his/her mobile wallet.” *Grigg (EX1005)*, [0008]. For example,

“the user 202 may provide the financial institution application 258 with information associated with a mobile wallet, including ... adding payment devices to the mobile wallet ... and the like. This information may be provided from the user 202 by manual input and/or may be automatically provided.” *Grigg (EX1005)*, [0048]; *see also*, [0072] (“The user application 222 may allow a user 202 to add payment devices to his/her mobile wallet.”), [0078]-[0079], [0087] (“If the user 202 does activate his/her mobile wallet at decision block 402, the user 202 may input payment devices onto his/her mobile wallet, as illustrated in block 404.”). A “payment device” includes “any means of payment for a product of a transaction[,]” such as “a credit card, debit card, [etc.]” *Grigg (EX1005)*, [0029], [0079] (“The payment device accounts may include one or more of credit card numbers, debit account numbers, [etc.]”). A POSITA would understand that a credit card number (i.e., payment device) input by the user to the mobile wallet on the user’s device, e.g., a smartphone with a touchscreen, is issuer provided payment information.

c) Motivation to Combine

120. A POSITA would have found it obvious and been motivated to modify Toomer’s mobile device to permit a user to input payment information, e.g., account numbers, into the mobile wallet application, as taught by Grigg, using the touch screen display. Toomer even describes such manual entry of payment information into an electronic device. *Toomer (EX1004)*, [0003]. A POSITA would have

understood that Toomer's mobile wallet application would have to be initialized with desired payment information before allowing a user to perform payment transactions using the mobile device. A POSITA would have further found it obvious to allow for adding payment devices to Toomer's wallet application through the touchscreen. A POSITA would have understood that initializing the mobile wallet application, or adding payment accounts to the application, directly on the mobile device to be used would be more efficient and convenient than initializing via an indirect means, such as a desktop computer. This convenience would have been desirable to users and motivated a POSITA to utilize such a feature.

121. Moreover, touchscreen input was well-known and predictable long before the '520 Patent, including for adding financial accounts to an application through which financial transactions are conducted. For example, Lin describes a mobile device, such as an iPhone, having a transaction application for conducting financial transactions via NFC. *Lin (EX1008)*, Abstract, 14:22-15:9, 30:3-31:4, Figs. 4, 11A-B, 12A-C. A user can add different financial accounts to the phone through user inputs to the touchscreen interface. *Lin (EX1008)*, 38:17-43:22, Figs. 5A-B. As an additional example, U.S. Publn. No. 2009/0307132 to Phillips (assigned to MasterCard) (EX1044), describes a mobile phone having a virtual wallet with stored payment account numbers for use in a transaction with a proximity reader (e.g., NFC). *Phillips (EX1044)*, Abstract, [0012], [0025]-[0027], [0029]-[0032], [0042],

Figs. 2A, 4. The virtual wallet allows a user to “Add New Card[,]” “whereby a new payment card is added to the account.” *Phillips (EX1044)*, [0036], Fig. 4 (item 412). This option can be selected through “a touch screen, and selection of a menu item may be accomplished by the user touching the display with his/her finger or a stylus at the location of the menu item to be selected.” *Phillips (EX1044)*, [0045]. Therefore, a POSITA would have been well-aware and motivated to combine well-known prior art elements according to known methods to yield the predictable result of allowing the user to add desired payment vehicles using the mobile device’s mobile wallet application through Toomer’s touchscreen display.

122. A POSITA would have had a reasonable expectation of success in making the proposed combination. Because a mobile wallet and touchscreen input were both well-known and conventional prior to the ’520 Patent, there would have been a reasonable expectation of success in using a touch screen as a user input element in Toomer’s mobile device to add payment accounts for selection to use in a transaction. Indeed, Toomer already teaches providing input to select a payment vehicle through a touchscreen. *Toomer (EX1004)*, [0063], Fig. 6. Thus, modifying Toomer with the teachings of Grigg, to allow user input of issuer provided payment information is simply a combination of known elements that would yield predictable results.

123. In combination, Toomer's mobile device is modified to accept a user input of issued payment information at a touchscreen display of the mobile device, wherein the payment information in both Toomer and Grigg comprises issuer provided payment information.

3. 10(b): wherein the electronic device comprises device-specific and user-specific information; and,

124. Toomer teaches that the mobile wallet application maintains "account numbers and/or other information, i.e., electronic payment credentials, related to one or more financial accounts." *Toomer (EX1004)*, [0052]; *see also*, [0024], [0038], [0063].

125. The mobile device 324 includes a memory storing a unique static identifier. *Toomer (EX1004)*, [0005], [0007], [0059]. The unique static identifier is "information identifying the electronic device presenting the payment credential," e.g., "a device serial number for the mobile electronic device." *Toomer (EX1004)*, [0059]. Dependent claim 12 of the '520 Patent describes "device-specific information" as including "device identifiers[.]" *'520 Patent (EX1001)*, 17:41-43.

126. Toomer also teaches that the mobile device memory stores the payment vehicle information utilized by mobile wallet application. *Toomer (EX1004)*, [0024], [0027], [0063]. Payment vehicle information includes "information identifying one or more financial accounts such as credit accounts [or] debit accounts." *Toomer (EX1004)*, [0063]. Toomer also teaches mobile device 324 storing "information such

as a bank name, account number, account type, etc.” *Toomer (EX1004)*, [0038], [0053]. Dependent claim 13 of the ’520 Patent describes that “user-specific information comprises at least one of a set comprising: [. . .] **bank accounts; payment information**[.]” *’520 Patent (EX1001)*, 17:45-49. A POSITA would have understood that a debit account is a type of *bank account*, and that information relating to credit, debit, stored-value accounts is *payment information*. Therefore, Toomer’s teaches *user-specific information*.

4. 10(c): wherein the issuer provided payment information is communicated wirelessly; and,

127. Toomer teaches mobile device 324 being a cellular phone capable of “a cellular or other wireless communications service.” *Toomer (EX1004)*, [0022]-[0023]. Toomer’s system includes one or more user computers, such as “servers ... to execute a plurality of processes related to financial transactions of one or more consumers on behalf of one or more client financial institutions.” *Toomer (EX1004)*, [0040]. The system also includes one or more computers “operated by a ... consumer” including “Internet-enabled mobile telephone, and/or personal digital assistant, capable of communicating via a network [115].” *Toomer (EX1004)*, [0042]. The network 115 includes a “wireless network.” *Toomer (EX1004)*, [0041].

128. Grigg’s also describes that its mobile device is a wireless device such as a cellular or smart phone that communicates with the financial institution server, and other devices, over a wireless network. *Grigg*, [0040], [0042], [0069], [0072],

Fig. 2. In Grigg, a user “input[s] payment devices onto his/her mobile wallet” (issuer provided payment information), which are then transmitted to the financial institution server. *Grigg (EX1005)*, [0087]. Grigg’s “user application [] may allow a user [] to add payment devices to his/her mobile wallet” by “communicate the information associated with the added payment device ... through a network 201 to the financial institution server 208.” *Grigg (EX1005)*, [0072]. The network 201 is a “wireless” connection “between devices on the network,” e.g., the user device and financial institution server. *Grigg (EX1005)*, [0042], Fig. 2.

129. As discussed in Claim 10(a), it would have been obvious to a POSITA to configure Toomer’s mobile device to implement Grigg’s method of initializing and adding payment devices to a mobile wallet through wireless communications. See Claim 10(a). This includes wirelessly communicating the issuer provided payment information.

5. ***10(d): receiving wirelessly a static device account number payment information for storage on the electronic device;***

a) *Toomer’s Teachings*

130. Toomer describes the use of either “a **unique static identifier**” or “a unique dynamic identifier” as “information identifying the electronic device presenting the payment credential[.]” *Toomer (EX1004)*, [0005], [0007], [0059]. When a dynamic identifier is used, an acquirer system 312 can “save the unique device identifier in the information identifying the account 410 or 411, and transfer

the unique device identifier to the electronic device 324.” *Toomer (EX1004)*, [0059]. Because the acquirer system is a processing entity remote from mobile device, and mobile device 324 communicates via “a cellular or other wireless communications service,” or other wireless networks, mobile device receives the unique device identifier wirelessly. *Toomer (EX1004)*, [0021]-[0023].

131. Toomer further teaches storing the unique device identifier and payment credentials, such as the account number or “unique identifier for use by other systems in identifying one or more accounts associated with the mobile wallet,” on the mobile device. *Toomer (EX1004)*, [0038], [0052]-[0053], [0063].

b) Grigg’s Teachings

132. As discussed in Claim 10(c), Grigg teaches that a user device and financial institution server communicate over wireless connections. *See Claim 10(c); Grigg (EX1005)*, [0042].

133. Grigg teaches that the mobile wallet on the user device will be assigned a “mobile wallet account number” (device account number) to be used by the user device in place of a traditional account number such as a credit card number (PAN). *Grigg (EX1005)*, [0006], [0047], [0051]. The mobile wallet account number “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*, [0011]. Grigg’s mobile wallet

account number “may be permanently associated with the mobile wallet” on the user device. *Grigg (EX1005)*, [0051]. “Payment device” refers to “means of payment for a product” such as a “credit card,” “debit card,” or a “payment device account number (such as a traditional bank account number)[.]” *Grigg (EX1005)*, [0006], [0029]. Grigg teaches that “there may be a different mobile wallet account number for each payment device [e.g., credit card] associated with the mobile wallet.” *Grigg (EX1005)*, [0006], [0011]. The mobile wallet number is provided by the financial institution to the mobile wallet application of the device over a wireless network. *Grigg (EX1005)*, [0042], [0053].

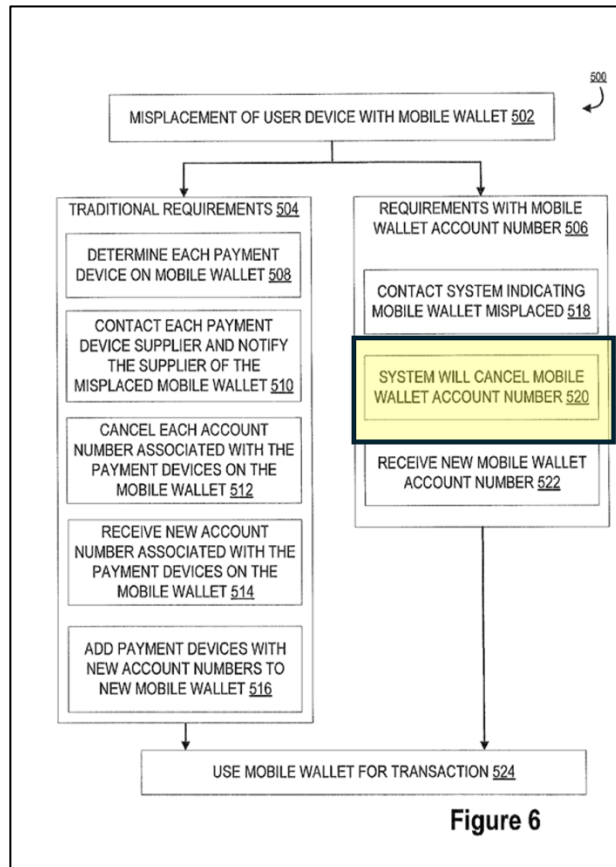
134. The financial institution, “create[s] a mobile wallet account number for the user’s mobile wallet,” which is “permanently associated with the mobile wallet.” *Grigg*, [0051]. A POSITA would have understood that since the mobile wallet account number is permanently assigned to the device 204, it is static. Grigg’s mobile wallet application 222 running on the mobile device 204 “receive[s] a mobile wallet account number” and “store[s] the mobile wallet account number in the memory device 216.” *Grigg*, [0073]. A POSITA would have understood that since Grigg’s mobile wallet account number is specifically assigned to the mobile wallet of device 204, it is device account number.

135. Grigg therefore teaches (1) a user device with a mobile wallet, (2) assigning a user’s payment device (e.g., credit card, etc.) associated with the device

mobile wallet a “mobile wallet account number” (*device account number*) to be used by the user device 204 in place of a traditional payment account number, and (3) allowing the user to present his/her mobile wallet with a mobile wallet account number at a point-of-transaction (POT) for payment. *Grigg (EX1005)*, [0043], [0047], [0051].

136. Grigg’s mobile wallet account number is a *device* account number. Grigg teaches that “the user 202 may use his/her user device 204 as a mobile wallet” (*Grigg (EX1005)*, [0043]) and that the “mobile wallet account number” is created “for the user’s mobile wallet” and “permanently associated with the mobile wallet.” *Grigg (EX1005)*, [0037], [0051], [0080].

137. The mobile wallet application running on the mobile device “*receive[s]* a mobile wallet account number” and “*store[s]* the mobile wallet account number in the memory device.” *Grigg (EX1005)*, [0073]. The financial institution server also stores the mobile wallet account number and associated payment device account numbers. *Grigg (EX1005)*, [0073]. If the user loses the user device being used as a mobile wallet, the mobile wallet account number may be cancelled and a new mobile wallet number assigned to the user’s new user device. *Grigg (EX1005)*, [0074], Fig. 6.



138. A POSITA would have understood that if you lose your phone, based on Grigg's teachings in Fig. 6 you cannot provision the old mobile wallet number to the new phone, so therefore Grigg's mobile wallet account number is specific to each device and card it is on. Grigg, therefore, teaches a device account number that is a static mobile wallet account number permanently associated with a particular device's mobile wallet. A POSITA would have appreciated that using Grigg's teachings does not require the user to have to get a new PAN if a device is lost. As taught by Grigg, if the user device 204 gets misplaced and another individual finds the device, the "other individual will not have access to all of the payment device

account numbers for the payment accounts the user 202 may have in his/her mobile wallet.” *Grigg*, [0074]. Accordingly, Grigg’s mobile wallet number is an account number for a particular payment device (credit card, etc.) that is specifically usable by the assigned mobile device (device account number).

139. The mobile wallet account number is also static in that it is only able to be used by the mobile wallet of the device and is cancelled by the user if the device is lost or stolen. Thus, Grigg’s mobile wallet account number is static device account number payment information.

140. Accordingly, Grigg teaches receiving wirelessly a static device account number payment information for storage on an electronic device.

c) Motivation to Combine

141. A POSITA would have found it obvious and been motivated to wirelessly receive and store Grigg’s mobile wallet account number in place of Toomer’s account number. Grigg’s mobile wallet account number is similar to Toomer’s “unique identifier” that is used “by other systems in identifying” an account. *Toomer (EX1004)*, [0038]. Grigg notes that using mobile wallet account numbers instead of an actual account number prevents bad actors from accessing the user’s real payment account numbers in the event the electronic device is lost or stolen. *Grigg (EX1005)*, [0002]-[0004]. Thus, this modification prevents bad actors from obtaining access to the actual account number if a user device is stolen or if the

account number is intercepted during a transaction. A POSITA would have appreciated that storing and using a mobile wallet account number is safer than storing the actual account number on Toomer's device. Indeed, the use of alternative account numbers in financial transactions was well-known prior to 2012. *See* Section VI.C.1. For example, Kranzley describes a VPAN for use in a transaction between a mobile device and terminal place of an account number issued to cardholders. *Kranzley*, [0066]. Smith '083 and Smith '508 similarly teaches use of a MCA and PPAN, respectively, assigned to a mobile device for use in a transaction in place of a PAN. *See* Section VI.C.1.

142. Thus, a POSITA would have been motivated to use Grigg's mobile wallet account number in place of Toomer's account number. Indeed, Toomer recognizes the mobile device may not store the account number, but instead store "a unique identifier for use by other systems in identifying one or more accounts associated with the mobile wallet," similar to Grigg's mobile wallet account number. *Toomer (EX1004)*, [0038]. It was well known in the art that a mobile device could be vulnerable to malicious attacks and therefore storing Grigg's mobile wallet account number instead of the account number on Toomer's mobile device would have increased security for the user's account. A POSITA would have recognized this benefit because if a user's device is lost or stolen, only the mobile wallet account number(s) would have to be cancelled; automatic transactions using the traditional

payment credentials (e.g., PAN) would not be impacted. *Grigg*, [0074], Fig. 6. The same would be true if the mobile wallet account number were intercepted by a bad actor during transmission to the terminal or issuer. A POSITA would have appreciated that such a modification would have improved card management, allowing the mobile wallet account number to be canceled if Toomer's mobile device is lost or compromised without affecting other devices using the same underlying PAN.

143. A POSITA would have had a reasonable expectation of success in implementing *Grigg*'s mobile wallet account number in Toomer's payment application without undue experimentation because Toomer already teaches use of unique account identifiers in the payment credential for identifying an account and a POSITA would have been familiar with using account number alternatives when making mobile payments. *See* Section VI.C.1. In the combination, *Grigg*'s mobile wallet account number would perform the same function as Toomer's PAN or unique identifier—provide an alternative account number that can be used for a payment transaction. *Grigg* (*EX1005*), [0051]. A POSITA would have understood this modification would be combining prior art elements according to known methods to yield the predictable result of increased security.

144. A POSITA would have recognized that modifying Toomer's system according to the teachings of *Grigg* required only basic software modifications and

routine skill as the constituent hardware components and information stored in the respective components is largely the same. A POSITA would recognize that the electronic device of Toomer could be beneficially modified to receive Grigg's mobile wallet number over a wireless connection and store in device memory for later use in a transaction.

145. In combination, Toomer's mobile device would wirelessly receive the assigned mobile wallet account number(s) and store the same in Toomer's device memory within the payment credentials as a replacement for Toomer's account number. *Toomer (EX1004)*, [0038]-[0039], [0052], [0063]. It was well known in the art that storing sensitive information such as an account number in fewer locations lessens the risks of this information being compromised. The mobile wallet account number would be used instead of the account number when making payment transactions, as taught by Grigg. *Grigg (EX1005)*, [0051]. A POSITA would again have recognized the increased security benefits because sensitive information like an account number would not be stored on the user device or transmitted.

146. This modification is a substitution of one known element for another predictably resulting in increased security of Toomer's payment system. Because Grigg's mobile wallet account number is used in the same way as a PAN in Toomer, there would have been a reasonable expectation of success configuring Toomer's device to make payments using the mobile wallet account number, as such would

have been a combination of known elements that would yield predictable results in increasing transaction security.

147. Additionally, Griggs teaches that “in some embodiments, there may be a different mobile wallet account number for each of the payment devices [e.g., credit card] associated with the mobile wallet.” *Grigg (EX1005)*, [0006], [0011]. It would have been obvious and a POSITA would have been motivated to apply this teaching to the embodiments illustrated in Grigg Figs. 1-6. *Grigg (EX1005)*, [0035]. A POSITA would have recognized that assigning a different mobile wallet account number for each payment device would allow the user to “select the payment device that he/she wishes to use for the transaction” (*Grigg (EX1005)*, [0054], [0084], [0089]) and still receive the increased security benefits from not storing traditional account information. A POSITA would have understood that having a separate account number for each of the user’s payment methods on the user device was well-known and would have had a reasonable expectation of success.

148. Further, it would have been obvious and a POSITA would have been motivated to apply Grigg’s teaching that the mobile wallet account number is permanently assigned to the device because Grigg’s mobile wallet account number is used in place of payment information (e.g., PAN) which is also static. *Grigg (EX1005)*, [0051]. It is also a more simple solution requiring less system resources. A POSITA would have been familiar with permanent account numbers and would

have had a reasonable expectation of success in assigning and wirelessly sending a permanent mobile wallet account number(s) (static device account number) to Toomer's payment device(s) and storing the same thereon.

149. Accordingly, it would have been obvious to modify Toomer with the teachings of Grigg such that Toomer's mobile device receives wirelessly a static device account number payment information for storage on the electronic device.

6. 10(e): and wherein

at least a portion of the payment information is a limited-use number for limited use by the device, in place of a issuer provided payment information; and,

150. Grigg's mobile wallet account number is a limited-use number in that it is only able to be used by mobile wallet of the device and is cancelled by the user if the device is stolen. Thus, Grigg's mobile wallet account number (i.e., at least a portion of the payment information) is a limited-use number for limited use by the device. See Claim 10(d). As discussed in Claim 10(d), a POSITA would have found it obvious and been motivated to use Grigg's mobile wallet account number in place of Toomer's account number in the payment credential (issuer provided payment information).

7. ***10(f): dynamically generating a one-time limited-use number based on at least one of a set of information including: user-identifying information; ... time; merchant; sequence count; payment information; account information; amount; ...; and***

151. It would have been obvious to modify Toomer-Griggs to dynamically generate a one-time limited-use number based on multiple data elements in view of Hammad.

a) *Toomer's Teachings*

152. Toomer teaches the mobile device stores payment credentials, which includes information representing an account (e.g., bank name, account number, account type, etc.). *Toomer (EX1004)*, [0038]. Toomer further teaches that the mobile device can “generate a unique identifier for use by other systems in identifying ... accounts associated with the mobile wallet.” *Toomer (EX1004)*, [0038]. The payment credentials are used in authorizing a transaction. *Toomer (EX1004)*, [0052]-[0054].

153. A POSITA would have understood that in a contactless or wireless payment transaction, such as those described in Toomer and Hammad (described below), a mobile device would transmit a security code (e.g., CVV), with other payment information stored on the mobile device, to a point-of-sale device. *Toomer (EX1004)*, [0002], [0062]; *Hammad*, 1:34-45, 3:60-67, 4:7-20.

b) Hammad's Teachings

154. Hammad describes using a mobile device application for use in a mobile payment transaction. *Hammad (EX1006)*, 2:65-3:11, 3:51-4:6. In performing a transaction, the mobile device dynamically generates a card verification value (“dCVV”). *Hammad (EX1006)*, 2:65-3:11, 3:51-4:6. The dCVV is generated from multiple dynamic and static data elements. *Hammad (EX1006)*, 4:45-60. Specifically, the dCVV is generated from “at least two (e.g., at least three or four) dynamic data elements,” including an “application transaction counter (ATC),” “a cryptogram, digital signature, or hash value based on transaction data,” “a time of day, a current transaction amount, a terminal ID, a merchant ID, and a randomly generated number from a terminal, etc.,” or information “relat[ing] to a consumer’s portable consumer device ...and/or the consumer generally.” *Hammad (EX1006)*, 4:21-56, 4:62-7:5, Figs. 1-3. The “static data elements” include “telephone number, a SIM card number, an account number, birthday, home address, expiration date, etc.” and “service code” to generate a dCVV. *Hammad (EX1006)*, 4:52-60, 5:2-5. In generating a dCVV, the mobile device combined these various data elements with multiple encryption keys, including a master derivation key, resulting in a 3-digit dCVV. *Hammad (EX1006)*, 5:34-6:39, Figs. 1-3. The master derivation key is provided by the service provider and used to generate the dCVV. *Hammad (EX1006)*, 5:38-57, Fig. 2.

155. The dCVV is embedded into payment data, which includes the account number, service code, PVKI, PIN verification data, and/or other information, and transmitted to the point-of-sale terminal and then to the service provider. *Hammad (EX1006)*, 6:40-42, 6:49-7:27, 7:55-61, Figs. 4-5. The service provider uses the dCVV to determine the authenticity of the payment service. *Hammad (EX1006)*, 7:29-38, 7:61-8:50, Fig. 6.

156. A dCVV is generated for “each transaction” and included with other payment data. *Hammad (EX1006)*, 4:61-65; *see also*, 4:61-6:34. Because the dCVV is generated from the ATC, which will change with each transaction, the dCVV will also change and be limited in use to that one transaction. *Hammad (EX1006)*, 4:22-33, 4:63-5:5. Additionally, adding other dynamic and static data elements will further ensure that the dCVV is limited to a single use. Thus, a POSITA would understand that a dCVV is a one-time limited-use number.

c) Motivation to Combine

157. Based on the teachings of *Hammad*, it would have been obvious, and a POSITA would have been motivated to generate a dCVV including dynamic and static data elements, as taught by *Hammad*, in *Toomer-Grigg*.

158. *Hammad* recognizes the risk of fraud in using a static CVV in a contactless transaction. *Hammad (EX1006)*, 1:20-22, 1:34-45, 3:60-67, 4:7-20. In order to address this risk, *Hammad* teaches generating a dCVV from “at least three

or four” dynamic data elements and static data elements, which makes it “highly unlikely that a skimmer can determine the dCVV.” *Hammad (EX1006)*, 4:46-60. As described above, the data elements include a telephone number, birthday, home address (user-identifying information), a time of day (time), merchant ID (merchant); ATC (sequence count); account number (payment information or account information); and current transaction amount (amount); among other data elements, which are combined using a master derivation key. *Hammad (EX1006)*, 4:21-5:5, 5:38-58.

159. A POSITA would have found it obvious to include this information in addition to Grigg’s mobile wallet account number (account information) in generating a dCVV to be used with the payment credentials of Toomer-Grigg when conducting a payment transaction. Indeed, Hammad recognizes that only including one dynamic data element, such as a counter, is susceptible to fraud. *Hammad (EX1006)*, 1:66-2:4. Hammad, therefore, teaches including at least three or four dynamic data elements and static data elements (set of information). A POSITA would have been motivated to include more data elements in generating a dCVV because it would decrease the likelihood that, even if the payment credentials were intercepted, a bad actor could use any of the payment data for fraudulent purposes. Therefore, a POSITA would have been motivated to use additional data elements to

generate a dCVV as part of Toomer's payment credentials sent to a financial institution.

160. A POSITA would have further recognized that modifications to Toomer-Grigg would be minimal as it would require straight-forward and known methods of generating a dynamic CVV and providing the same with other account information, such as Grigg's mobile wallet account number, for authorization by an external device. This modification of known techniques would have yielded the predictable result of increasing security of the transaction.

161. A POSITA would have had a reasonable expectation of success in implementing Hammad's dCVV in Toomer's payment credentials without undue experimentation because Toomer already teaches including various pieces of information in the payment credential and a POSITA would have been familiar with using a dCVV when performing payment transactions. Because Hammad's dCVV is used in a transaction in the same way as Toomer's payment credentials, i.e., to authorize a payment transaction, there would have been a reasonable expectation of success configuring Toomer's device in this way to securely authorize a payment transaction. *Grigg (EX1005)*, [0051]. Such a modification is combining known prior art elements according to known methods to yield the predictable result of increased security.

162. A POSITA would have recognized that modifying Toomer's system according to the teachings of Hammad required only basic software modifications and routine skill because the constituent hardware components and information stored in the respective mobile devices and authorizing systems is largely the same.

163. Accordingly, it would have been obvious to modify Toomer-Grigg with the teachings of Hammad to dynamically generat[e] a one-time limited-use number based on at least one of a set of information including at least user-identifying information, time, merchant, sequence count, payment information, account information, amount, and/or device-unique information.

8. *10(g): using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.*

164. Toomer teaches completing a contactless financial transaction using a payment credential, which includes making "a request to authorize the transaction." *Toomer (EX1004)*, [0006], [0039]. The mobile device transmits payment credentials to a financial institution, via a point-of-sale device and acquirer, during a transaction. *Toomer (EX1004)*, [0038]-[0039], [0051]-[0054], Fig. 4. The payment credentials include "information and/or credential related to a financial account in the mobile wallet[.]" *Toomer (EX1004)*, [0055]; *see also* [0038], [0052]-[0053]. The transaction is authorized based on the validity of the payment credentials and other information

and “whether the mobile device is authorized to use the account for which information or credential has been provided.” *Toomer (EX1004)*, [0054].

165. As discussed in Claim 10(d), Toomer-Grigg render obvious receiving a static device account number for conducting a payment transaction. As discussed in Claim 10(f), Toomer-Grigg-Hammad render obvious dynamically generating a dCVV (one-time limited-use number) for a transaction.

166. It would have been obvious to use the mobile wallet account number and dCVV in place of Toomer’s account number and other information (issuer provided payment information) in conducting a transaction. A POSITA would have recognized that in the contactless transactions described in Toomer, another security measure, such as Hammad’s dCVV, would beneficially provide an additional layer of security beyond those provided for in Toomer-Grigg. *See also* Claim 10(f), *supra*. The risks involved in such transactions was well-known at the time and a POSITA would have been motivated to increase security of a transaction and a user’s account information by implementing these functionalities.

167. Therefore, the combination of Toomer, Grigg and Hammad renders obvious using the mobile wallet account number (static device account number) and dCVV (dynamically generated one-time limited-use number) together in the place of issuer provided payment information for making a payment transaction.

B. Claim 11

- 1. 11. The method of claim 10, wherein the electronic device is configured to accept the user input by at least one of a means comprising: a touch sensor array; a touch screen; a keypad; buttons;**

168. As discussed in Claim 10(a), Toomer teaches that a user can interface with the mobile device 324 “by manipulating a **keypad**, wheel, **touch screen**, or other input device 682.” *Toomer (EX1004)*, [0063]; Fig. 6. Toomer further teaches that “accounts represented by information stored in such electronic devices” may be “manually entered by a user of the device.” *Toomer (EX1004)*, [0003]. A POSITA would have understood that such user input would be manually provided to the mobile device through Toomer’s touch screen or keypad, or found it obvious to modify Toomer to allow for manual entry of account information through the touchscreen.

169. In addition, and as further discussed in Claim 10(a), Grigg teaches a user entering new payment accounts to the device mobile wallet by providing information, such as a credit card number. *See Claim 10(a); Grigg (EX1005)*, [0008], [0048]. For the reasons discussed in Claim 10(a), a POSITA would have found it obvious and been motivated to modify Toomer’s mobile device in view of Grigg’s teaching to allow for input on the device touchscreen or keypad, and would have had a reasonable expectation of success in modifying Toomer in this way.

C. Claim 12

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

170. Toomer teaches that the device-specific information stored on the mobile device comprises [. . .] device identifiers. See Claim 10(b). Grigg teaches storing the mobile wallet account number (device account numbers) on the payment device. Hammad teaches storing an ATC (device usage sequence counters) on the mobile device. See Claim 10(f).

171. It would have been obvious to modify Toomer with the teachings of Grigg and Hammad to maintain two or more of these data elements (at least one of a set) on the electronic device for the same reasons discussed in Claims 10(d) and (f).

D. Claim 13

- 1. 13. The method of claim 10, wherein the user-specific information comprises at least one of a set comprising: ... user information; bank accounts; payment information; device account numbers; ... currency amount**

172. Toomer teaches that the user-specific information comprises [. . .] bank accounts; payment information. See Claim 10(b); see also Toomer (EX1004), [0053] (“current balance levels for the account” i.e., currency amount). Grigg teaches storing the mobile wallet account number (device account numbers) on the payment

device. *See* Claim 10(d). Hammad teaches using birthday or home address (user information) to generate a dCVV. *See* Claim 10(f). A POSITA would have understood that this user information would need be stored, at a minimum transitorily, in order for the mobile device processor to generate a dCVV.

173. It would have been obvious to modify Toomer with the teachings of Grigg and Hammad to maintain multiple data elements (at least one of a set) on the electronic device for the same reasons discussed in Claims 10(d) and (f).

X. GROUND 2: CLAIMS 14-17 ARE OBVIOUS OVER TOOMER, GRIGG, HAMMAD, MULLEN '449, AND LIN

A. Claim 14

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

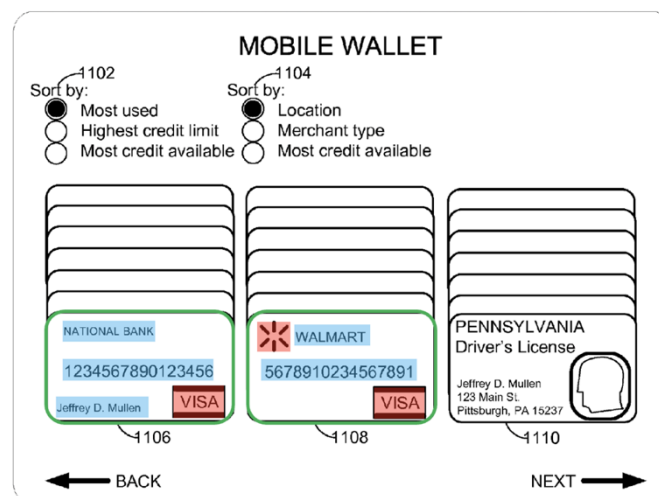
a) Toomer's Teachings

174. Toomer's mobile wallet stores "multiple payment vehicles" and provides "a user interface that can be displayed on a screen or **display device 680**["] *Toomer (EX1004)*, [0063]. The display 680 "may allow the user to review accounts that are **stored** [in] the mobile device 324 and select an account for a particular transaction such as a purchase." *Toomer (EX1004)*, [0052], [0063]. "Payment

vehicles” are payment method types, such as “credit, debit, ... and other types of accounts.” *Toomer (EX1004)*, [0027].

b) Mullen '449's Teachings

175. Mullen teaches a mobile device 100 configured to display a mobile wallet. *Mullen '449 (EX1007)*, [0058], Fig. 1. “[The] mobile device may accept payment and other information from any payment card, **store** and display such information as a virtual card on a GUI [graphical user interface] of the mobile device[.]” *Mullen '449 (EX1007)*, [0021]. Particularly, “information (e.g., payment card number, cardholder name, bank logos and issuer identification) may be stored within memory 160 and **rendered onto display** 154 as a virtual representation of a card.” *Mullen '449 (EX1007)*, [0064]. Figure 11 below illustrates the GUI of a mobile device and depicts payment method types (e.g., credit cards and categories of cards) as images of payment cards (annotated in green), the images including alphanumeric characters (blue) and iconography (red) on the cards.



Mullen '449 (EX1007), Fig. 11; *see also*, [0112]-[0118] (“One or more payment cards, for example, may be rendered onto GUI 1100 and each payment card may be aligned within category 1106.”). Figure 11 depicts alphanumeric characters and iconography, including card network icons (e.g., VISA icons), an issuer logo (e.g., Walmart logo or VISA icon), a portion of the account number, and a cardholder name.

c) Motivation to Combine

176. A POSITA would have found it obvious and been motivated to configure Toomer’s mobile device 324 to similarly render each payment vehicle for selection with its associated images, alphanumeric characters, and iconography, as taught by Mullen ’449. A POSITA would have appreciated that this combination of prior art elements according to known methods would enable the user of the mobile device to easily identify and discern between the payment vehicles stored by the mobile wallet application. A POSITA would have recognized that configuring the mobile device to display the components necessary to complete a transaction – e.g., the card number, cardholder name, etc. – allow the virtual payment vehicle to retain its utility in a contactless transaction.

177. A POSITA would have had a reasonable expectation of success in making such a combination because a mobile wallet and a display screen were both well-known and conventional on mobile devices prior to the ’520 Patent, as shown

by Toomer and Mullen '449. Additional examples of mobile wallet displays allowing a user to identify payment accounts for selection are found in Lin and Phillips. *See* Claim 10(a); *see Lin (EX1008)*, 55:9-15, 72:7-73:17, Figs. 11B, 14E; *Phillips*, Figs. 2A, 4. Further, the teaching of Mullen '449 would enhance the user experience of displaying accounts for selection.

178. In the combination, Toomer's mobile device is configured to render the stored payment methods on its display device, including images, alphanumeric characters and iconography relating to the holder, issuer, account number, and/or payment network associated with the payment methods, as taught by Mullen '449.

B. Claim 15

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

a) Toomer's Teachings

179. Toomer's mobile device allows a user to "select a specific payment vehicle by manipulating a [. . .] touch screen" for use in "a particular transaction." *Toomer (EX1004)*, [0063], [0052] ("The mobile device ... allow[s] the user to review accounts that are stored or identified in the mobile device 324 and **select an account for a particular transaction** such as a purchase."). As discussed in Claim 10(a), Toomer's interface includes a touchscreen that accepts user input or it would

have been obvious to modify Toomer to accept user input relating to payment accounts in view of Grigg. *Grigg (EX1005)*, [0054], [0084]. Thus, Toomer teaches, or renders obvious in view of Grigg, accepting a user selection of a payment vehicle (i.e., a payment method type for use in a transaction) from the payment vehicles displayed using a touch screen interface for the user selection. See Claim 14.

b) Mullen '449's Teachings

180. Alternatively, as discussed in Claim 14, Mullen '449 teaches a similar mobile wallet application that renders on a mobile device display a list of card images representing different payment methods for selection and use. *Mullen '449 (EX1007)*, [0112], Fig. 11. The user may “select one of sort options 1104” (e.g., merchant type) to display a list of cards within that category. *Mullen '449 (EX1007)*, [0116], Fig. 11; *see also*, [0114]-[0115]. “GUI ... allow[s] a user ... to select (e.g., touch) one of the virtual cards rendered ... [and] confirm ... that the selected card is the desired virtual card for use.” *Mullen '449 (EX1007)*, [0120], Fig. 13; *see also* [0119], Fig. 12.

c) Motivation to Combine

181. For the same reasons discussed in Claim 14, a POSITA would have found it obvious and been motivated to configure Toomer's mobile device to render a list of card images representing different payment vehicles in various categories that are available for user selection on the touch screen display, as taught in Mullen

'449. *See* Claim 14. A POSITA also would have had a reasonable expectation of success in the combination as such functionality was commonplace at the time. *See* Claim 14.

C. Claim 16

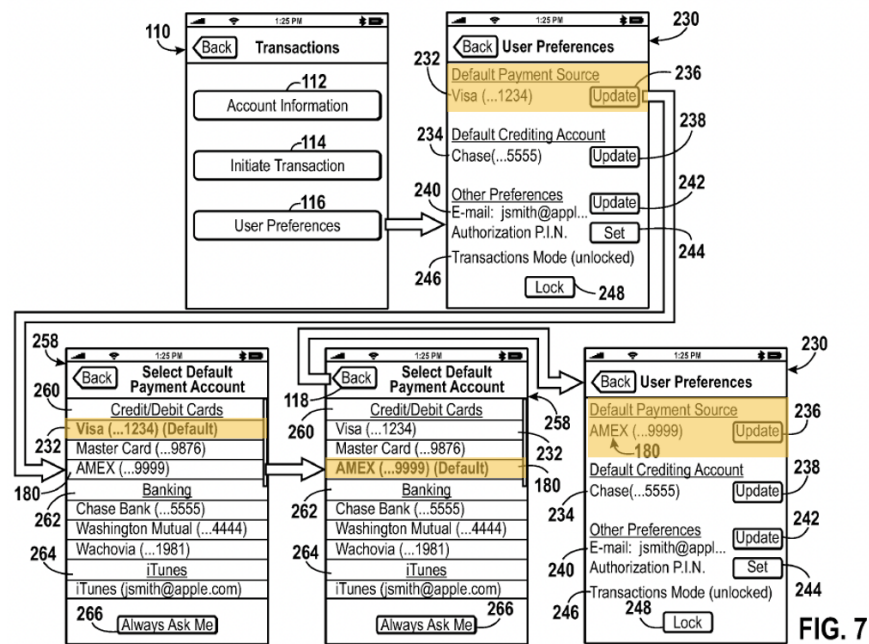
1. ***16. The method of claim 15, wherein the user selection is a default payment method to be used in transactions.***

- a) *Toomer's Teachings*

182. Toomer teaches a *user selection* of a payment method *to be used in transactions*. *See* Claim 15.

- b) *Lin's Teachings*

183. Lin teaches a similar mobile wallet application on a mobile device that “may include a user-specified preferred or **default payment account** or source[.]” *Lin (EX1008)*, 25:22-27. The user selects the default payment method to be used in transactions from screen 110, which “represent[s] a ‘home’ or ‘main’ screen for the transaction application” (i.e., the mobile wallet application). *Lin (EX1008)*, 37:22-25, 40:1-7, 47:1-2, 71:24-31, Fig. 14E.



Lin (EX1008), Fig. 7 (illustrating a process for selecting a default payment method).

c) Motivation to Combine

184. It would have been obvious and a POSITA would have been motivated to configure Toomer's mobile wallet application to allow the user to select a default payment method, as taught by Lin. A POSITA would have appreciated that allowing the user to select a default payment method would have been an added convenience to the user, increasing the speed of financial transactions. Therefore, a POSITA would have been motivated to combine prior art elements according to known methods to enhance both the user experience and the overall convenience of Toomer's mobile wallet application. A POSITA would have had a reasonable expectation of success in making such a combination without undue

experimentation, because both the use of a mobile wallet application and the ability to establish a default payment method in such a mobile wallet application were known prior to the '520 patent.

185. Thus, in combination, Toomer's mobile device is configured to permit a user to select a default payment method stored on its mobile wallet application for use in transactions, as taught by Lin.

D. Claim 17

1. ***17. The method of claim 15, wherein the issuer provided payment information is selected from at least one of a set comprising: account number; card number; device account number; ... an account type;***

186. As discussed in Claim 10(a), the combination of Toomer and Grigg teach or render obvious accepting user input of issuer provided payment information. Toomer teaches or renders obvious that this information includes "accounts" manually entered by the user and selecting an account by reviewing "account number, account type, etc[.]" Toomer (EX1004), [0003], [0052]; *see also* Claim 10(a); Similarly, Grigg similarly teaches inputting payment devices, e.g., a credit card (account number/card number), to a mobile device and receiving and storing a mobile wallet account number (device account number) for selection, which is provided by the issuer and stored on the mobile device. *See* Claims 10(a), (d).

187. Accordingly, the proposed combination teaches an electronic device with issuer provided payment information is selected from at least one of a set of the recited information based on accepted user input.

XI. GROUND 3: CLAIMS 1, 4-6, 8-9 ARE OBVIOUS OVER TOOMER, CASEY, GRIGG, AND HAMMAD

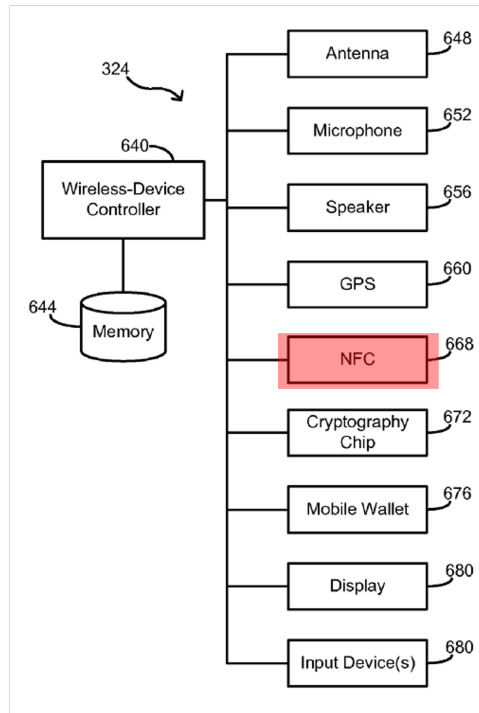
A. Claim 1

1. *1(pre): An electronic device comprising:*

188. Toomer in view of Casey, Grigg, and Hammad teaches an mobile device, such as a phone or smart card, (electronic device) including the recited elements. *Toomer (EX1004)*, [0023], [0051]-[0052], Figs. 2, 4, 6; *see below* Claims 1(a)-(n).

2. *1(a): a near-field communication (NFC) unit;*

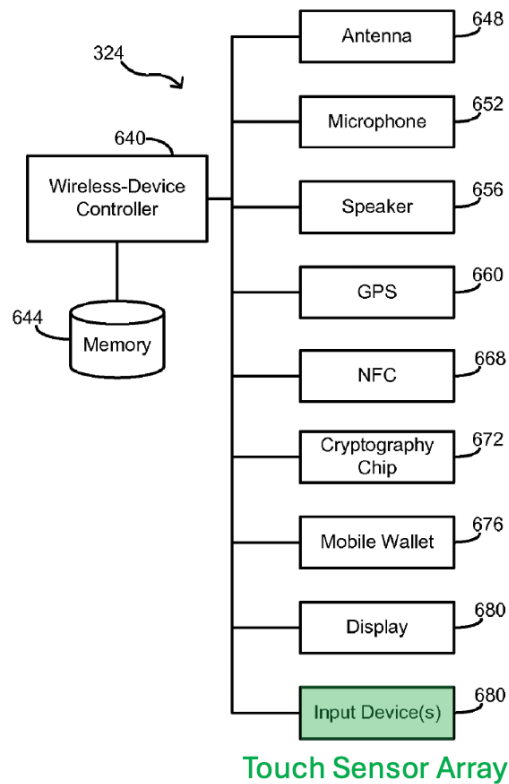
189. Toomer's mobile device includes a "Near Field Communications (NFC) transponder" and a "NFC module 668 ... provided to encode and decode transmissions sent and received electromagnetically with the point of sale device." *Toomer (EX1004)*, [0062]; *see also* [0023], [0025], [0051]-[0052], [0055], [0063].



Toomer (EX1004), Fig. 6 (annotated); *see also* Fig. 4.

3. 1(b): a touch sensor array;

190. Toomer's mobile devices includes a user interface, such as a touch screen and keypad as input device 682, displayed on a screen and through which a user can interact with the mobile wallet. *See* Claim 10(a); *see also Toomer (EX1004)*, [0063], Fig. 6.



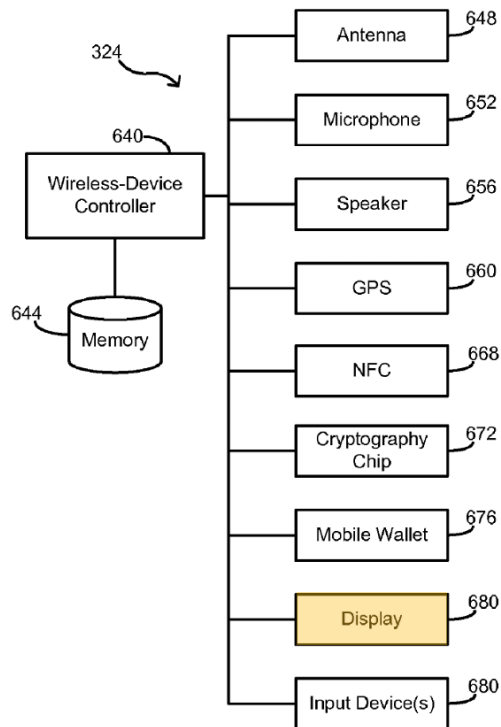
Toomer (EX1004), Fig. 6 (annotated).¹

191. The '520 Patent specification discloses that a touch sensor array “may comprise a touch screen panel, a keypad, or a combination thereof.” ‘520 Patent (*EX1001*), 5:49-51. Therefore, Toomer’s touch screen is a touch sensor array.

4. 1(c): a display;

192. Toomer’s mobile device includes a “screen or display device 680.”
Toomer (EX1004), [0063]; *see also* [0044].

¹ Figure 6 incorrectly identifies the input device as 680.



Toomer (EX1004), Fig. 6 (annotated); *see also* Fig. 2.

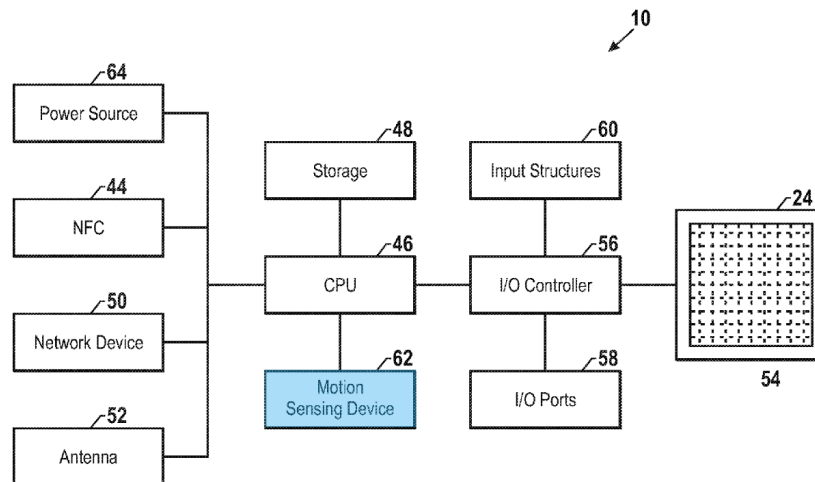
5. 1(d): a motion rate detection array;

a) Toomer's Teachings

193. Toomer's mobile device includes "a keypad, wheel, touch screen, or other input device 682." *Toomer (EX1004)*, [0063].

b) Casey's Teachings

194. Casey teaches a similar mobile device for use in a payment transaction. *Casey (EX1009)*, Abstract, 1:45-46, 3:10-14, 3:38-46, Figs. 1, 3. The mobile device includes "a motion sensing device 62 for receiving user input." *Casey (EX1009)*, 7:59-61.



Casey (EX1009), Fig. 2 (annotated).

195. The motion sensing device is “any device configured to measure motion or acceleration,” including a three-axis accelerometer. Casey (EX1009), 7:61-8:3. “Motion data acquired by the motion sensing device 62 may be used to confirm a payment transaction.” Casey (EX1009), 8:4-13; see also 9:47-10:2, 18:39-19:10, Figs. 12-13.

196. A POSITA would have understood a 3-axis accelerometer incorporated three single-axis accelerometers or sensors positioned to allow motion detection in all three directions (i.e., along X, Y, and Z axes). Such 3-axis (or tr-axial) accelerometers were known to have been formed by including three accelerometers in a single package. For example, a paper from Che in 2005 describes a “3-axis chip” accelerometer as “a monolithic integration of three individual single-axis accelerometers,” one accelerometer for each of the x, y, and z axes. Che (EX1045),

1.

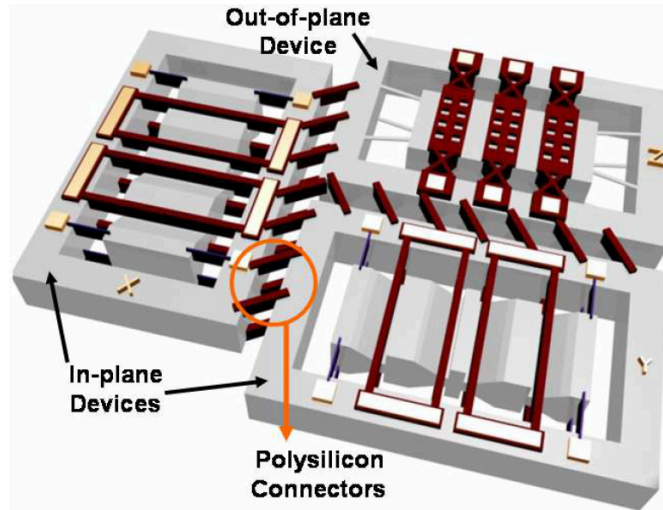


Figure 1: 3-axis *single-chip* micro-g accelerometer.

197. This structure is similarly described in U.S. Patent No. 8,351,910 to Horodezky which states that “[a] three-dimensional accelerometer ... may comprise three one-dimensional accelerometers.” EX1046, 5:8-11; *see also* EX1047 (U.S. Patent No. 8,952,832 to Nasiri), 4:67-5:8, Figs. 2 (“Accelerometers 28 can measure the linear acceleration of the device 10 (or portion thereof) housing the accelerometers 28. From one to three accelerometers can typically be provided, depending on the motion that is desired to be sensed in a particular embodiment. For example, if three gyroscopes 26 and three accelerometers 28 are used, then a 6-axis sensing device is provided providing sensing in all six degrees of freedom.”). Further, U.S. Patent No. 6,938,484 to Najafi describes “a monolithic, three-axis accelerometer including three individual single-axis accelerometers is provided.” EX1048, 8:45-48, 9:3-7. U.S. Patent No. 7,258,012 to Xie similarly describes a “monolithic integrated three axis accelerometer 700 ... comprising x-sensing

accelerometer 710, y-axis accelerometer 720 and z-axis accelerometer 730, all disposed on the same chip.” EX1049, 10:41-45, Fig. 7A. Finally, U.S. Patent No. 8,892,390 to MacGougan describes an accelerometer having “accelerometers on each axis” that observe “components of gravity” to determine the “motion state of a mobile device.” EX1050, 5:60-6:8, Abstract, Figs. 1-2.

198. Dependent claim 2 of the ’520 Patent recites that a motion rate detection array includes a plurality of accelerometers. Thus, a POSITA would understand that Casey teaches a motion rate detection array.

c) Motivation to Combine

199. It would have been obvious and a POSITA would have been motivated to include Casey’s motion sensing device in Toomer’s mobile device. A POSITA would have appreciated that mobile devices at the time of the ’520 Patent typically included inertial sensor arrays, such as accelerometers. For example, the iPhone 4, introduced in 2010, incorporated a three-axis accelerometer. See EX1051 (<https://www.apple.com/newsroom/2010/06/07Apple-Presents-iPhone-4/>); EX1052 (<https://www.memsjournal.com/2010/12/motion-sensing-in-the-iphone-4-mems-accelerometer.html>) (“The iPhone 4 is the first portable consumer device to incorporate a three-axis accelerometer”). Motorola had at least 2 phones (ES4300 and Droid by Google) that included a 3-axis accelerometer. EX1053 (https://www.ruggedpcreview.com/3_handhelds_motorola_es400.html) (“a 3-axis

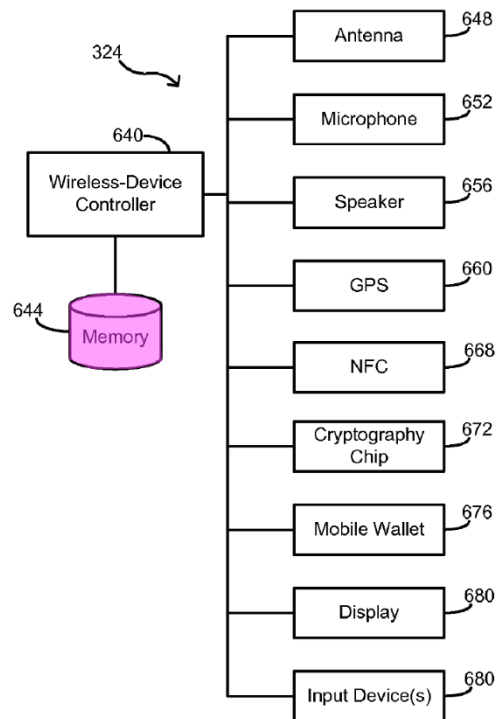
accelerometer that's presumably used to provide some of the motion-sensing functionality expected from a modern smartphone.”); EX1054 (<https://www.andybrain.com/2009/review-of-the-motorola-droid-from-verizon-wireless/>) (“Extras 802.11b/g , 3-axis accelerometer”). HTC phones also included an accelerometer, including a 3-axis accelerometer. EX1055 (<https://www.ibtimes.com/top-10-htc-smartphones-2011-388788>). Similarly, U.S. Publn. No. 2009/0320123 to Yu (EX1056) describes a mobile phone that includes a “motion detection device 210” comprising “one or more accelerometers” for detecting motion of the device. *Yu (EX1056)*, [0023], [0028], Fig. 2. The mobile device can be used to access a banking or e-commerce services after the user is authenticated through a motion. *Yu (EX1056)*, [0018]-[0020], [0025], [0037]-[0038], [0042], Figs. 3-4, 7. These examples demonstrate that the presence accelerometers in mobile phones before 2012 was ubiquitous, which would have motivated a POSITA to include the same in the mobile device of Toomer to keep up to date with technologies expected by users to present in a mobile phone.

200. Moreover, a POSITA would have understood that including an accelerometer array would have allowed Toomer’s mobile device to interpret user motions to confirm or deny payment transactions. Indeed, Casey teaches that the “accelerometer[] may sense movement of the electronic device and move the graphical element in response to the motion[,]” “to confirm or decline a payment

transaction using a selected payment instrument.” *Casey (EX1009)*, Abstract, 7:59-8:13, 9:47-52, 19:1-10, Figs 3, 5-6, 10-13. Providing more than one way to confirm or deny transactions, including using motion detection units, would have enhanced the user experience by making confirmation or denial easier and more efficient and providing options for the user to perform a transaction. It also reduces the possibility of an erroneous transaction as the “motion based confirmation may impress upon a user the significance of the payment transaction.” *Casey (EX1009)*, 13:62-14:2. Thus, a POSITA would have been motivated to combine prior art elements according to known methods to yield predictable results of user convenience and increased security.

6. *1(e): a memory for storing a user data and a currency amount;*

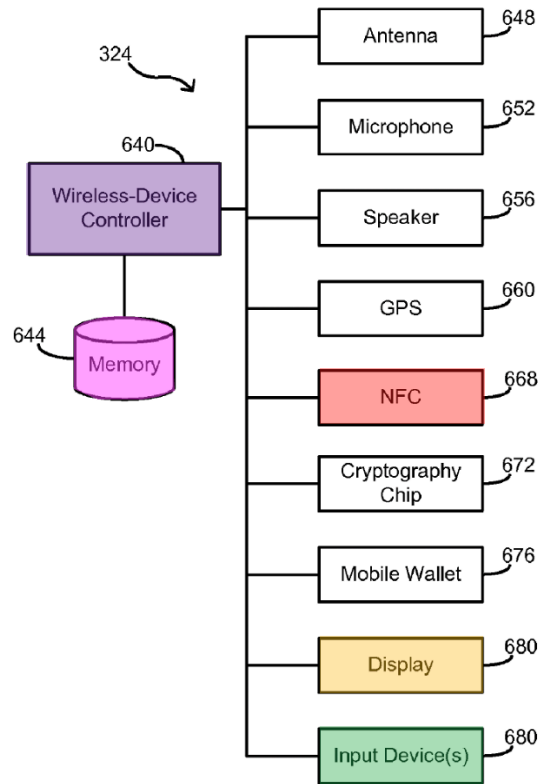
201. Toomer’s mobile device includes a memory 644. *Toomer (EX1004)*, [0061]; *see also* [0044]. Toomer’s memory is used to store payment information, which includes “ownership details of the account” (i.e., a user data) and “current balance levels for the account” (i.e., a currency amount). *Toomer (EX1004)*, [0052]-[0053]; *see also* [0024], [0027].



Toomer (EX1004), Fig. 6 (annotated); *see also* Fig. 2.

7. ***1(f): a processor operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory;***

202. Toomer’s mobile device, like any mobile device, includes a processor. Specifically, the mobile device includes a wireless-device controller “which can comprise a microprocessor or other computing device executing software stored ... in memory 644 for coordinating the functions of a variety of components.” *Toomer (EX1004)*, [0061]; *see also* [0044]-[0045]. Figure 6 shows that the processor 640 is operatively coupled to the NFC unit, the touch sensor array (input device 682), the display, and the memory.



Toomer (EX1004), Fig. 6 (annotated); *see also* Fig. 2.

203. As discussed, it would have been obvious to a POSITA to modify Toomer's mobile device to include a motion rate detection array, as taught by Casey. *See* Claim 1(d). For the same reasons, it would have been obvious to couple Toomer's processor 640 to the motion rate detection array so that the processor may coordinate functions using the array.

8. ***1(g) a computer readable medium having instructions stored thereon that, responsive to execution by the electronic device, cause the electronic device to perform operations comprising:***

204. Toomer teaches a "mobile wallet application" that is "a client software application that can reside on and/or be executed by a mobile device." *Toomer (EX1004)*, [0024]. The mobile wallet application "store[s] payment vehicle

information[,]” “provide[s] a user interface that can be used to select a specific payment vehicle[,]” and “can be adapted to provide security to deter fraudulent and unauthorized use of the payment vehicles” in performing a transaction. *Toomer (EX1004)*, [0024], [0052], [0055], [0063]. The applications residing on the computer “implement the methods of the invention as described herein,” including those required by limitations 1(i)-(n) (as modified by the references discussed therein). *Toomer (EX1004)*, [0047] *see also* Claims 1(i)-(n).

205. Toomer’s mobile device includes a machine readable medium” having “a series of instructions which, when executed by a processor, cause the processor to authorize a financial transaction” by performing various steps. *Toomer (EX1004)*, [0008]; *see also*, [0036], [0061], [0063] [0072], Claim 26.

9. 1(h)-(n):

206. *See* Ground 1, Claims 10(a)-(g).

B. Claim 4

1. *4. The electronic device of claim 1, wherein the user input comprises one or more of:*

an introduction of a transaction-specific identifier;

a confirmation or a denial of an indicated transaction; and

a lock/unlock command determining operation of the electronic device according to an input sequence or a gesture across the plurality of touch sensors.

a) Casey's Teachings

207. Casey teaches “a graphical element 180 to confirm the payment transaction” including “a slide bar 182 that may be moved to the right or to the left using the touch screen 54 (FIG. 2).” *Casey (EX1009)*, 13:39-43; *see also* 13:46-48, Fig. 5. This action may “decline the payment” or “confirm the payment transaction.” *Casey (EX1009)*, 13:48-51, Figs. 5-6; *see also* 18:39-19:10, Figs. 12-13.

208. Casey further teaches “a personal identification number (PIN), password, or other type of identifier, may be associated with a payment instrument.” *Casey (EX1009)*, 9:15-17, 12:46-53, 12:66-13:1, 17:4-11. A “user may enter a PIN ... through a keypad[.]” *Casey (EX1009)*, 12:66-13:3. The PIN (lock/unlock command) is a sequence used to verify the payment instrument and authorize a transaction (determining operation of the electronic device). *Casey (EX1009)*, 9:17-22, 13:4-6, 17:4-11.

b) Motivation to Combine

209. Based on the teachings of Casey, it would have been obvious, and a POSITA would have been motivated to configure Toomer's mobile wallet application to similarly accept user inputs on the touch screen to allow the user to enter a PIN or confirm/deny a transaction using the touchscreen. A POSITA would have understood that Toomer's mobile wallet would have needed to provide a way for the user to confirm/deny a transaction before it is completed in order to limit erroneous transactions. A POSITA would have further understood that requiring a PIN to access the payment method would increase the security of the transaction. Using Casey's input method of inputting a PIN or confirming/denying the transaction would have represented a combination of prior art elements according to known methods to yield the predictable result of requiring the user to enter a PIN or to approve/deny a transaction before it is completed, thereby providing additional security. Entry of a PIN to access or authorize a payment transaction and confirming a transaction were well-known functionalities. For example, Lin teaches both entering a PIN and confirming a transaction. *Lin (EX1008)*, 51:8-52:15, 75:5-76:12, Figs. 10A-B, 14H. Similarly, U.S. Patent No. 9,721,319 to Smets (assigned to MasterCard) describe conducting a transaction with a merchant in which a user is required to confirm payment ("Pay") and enter a PIN. *Smets (EX1057)*, Abstract, 11:9-19, 11:51-12:19, Figs. 8-10; *see also* EX1043 (U.S. Publn. No. 2011/0140841

to Bona), [0007] (“Once the card has been verified as authentic, the customer enters a 4-digit PIN, which is checked against the PIN stored on the card; if the two match, the transaction completes.”); [0120] (“the user is authenticated, such as using biometrics if the cell phone (or smart card) has biometric capabilities or a PIN or password authentication scheme.”). Modifying Toomer’s mobile device in this way would have require minimal work and required routine skill given the prevalence and ways for interacting with a mobile device in a payment transaction at the time.

C. Claim 5

- 1. 5. *The electronic device of claim 1, further comprising a sequence counter which generates a sequential parameter when the processor initiates a transaction, wherein the sequential parameter is combined with any of a user information, a transaction identifier, a user secret, and a credit card authority secret and the processor is operable to generate a limited-duration credit card number therefrom.***

210. Toomer in view of Hammad teaches combining the master derivation key (credit card authority secret), telephone number, birthday, home address (user information), and an ATC (a sequential parameter) to generate a dCVV. *See* Claim 10(f). Hammad’s ATC (a sequential parameter) used in generating a dCVV is generated by increasing an ATC counter (sequence counter) for every transaction. *Hammad (EX1006)*, 4:22-26. Hammad further teaches that the time of day can be used in generating a dCVV. *Hammad (EX1006)*, 3:9-11, 4:36-40. The time of day,

if within a predetermined range of times, can be used in the authorization process.

Hammad (EX1006), 8:11-14, 8:28-36.

211. It would have been obvious to a POSITA and a POSITA would have been motivated to include the time of day in generating the dCVV, both of which are included in the payment information. As combined with teachings of Grigg, Toomer's mobile device would generate the dCVV from mobile wallet account number, user information, and time of day, in addition to other static and dynamic data elements and provide the mobile wallet account number and dCVV, among other information, to an authorizing server. *See* Claims 1(n), 10(g). A POSITA would understand that the mobile wallet account number and dCVV, in combination, are limited in duration to a single transaction within a time specific time window (limited-duration credit card number) and absent a valid dCVV, generated with the time of day and received within a valid time window, the wallet account number will not be authorized. A POSITA would have been motivated to include the time of day, in addition to other data elements, as an additional layer of security in authorizing the transaction. *See also* Claims 1(m)-(n), 10(f)-(g). Using more data elements, including time, decreases the likelihood of a bad actor intercepting the payment credentials and using the elements to determine the dCVV generation or otherwise using the payment information. *See* Ground 1, Claim 10(f).

D. Claim 6

- 1. 6. The electronic device of claim 1, wherein the limited-use number has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions.**

212. As discussed in Claim 10(f), Hammad's dCVV (limited-use number) is limited to a single transaction (limited in scope of use to a predetermined number of authorized transactions). Thus, the "predetermined number of authorized transactions" for the dCVV is 1. A POSITA would have understood that Hammad's dCVV could also not be validly used in another transaction (limited recurrence) because the ATC changes for each transaction. See Ground 1, Claim 10(f); Ground 3, Claim 5.

E. Claim 8

- 1. 8. The electronic device of claim 1, wherein the payment transaction comprises a cryptographic hash of the transaction unit, wherein the cryptographic hash is processed and stored in said memory.**

a) Hammad's Teachings

213. Hammad teaches that, in addition to an ATC, a "hash value based on the transaction data" may be used in generating the dCVV. *Hammad (EX1006)*, 4:33-36; see also Claim 10(f). When the payment data is transmitted to a financial institution, the cryptographic hash, like the ATC, would be stored and included in the payment data. *Hammad (EX1006)*, 6:49-7:3, 7:4-28, Figs. 4-5. A POSITA would have understood that the cryptographic hash is performed by the mobile device

processor and stored in memory, like the ATC, prior to being embedding in payment data for transmission.

b) Motivation to Combine

214. A POSITA would have found it obvious and been motivated to use the cryptographic hash, as an additional dynamic data element, in generating the dCVV in the combination for the same reasons discussed in Claim 10(f).

F. Claim 9

1. 9. *The electronic device of claim 1, further comprising a USB connector for connection to a standard computing device.*

215. Casey's electronic device includes I/O ports "configured to connect to a variety of external devices, including but not limited to a power source ... a computer" where the I/O port "may support any interface type, such as a universal serial bus (USB) port[.]" *Casey (EX1009)*, 5:35-43. Thus, Casey's device includes a USB connector for connection to a standard computing device.

216. It would have been obvious and a POSITA would have been motivated to configure Toomer's mobile device to include a USB port for connection to standard computing devices, as taught by Casey. POSITAs at the time of the '520 Patent would have understood that mobile devices typically included I/O ports, e.g., USB ports, for connection to other computing devices or components. For example, Lin describes that its electronic device includes "various input/output ports (I/O)" to "allow a user to connect the device 10 to or interface the device 10 with one more

external devices[,]” such as “a computer.” *Lin (EX1008)*, 17:29-18:11; *see also* 18:15-20. The “I/O ports” that support “any suitable interface type such as a universal serial bus (USB) port[.]” *Lin (EX1008)*, 18:11-13, Fig. 1 (item 36). Thus, a POSITA would have been motivated to combine prior art elements according to known methods to yield the predictable result of allowing Toomer’s mobile device to communicate with a computing device or connect to a power source via a USB connection.

XII. GROUND 4: CLAIM 7 IS OBVIOUS OVER TOOMER, GRIGG, HAMMAD, CASEY, AND LIN

A. Claim 7:

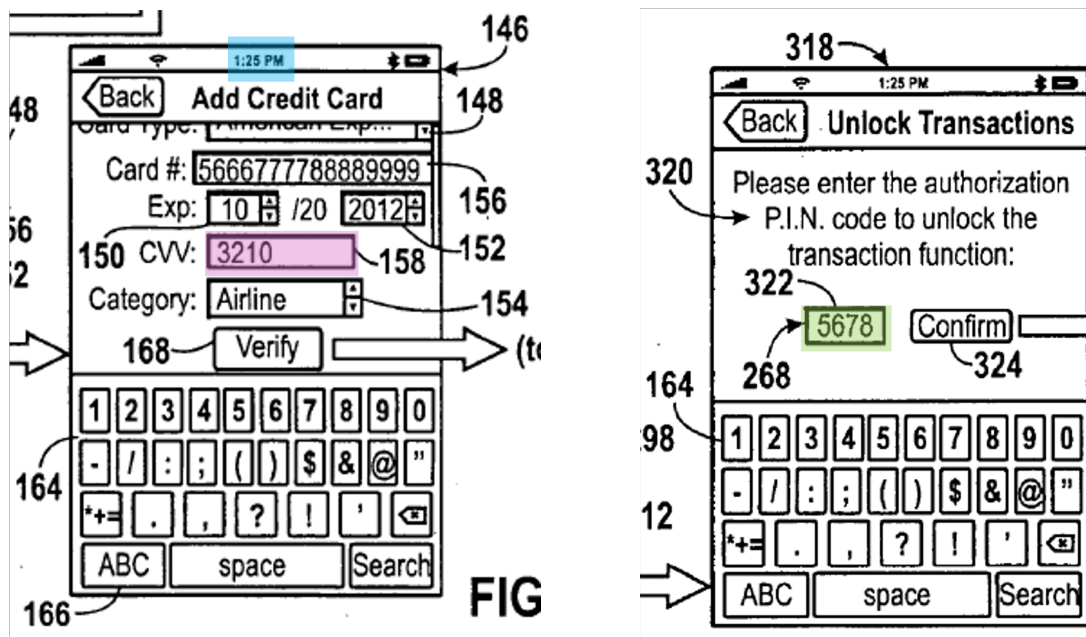
1. ***7. The electronic device of claim 1, wherein the display enables information to be displayed regarding the limited-use number, the time, a passcode, a sequence code, a currency amount, and other credit card transaction information of the user, a merchant, a bank or a credit card authority.***

a) Toomer and Grigg’s Teachings

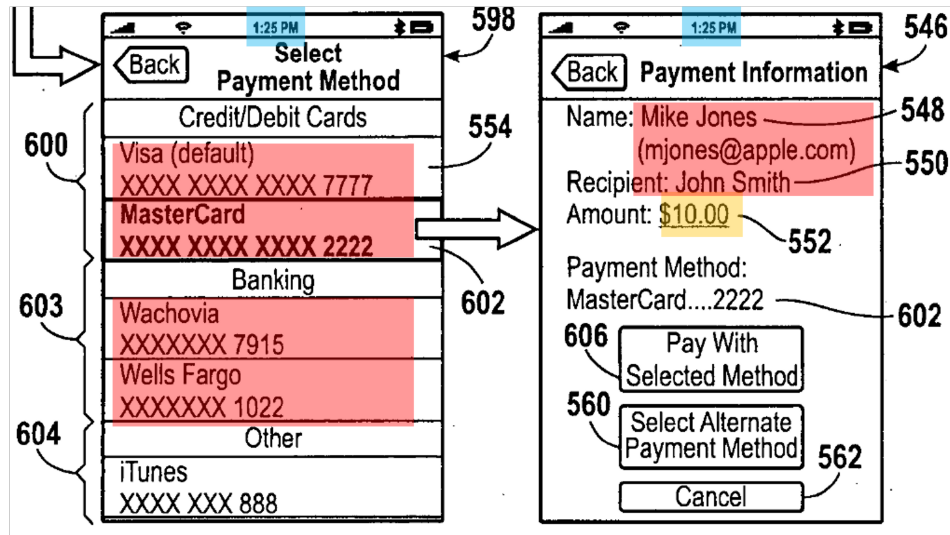
217. Toomer teaches a mobile wallet application on a mobile device that allows for entry, display, and selection of an account for a particular transaction. *Toomer (EX1004)*, [0052]. Alternatively, in combination with Grigg, this includes accepting user input and displaying information associated with adding card information to a user device and displaying a mobile wallet account number (*limited-use number*). *See* Claims 10(a), 10(d), 11, 14-15.

b) Lin's Teachings

218. Lin also teaches displaying information associated with registering a card with a mobile device and conducting an NFC transaction with a selected account, including entering a PIN to access the payment application. *Lin (EX1008)*, 37:20-25, 38:17-39:31, 40:19-24, 41:1-24, 52:1-13, 71:7-72:17, 73:4-17, Figs. 5A, 10B, 14E. As seen below, displayed information in these processes includes the account number, time (blue), PIN (passcode) (green), CVV (sequence code) (purple), currency amount (orange), and other credit card transaction information of the user, a merchant, a bank or a credit card authority (red).



Lin (EX1008), Figs. 5A, 10B.



Lin (EX1008), Fig. 14E.

c) Motivation to Combine

219. A POSITA would have found it obvious and been motivated to display user and transaction information on the touchscreen display of Toomer's mobile device. A POSITA would have understood that prior to the time of the alleged invention, the use of smart phones with touchscreen displays, as described in Lin, was prevalent. It was well-known that such a device could display various pieces of information related to entering card information and a payment transaction, as discussed in Claims 14 and 15. Toomer recognized that such information would be displayed on a touchscreen, e.g., to allow for user selection of payment method, and Lin expanded on this recognition by detailing further information that could be displayed.

220. A POSITA would have been motivated to combine Lin with Toomer to allow for the display of this information. Providing this information was commonplace at the time and would have benefited the user experience to guide the user through the transaction process.

221. A POSITA would have had a reasonable expectation of success in combining Lin's display of specific information on Toomer's display, which also displays related information, as a combination of known elements that would yield predictable results of user satisfaction and convenience in performing a transaction. Like Toomer, Lin describes using the mobile device to conduct a transaction via NFC. *Lin (EX1008)*, Abstract, 3:29-4:5, 15:5-9, 31:1-15, 31:29-32:10, 56:28-57:27, 59:16-60:2, 68:10-70:27, Figs. 3, 12A-B, 13, 14B-D, 15B.

222. A POSITA would have appreciated that modifying Toomer to display additional information to conduct a transaction, as taught by Lin, is a natural extension of the teachings in Toomer that would have further enhanced the user experience in conducting a transaction. In the combined system, Toomer would display on its touchscreen display the information depicted in Lin.

XIII. GROUND 5: CLAIMS 1-2 ARE OBVIOUS OVER TOOMER, GRIGG, HAMMAD, AND MULLEN '760

A. Claim 1

1. 1(pre)-(c), (e)-(n):

223. I discuss these limitations in Ground 3, Claim 1 (pre)-(c), (e)-(g); Ground 1, Claim 10(a-g).

2. 1(d): a motion rate detection array;

a) Toomer's Teachings

224. Toomer discloses that its mobile device may be a smart card. *Supra*, Ground 3, Claim 1(a); *Toomer (EX1004)*, [0002], [0023] (“[A] mobile device can include ... a smart card or other contactless device” and incorporating by reference application entitled, “Mobile Payment Device with Magnetic Stripe”); *see also* Claim 1(pre). Smart cards for conducting payment transactions were well-known prior to 2012. *See EX1024 (Finkenzeller)*, pp. 4-6, 240-266, 361-362; *EX1058 (U.S. Publn. No. 2013/0087627 to Marseille)*; *EX1043 (U.S. Publn. No. 2011/0140841 to Bona)*; *see also* Sections VI.A-B.

b) Mullen 760's Teachings

225. Mullen '760 teaches a smart credit card capable of communicating payment information (e.g., dynamic credit card number) for a transaction through a magnetic stripe or in a contactless manner. *Mullen '760 (EX1010)*, [0002]-[0003] (“This invention relates to payment cards such as credit cards. ... A card is provided

with a dynamic number. For example, a payment card, such as credit card, is provided with a dynamic payment card number, such as a dynamic credit card number. A dynamic credit card number may, for example, change based on time or use.”), [0016], [0021] (“A card is provided, such as a credit card or security card, that may transmit information to a magnetic stripe reader via a dynamic magnetic communications device such as a magnetic emulator or a magnetic encoder.”), [0023], [0245], [0300]-[0301], Figs. 11, 22. The credit card can include inertial movement sensors, such as one or more accelerometers, that detect “the swiping motion of a card.” *Mullen ‘760 (EX1010)*, [0019], [0245] (“Inertial movement sensor 1120 may be included to detect a swipe in order to initiate one or more emulators. Inertial movement sensor 1120 may include, for example, any number of accelerometers and/or gyroscopes.”). A POSITA would have understood that using multiple accelerometers, as taught by Mullen ‘760, is an array of accelerometers that detect the swiping motion of a card. Mullen ‘760 also teaches a plurality of inductor coils and companion magnetic-field pickup coils and an optical sensor array, as I discuss in Claim 2 below. *See* Claim 2. The ‘520 Patent describes that a motion rate detection array may include a plurality of accelerometer, a plurality of inductor coils and companion magnetic-field pickup coils and an optical sensor array.

226. Mullen ‘760’s inertial movement sensor may “detect a swipe in order to initiate one or more [magnetic] emulators.” *Mullen ‘760 (EX1010)*, [0245]. “[T]he

swiping motion of a card may be detected via one or more inertial sensors such as accelerometers and/or gyroscopes.” *Mullen '760 (EX1010)*, [0019]. The magnetic emulators are operable to communicate payment information to a reader, such as “a dynamic security code [and] a dynamic card number to authorize a payment transaction.” *Mullen '760 (EX1010)*, [0013]; *see also*, [0016], [0021], [0023].

c) Motivation to Combine

227. It would have been obvious in view of *Mullen '760* and a POSITA would have been motivated to include *Mullen '760*'s motion sensing device in Toomer's smart card. A POSITA would have appreciated that smart cards at the time of the '520 Patent often included inertial sensor arrays including accelerometers. For example, U.S. Patent No. 8,909,138 to Rhelimi describes a contactless card that includes an accelerometer that is “made to provide information about the movement of the wireless mobile communication device in space.” *EX1059 (Rhelimi)* at 1:9-15, 5:31; *see also* 3:63-67, Fig. 1. U.S. Publn. No. 2013/0087627 to Marseille similarly describes a smart card including an accelerometer. *EX1058 (Marseille)*, Abstract, [0029]. Moreover, a POSITA would have understood that including an accelerometer array would have allowed Toomer's contactless device to interpret user motions to initiate a transaction, as taught by *Mullen '760*. Providing more than one way to initiate transactions would have enhanced the user experience by making transaction initiation easier and more efficient. Thus, a POSITA would have been

motivated to combine prior art elements according to known methods to yield predictable results of increased user satisfaction and convenience.

B. Claim 2

1. ***2. The electronic device of claim 1, wherein the motion rate detection array comprises a set of motion rate detection units, wherein the set comprises: a plurality of inductor coils and companion magnetic-field pickup coils; an optical sensor array; and a plurality of accelerometers, and wherein a detected proximity between the electronic device and a second electronic device is determined from at least one of the set of motion rate detection units.***

228. Toomer-Grigg-Hammad-Mullen '760 discloses that a contactless device may include a plurality of accelerometers. *See* Ground 5, Claim 1(d). I understand that in the litigation, Patent Owner contends that Claim 2 is met by simply pointing to the “motion rate detection array” of Claim 1(d), without identifying of the specific components or functions required by Claim 2. *See* EX1060 (*EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520*), page 49 (mapping of Claim 2 referring back to limitation 1[d]), page 6 (mapping of Claim 1[d] pointing to gyroscope, accelerometer, or proximity sensor as the “motion rate detection array”). To the extent this apparent interpretation is correct, Toomer, as modified in view of Mullen '760's teachings in Ground 5, Claim 1(d), render Claim 2 obvious. Nonetheless, as described below, the combination in view of Mullen '760 renders all the limitations of Claim 2 obvious.

229. Mullen '760 also teaches that its card includes a plurality of inductor coils and companion magnetic-field pickup coils and an optical sensor array.

a) Mullen 760's Teachings

230. Mullen '760 teaches that “a magnetic emulation circuit may be provided as ... a coil.” *Mullen '760 (EX1010)*, [0037]. The magnetic emulation circuits generate electromagnetic fields by providing current through the coils to transmit information, such as payment information, to a magnetic stripe reader.

A magnetic emulator may be provided on a card (e.g., a credit or debit card). Such a magnetic emulator may include one or more wires that are able to produce an electromagnetic field that is operable to be read by, for example, a magnetic stripe reader. The magnetic emulator may be provided about a magnetic stripe and may be utilized to produce an electromagnetic field such that, for example, a magnetic stripe reader may seamlessly read a portion of the magnetic stripe, then read fields generated from the magnetic emulator, then read another portion of the magnetic stripe. In doing so, for example, only particular information related to an account (e.g., all or a portion of a credit card number) may be communicated via a magnetic emulator and, as such, may be operable to be changed.

Mullen '760 (EX1010), [0007]; *see also* [0028], [0036]-[0041], [0088], [0240], [0247], [0295], [0302], [0305], [0348] (“a magnetic emulator (or multiple magnetic emulators) may magnetically communicate financial data”).

231. A card may include multiple magnetic emulators (i.e., coils) that “span the length of a track” where “each emulator may provide different track information” to different read-heads. *Mullen* ‘760 (*EX1010*), [0030] (“More than one emulator may be provided on a card or other device and a processor may drive such emulators in a variety of different manners.”), [0302] (“Card 2250 may be provided and may include static magnetic track 2253, magnetic emulators 2251 and 2252, and magnetic read-heads 2254-2257”), [0347] (“Circuit 4300 may also include, for example, magnetic emulation circuits 4310, 4320, and 4330.”), [0354], [0362], Figs. 22-23, 43 (elements 4310, 4320, 4330), 44, 51 (elements 5170, 5180, 5185); *see also* [0035], [0253], [0354]-[0355], Figs. 44-45, 51. *Mullen* ‘760 further teaches that “multiple emulators ... may be utilized ... (e.g., one for each track)” and that “two arrays of magnetic emulators may be utilized ... each array located on a different end of the card.” *Mullen* ‘760 (*EX1010*), [0375], Fig. 53. The card also includes an RFID antenna and RFID field detector. *Mullen* ‘760 (*EX1010*), [0301], [0304]. A POSITA would understand an RFID antenna and/or field detector includes coils for magnetic-field pickup from an RFID reader. *Mullen* ‘760 further teaches an emulator may “communicate information (e.g., payment information that includes dynamic information) to an RFID receiver when an RFID field is present and to a magnetic stripe reader when a magnetic stripe is present.” *Mullen* ‘760 (*EX1010*), [0305]; *see also* [0029], [0308], [0321].

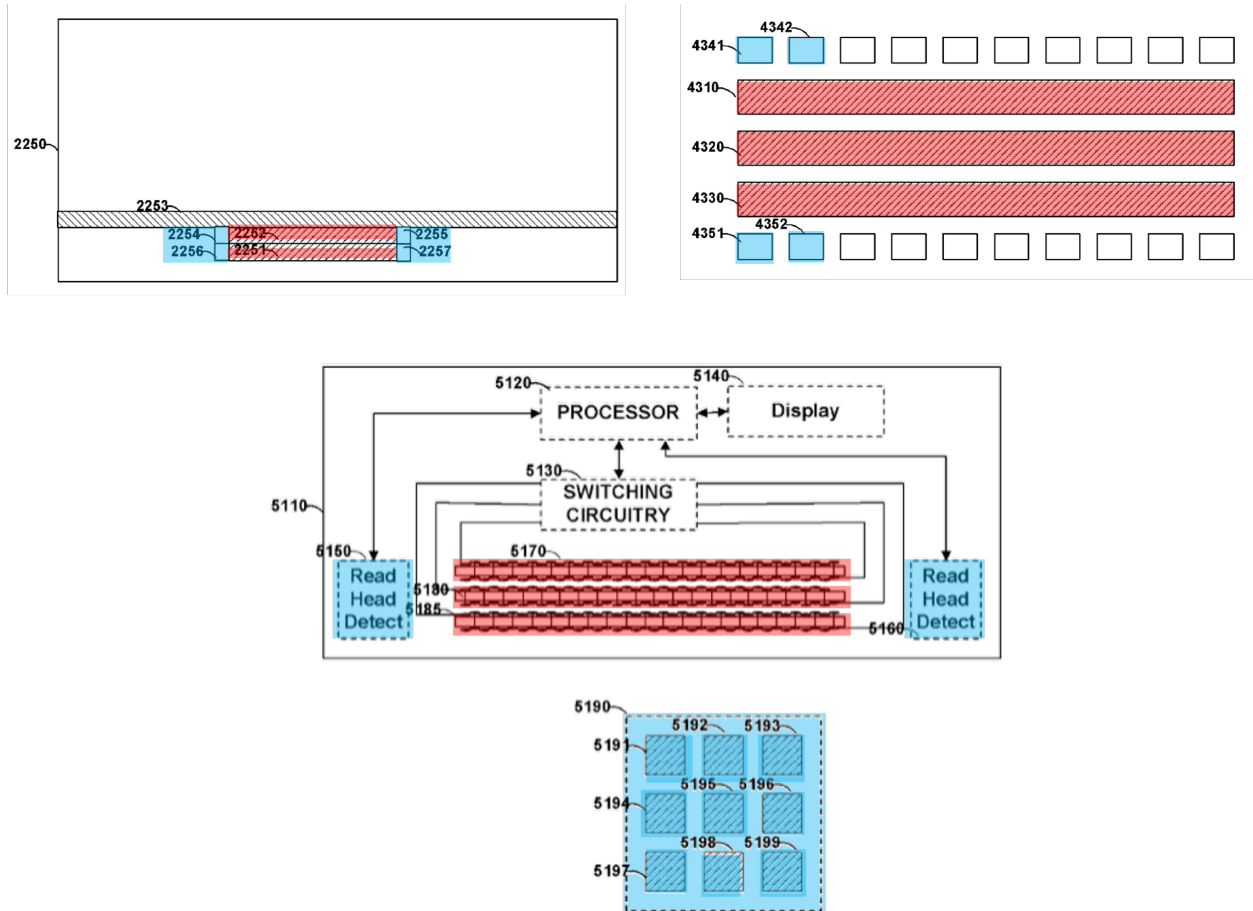
232. Additionally, portions of the emulator circuit coils “may be utilized to detect a read-head” such that the current in the electromagnetic field undergoes a phase-shift when a magnetic material (e.g., read-head) is placed in the field. *Mullen '760 (EX1010)*, [0037], [0041], [0339], [0341], [0365]. A POSITA would understand that when used in this way, the multiple emulator circuits act as a magnetic-field pickup coil, and when transmitting data to the read head would be an inductor coil (a plurality of inductor coils and companion magnetic-field pickup coils).

233. *Mullen '760* also teaches that a card includes a read-head detector for detecting a read-head of a magnetic stripe reader. *Mullen '760 (EX1010)*, [0338], Fig. 37; *see also* [0026], [0037], [0041]. *Mullen '760* further teaches an “array of read-head detectors” that “determine ... when a motorized reader was utilized, an insertion reader was utilized, or a user-swipe reader was utilized.” *Mullen '760 (EX1010)*, [0042]; *see also* [0048], [0245], [0302]-[0303], [0347], Figs. 22-23, 43. The read-head detector causes the magnetic emulator to transmit payment information to a read-head. *Id.*, [0256], [0305]. *Mullen '760* teaches that the card may include multiple read-head detectors 5150 and 5160. *Mullen '760 (EX1010)*, [0363], Fig. 51; *see also* [0338] (“Circuit 3700 may also include read-head detectors 3741, 3742, 3743, and 3744. Read-head detectors 3741, 3742, 3743, and 3744 may detect a read-head and/or a read-head housing of a magnetic stripe reader. Capacitive

coupling, sonar, optical, or any other technique may be utilized to determine the presence of a read-head or read-head detector. ... Multiple read-heads may be utilized, for example, to determine the direction that a read-head is moving as well as the read-heads velocity and/or acceleration.”). Each read-head detector may comprise a “cluster” of read-head detectors, including “optical” detectors “utilized to determine the presence of a read-head.” *Mullen '760 (EX1010)*, [0338], [0364], Fig. 51 (5190), Fig. 37; *see also* [0041], [0295]. Thus, a POSITA would understand that Mullen '760 teaches an “optical sensor array.” The read-head detectors allow a processor to determine that a user swiped the card through a particular reader, e.g., if the read-head detectors detect an object in a particular order it can know a particular reader is being used. *Mullen '760 (EX1010)*, [0364].

234. Accordingly, a detected proximity between the card (electronic device of Claim 1) and magnetic stripe reader's read-head (second electronic device) is determined by the optical detectors and/or emulator of the card (motion rate detection units) of the card.

235. Exemplary cards with multiple magnetic emulators (plurality of inductor coils and magnetic-field companion pickup coils) [annotated in red] and multiple read-head detectors (e.g., optic detectors) [blue] in a cluster (an optical sensor array) are depicted below:



Mullen '760 (EX1010), Figs. 22, 43, 51 (annotated).

b) Motivation to Combine

236. Alternatively, it would have been obvious and a POSITA would have been motivated to include Mullen '760's magnetic emulators and optical detector in Toomer's smart card. Based on Mullen '760's teachings, when using an optical detector as the read-head detector, the optical detector would determine that the read-head is being swiped in a particular reader. An emulator used as a read-head detector would similarly detect the presence of a particular read-head, as taught by Mullen '760. A POSITA would have understood that including these elements would have

allowed Toomer's contactless payment device to operate with various readers, such as in contactless and magnetic stripe transactions, as taught by Mullen '760. Providing more than one way to conduct transactions would have offered flexibility to a user where a merchant may have only a magnetic reader or contactless terminal, but not both. Thus, a POSITA would have been motivated to combine prior art elements according to known methods to yield predictable results of user convenience in performing a transaction with various types of readers.

XIV. GROUND 6: CLAIM 3 IS OBVIOUS OVER TOOMER, GRIGG, HAMMAD, MULLEN '760, AND GRIFFIN

A. Claim 3

- 1. 3. The electronic device of claim 2, wherein the plurality of accelerometers generate an indication of the detected proximity in response to a contact between said electronic device and said second electronic device.***

237. Mullen '760 teaches that the accelerometers “detect a swipe in order to initiate one or more emulators.” *Mullen '760 (EX1010)*, [0245]. The emulator “may be driven to electrically couple with an RFID receiver” and “communicate information (e.g., payment information that includes dynamic information) to an RFID receiver when an RFID field is present.” *Mullen '760 (EX1010)*, [0305], Fig. 25; *see also*, [0029]-[0030], [0321], Fig. 29.

238. I understand that in the litigation, Patent Owner contends that Claim 3 is met for the same reasons as Claim 2, i.e., by pointing to the “motion rate detection

array” of Claim 1(d), without identifying the specific components or functions required by Claim 3. See EX1060 (*EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520*), page 49 (mapping of Claim 3 referring back to Claim 2 which refers to limitation 1[d]), page 6 (mapping of Claim 1[d] pointing to gyroscope, accelerometer, or proximity sensor). To the extent this apparent interpretation is correct, Toomer, as modified in view of Mullen ’760’s teachings in Ground 5, Claim 1(d), render Claim 3 obvious. Alternatively, Claim 3 is obvious in further view of Griffin.

239. Nonetheless, as described below, the proposed combination in view of Griffin renders the limitations of Claim 3 obvious.

a) Griffin’s Teachings

240. Griffin teaches mobile devices that use NFC, such as those involving payment. *Griffin (EX1011)*, [0001], [0003]. The mobile device includes an accelerometer, such as a 3-axis accelerometer. *Griffin (EX1011)*, [0049]-[0050]. A POSITA would understand a three-axis accelerometer includes an array of three accelerometers measuring accelerations in the X, Y, and Z axes. See ¶¶195-197. “The accelerometer 137 recognizes the tapping of a communications device against ... another device, i.e., recognizes the vibrations.” *Griffin (EX1011)*, [0049]. “[W]hen the device is tapped against another object,” the NFC circuit is woken up

and communication is initiated. *Griffin (EX1011)*. Thus, the accelerometers generate an indication of the proximity of the mobile device to another device.

b) Motivation to Combine

241. It would have been obvious to use Mullen '760's accelerometers in a similar way as described in Griffin to generate an indication that the smart card is in proximity to a reader. In the combination, Mullen '760's emulator would be initiated upon the accelerometers detecting the card and a reader are in close proximity. This is a natural application of Griffin's teachings to Mullen '760's device and POSITA would understand it would implement Mullen '760's teachings relating to using the inertial movement sensor to initiate one or more emulators. This modification would have allowed the card to conserve power by only being power up when the accelerometer indicates that the card is in proximity to a reader. Thus, a POSITA would have been motivated to combine such prior art elements to improve similarly systems according to known methods to yield the predictable result of increased options and user experience in performing a transaction.

XV. CONCLUSION

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

Declaration of Dr. Clifford Neuman
U.S. Patent No. 11,176,520

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.