

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
Patent No. 10,339,520

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,339,520, CLAIMS 1-17**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	SUMMARY OF THE '520 PATENT.....	1
A.	BRIEF DESCRIPTION	1
B.	FIELD OF ENDEAVOR AND PROBLEM SOLVED BY THE INVENTORS	3
C.	PRIORITY AND PROSECUTION HISTORY	3
D.	LEVEL OF SKILL OF A POSITA	4
III.	REQUIREMENTS UNDER 37 C.F.R. § 42.104	5
A.	GROUND FOR STANDING UNDER 37 C.F.R. § 42.104(A).....	5
B.	IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B)	5
C.	CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3).....	6
IV.	SHOWING OF ANALOGOUS, PRIOR ART	7
A.	TOOMER.....	7
B.	GRIGG	8
C.	HAMMAD	9
D.	MULLEN '449.....	9
E.	LIN.....	9
F.	CASEY.....	10
G.	MULLEN '760.....	11
H.	GRIFFIN.....	11
I.	ANALOGOUS ART.....	11
V.	GROUND 1: CLAIMS 10-13 ARE OBVIOUS OVER TOOMER, GRIGG, AND HAMMAD	12
A.	CLAIM 10	12
1.	<i>10(pre): A method of storing and generating payment information in an electronic device, the method comprising:</i>	<i>12</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>13</i>
	a) Toomer's Teachings	13
	b) Grigg's Teachings	16
	c) Motivation to Combine	16
3.	<i>10(b): wherein the electronic device comprises device-specific and user-specific information; and, ...</i>	<i>18</i>
4.	<i>10(c): wherein the issuer provided payment information is communicated wirelessly; and, ...</i>	<i>19</i>
5.	<i>10(d): receiving wirelessly a static device account number payment information for storage on the electronic device;.....</i>	<i>20</i>
	a) Toomer's Teachings	20
	b) Grigg's Teachings	21
	c) Motivation to Combine	23
6.	<i>10(e): and wherein.....</i>	<i>27</i>
	at least a portion of the payment information [for making a transaction] is a limited-use number for limited use by the device, in place of a issuer provided payment information; and, ...	27
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>28</i>
	a) Toomer's Teachings	28
	b) Hammad's Teachings	29
	c) Motivation to Combine	30
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>33</i>

B.	CLAIM 11	34
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 means comprising: a touch sensor array; a touch screen; a keypad; buttons;</i>	34
C.	CLAIM 12	35
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>	35
D.	CLAIM 13	36
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>	36
VI.	GROUND 2: CLAIMS 14-17 ARE OBVIOUS OVER TOOMER, GRIGG, HAMMAD, MULLEN '449, AND LIN	37
A.	CLAIM 14	37
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>	37
a)	Toomer's Teachings	37
b)	Mullen '449's Teachings.....	38
c)	Motivation to Combine	39
B.	CLAIM 15	40
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</i>	

	<i>payment method images rendered [on] the display and using a touch screen interface for the user selection.</i>	<i>40</i>
	a) Toomer's Teachings	40
	b) Mullen '449's Teachings.....	41
	c) Motivation to Combine	41
C.	CLAIM 16	42
1.	<i>16. The method of claim 15, wherein the user selection is a default payment method to be used in transactions.....</i>	<i>42</i>
	a) Toomer's Teachings	42
	b) Lin's Teachings	42
	c) Motivation to Combine	43
D.	CLAIM 17	43
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>43</i>
VII.	GROUND 3: CLAIMS 1, 4-6, 8-9 ARE OBVIOUS OVER TOOMER, CASEY, GRIGG, AND HAMMAD	44
A.	CLAIM 1	44
1.	<i>1(pre): An electronic device comprising:</i>	<i>44</i>
2.	<i>1(a): a near-field communication (NFC) unit;</i>	<i>45</i>
3.	<i>1(b): a touch sensor array;</i>	<i>45</i>
4.	<i>1(c): a display;</i>	<i>46</i>
5.	<i>1(d): a motion rate detection array;</i>	<i>47</i>
	a) Toomer's Teachings	47
	b) Casey's Teachings	47
	c) Motivation to Combine	49
6.	<i>1(e): a memory for storing a user data and a currency amount;</i>	<i>49</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>50</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>	51
9.	<i>1(h)-(n):</i>	52
B.	CLAIM 4	52
1.	<i>4. The electronic device of claim 1, wherein the user input comprises one or more of:</i>	52
	<i>an introduction of a transaction-specific identifier;</i>	52
	<i>a confirmation or a denial of an indicated transaction; and</i>	52
	<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>	52
	a) Casey's Teachings	52
	b) Motivation to Combine	53
C.	CLAIM 5	54
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>	54
D.	CLAIM 6	55
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>	55
E.	CLAIM 8	56
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>	56

a)	Hammad’s Teachings	56
b)	Motivation to Combine	56
F.	CLAIM 9	57
1.	<i>9. The electronic device of claim 1, further comprising a USB connector for connection to a standard computing device.</i>	57
VIII. GROUND 4: CLAIM 7 IS OBVIOUS OVER TOOMER, GRIGG, HAMMAD, CASEY, AND LIN		
A.	CLAIM 7:	57
1.	<i>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.</i>	57
a)	Toomer and Grigg’s Teachings	58
b)	Lin’s Teachings	58
c)	Motivation to Combine	59
IX. GROUND 5: CLAIMS 1-2 ARE OBVIOUS OVER TOOMER, GRIGG, HAMMAD, AND MULLEN ’760		
A.	CLAIM 1	61
1.	<i>1(pre)-(c), (e)-(n):</i>	61
2.	<i>1(d): a motion rate detection array;</i>	61
a)	Toomer’s Teachings	61
b)	Mullen 760’s Teachings	61
c)	Motivation to Combine	62
B.	CLAIM 2	63
1.	<i>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</i>	

	<i>between the electronic device and a second electronic device is determined from at least one of the set of motion rate detection units.</i>	63
	a) Mullen 760’s Teachings	64
	b) Motivation to Combine	67
X.	GROUND 6: CLAIM 3 IS OBVIOUS OVER TOOMER, GRIGG, HAMMAD, MULLEN ’760, AND GRIFFIN	67
A.	CLAIM 3	67
1.	<i>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.</i>	<i>67</i>
	a) Griffin’s Teachings	68
	b) Motivation to Combine	69
XI.	DISCRETION UNDER 35 U.S.C. § 325(D).....	69
XII.	CONCLUSION.....	69
XIII.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8	71
A.	REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1).....	71
B.	RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2)	71
C.	LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3).....	71
D.	37 C.F.R. 42.8(B)(4) – SERVICE INFORMATION.....	72

I. INTRODUCTION

Apple Inc. (“Petitioner” or “Apple”) respectfully requests *inter partes* review (“IPR”) of claims 1-17 (“Challenged Claims”) of U.S. Patent No. 10,339,520 (“’520 patent”).

II. SUMMARY OF THE ’520 PATENT

A. Brief Description

The ’520 patent describes an electronic payment card capable of generating a “**limited-duration number**”¹ for use in a payment transaction. ’520 Patent, 2:24-29, 2:49-62, 10:3-11-55. Figure 7 depicts a process for generating and using a limited-duration number in a transaction:

¹ All emphasis added unless otherwise noted.

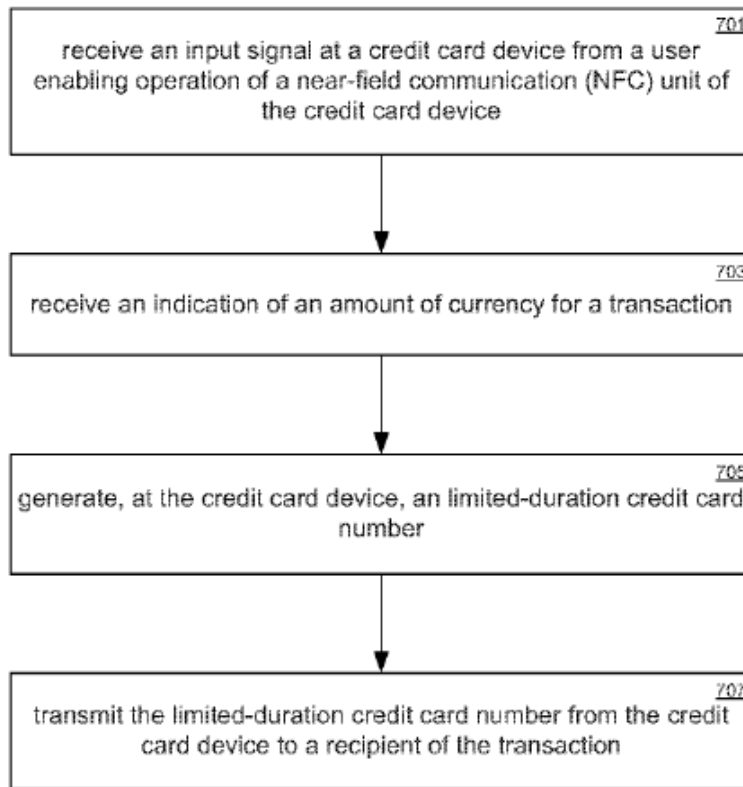


FIG. 7

'520 Patent, Fig. 7.

“The limited duration credit card number is able to be produced at the time the credit card device is performing a transaction, and is able to be generated according to the user’s private information, a bank information, information regarding the facility performing the transaction, and the time of day.” *Id.*, 10:13-23. The specification further discusses how “the number on the front of the card” can be static, dynamic, or a combination of static and dynamic digits. *Id.*, 10:32-52. In some cases, the disclosed credit card device is used to conduct transactions with an automated teller machine (ATM). *Id.*, 11:16-26, 12:44-53, 14:59-60.

B. Field of Endeavor and Problem Solved by the Inventors

The claimed invention of the '520 Patent relates to at least electronic or smart card devices. '520 Patent, 1:26-28, 2:14-31. These smart credit card devices are configured to “emulate behavior of a credit card” for use in financial transactions. '520 Patent, 2:14-24. Therefore, the field of endeavor includes at least smart payment devices. *Dec.*, ¶34.²

The '520 Patent is reasonably pertinent to the problem of security in financial transactions. '520 Patent, 1:32–2:4. *Dec.*, ¶35. Existing credit card device types include the conventional credit card, the card with an integrated chip, and the card with radio frequency identification (“RFID”) technology. '520 Patent, 1:32-62. These cards “have security limitations” and are each “susceptible to theft and/or compromise.” *Id.*, 1:63-67. The '520 Patent proposes to solve this problem by generating “a limited-duration credit card payment number for performing transactions using accounts of [the credit card device]” as an added security feature. *Id.*, 2:24-29, 10:4-7, 12:11-15.

C. Priority and Prosecution History

The '520 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. Because the '520 Patent claims the benefit of a filing date before March 16, 2013, Petitioner applies the pre-AIA versions of §§ 102, 103. For

² Citations to “*Dec.*” are to EX1003, Declaration of Dr. Neuman.

this proceeding, Petitioner applies March 15, 2013, as the priority date for the Challenged Claims.³ Unless noted, the below analysis would not change under the AIA.

The only rejection made during original examination was based on statutory double patenting. '520 *Patent File History* (EX1002), 69. The applicant responded to the rejection by substantially amending independent claim 1 and adding new claims 10-24. *Id.*, 107-121. No further rejections ensued, and the application was ultimately allowed after minor amendments. *Id.*, 134-141, 176-180, 200. The file history includes no indication that Examiner considered any of the prior art cited in this Petition. If this art had been considered—and particularly the combinations described in Grounds 1-4—the application never should have been allowed.

D. Level of Skill of a POSITA

A person of ordinary skill in the art (POSITA) at the time of the '520 Patent would have been a person having a bachelor's degree in computer science, computer engineering, electrical engineering, or a similar technical field, and one or two years

³ Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Unless specifically noted, the analysis presented in this petition remains the same regardless of whether March 15, 2013, or some later date is used as the Critical Date.

of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless and online technologies. *Dec.*, ¶¶28-29. 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. *Id.*

III. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies the '520 Patent is eligible for IPR.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b)

Petitioner requests the Challenged Claims be found unpatentable on the following grounds under 35 U.S.C. § 103:

Ground	Claim(s)	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, Casey (EX1009), Grigg, and Hammad
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 (EX11)

The earliest claimed priority date of the '520 Patent is March 15, 2013 (the “Critical Date”). Each of the prior art references applied in this Petition qualifies as prior art to the '520 Patent as shown:

Reference	Filed	Published	Issued	Prior Art Basis
Toomer	2/15/2008	8/20/2009	—	§102(b)
Grigg	6/28/2012	1/2/2014	—	§102(a)/(e)
Hammad	6/18/2007	—	6/22/2010	§102(b)
Mullen '449	5/10/2012	11/15/2012	—	§102(a)/(e)
Lin	8/11/2009	4/8/2010	—	§102(b)
Casey	1/9/2009	—	8/28/2012	§102(a)/(e)
Mullen '760	12/24/2008	7/2/2009	—	§102(b)
Griffin	9/24/2009	3/24/2011	—	§102(b)

None of these references were cited or discussed during prosecution of the '520 Patent.

C. Claim Construction Under 37 C.F.R. § 42.104(b)(3)

In this proceeding, claims are interpreted under the same standard applied by Article III courts (the *Phillips* standard). 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). For all terms not included below, Petitioner applies the ordinary and customary meaning of the claim terms as understood by a POSITA.⁴

For purposes of this proceeding only, Petitioner adopts the following constructions, proposed by Patent Owner in the underlying litigation. EX1012.

Claim language	Patent Owner's Construction
Claim 1: "the payment information"	"payment information for making a payment transaction"
Claim 15: "rendered the display"	"rendered on the display"

⁴ Petitioner's application of prior art to the Challenged Claims is not a waiver of any argument in litigation that any claim term in the '520 Patent is indefinite or invalid.

Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board.

IV. SHOWING OF ANALOGOUS, PRIOR ART

A. Toomer

Toomer describes an “electronic device that can be used to initiate or otherwise participate in a financial transaction.” *Toomer*, [0023]. The electronic device, specifically mobile device 324, is adapted to store and execute a mobile wallet application. *Id.*, [0024], [0052]. The mobile wallet application stores and maintains electronic payment credentials, i.e., information related to financial accounts of a user. *Id.*, [0052], [0063]. The user is able to select a 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. *Id.*, [0063]. The mobile device communicates with the POS device using wireless technology, such as near field communications (“NFC”). *Id.*, [0051]. Thus, the “mobile device 324 may be used ... instead of a card or other token representing an account.” *Id.*, [0051].

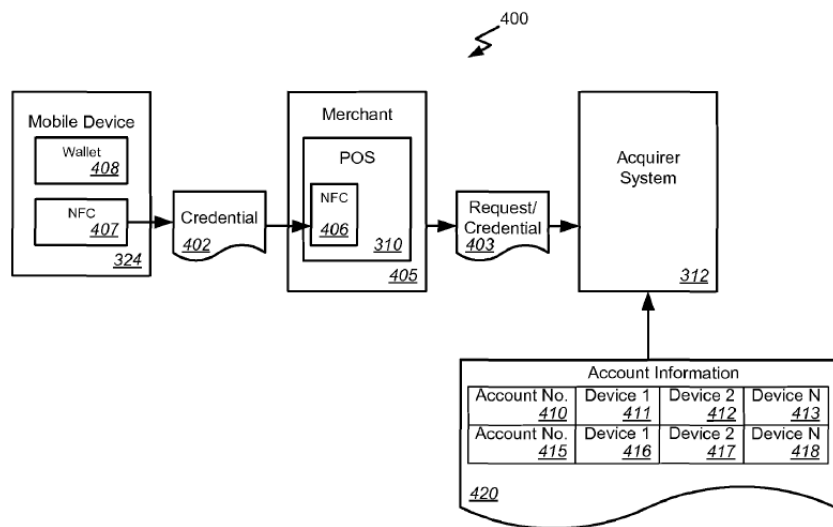


FIG. 4

Id., Fig. 4 (illustrating details of a system for processing financial transactions using mobile device 324).

B. Grigg

Grigg describes 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*, [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*, [0002], [0006]. Grigg notes that each payment device has a “different mobile wallet account number[.]” *Grigg*, [0011], [0003] (“[A] mobile wallet is typically associated with the individual’s mobile device[.]”). A financial institution “provide[s] the user 202 via the user

device 204 the assigned mobile wallet account number.” *Grigg*, [0053]. This mobile wallet number “may be permanently associated with the mobile wallet” *Grigg*, [0051].

C. Hammad

Hammad describes methods and systems for generating verification values on a portable device for use in a payment transaction. *Hammad*, 2:10-20, 2:65–3:11. The dynamically generated verification values are generated using two or more dynamic data elements and static data elements and embedded in payment data sent to a service provider. *Hammad*, 4:21-6:42.

D. Mullen ’449

Mullen ’449 describes a system to “generate a mobile wallet of virtual cards” on a mobile device, such as a cell phone, for use in payment transactions. *Mullen ’449*, Abstract, [0003], [0021], [0053]. The mobile device stores information from physical payment cards by communicating with the cards via a contactless communication channel, for example, RFID technology. *Id.*, [0003]-[0004], [0009]. The virtual cards are rendered onto a mobile device display, including each card’s particular card and cardholder information. *Id.*, [0009], [0010], Fig. 11. Thus, a user may convert her entire physical wallet or purse “into a virtual equivalent [] that resides electronically within the mobile device.” *Id.*

E. Lin

Lin describes “electronic devices configured to initiate and process” financial

transactions, including using near field communications (“NFC”). *Lin*, Abstract, 1:6-8, 3:29-4:5. Before initiating a payment transaction, a user may enter credit card information for one or more accounts into an application on the device (a “transaction application”), the information being verified by the card issuer and stored on the portable device. *Id.*, 3:2-6, 37:16-22, 38:17-39:31, 40:19-42:2, Figs. 5A-5B. The credit card information includes card number, expiration date, and CVV values. *Id.*, 31:25-32:6, 37:16-20, 40:19-28. The portable device initiates payments by transmitting payment information to another device using the transaction application. *Id.*, 3:16-22, 14:22-25, 20:4-9, 31:16-28, 55:7-56:5, Figs. 1 (ref. no. 34), 11B. *Lin* also describes the transaction application as providing for a “user-specified preferred or default payment account or source[.]” *Id.*, 25:22-27, 47:1-2, Fig. 7.

F. Casey

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

confirming (or declining) a transaction. *Id.*, 18:19-67, Figs. 12-13.

G. Mullen '760

Mullen '760 describes electronic credit cards that generate dynamic information for use in a financial transaction. *Mullen '760*, [0002]-[0007], [0016], [0198]-[0200]. The dynamic information may be a dynamic credit card number, verification code, or security number. *Id.*, [0023], [0033]-[0034], [0231]-[0232], [0261]-[0262]. A remote server verifies the payment information, including the dynamic information. *Id.*, [0231]-[0232], [0261]-[0262], [0292].

H. Griffin

Griffin teaches mobile devices that use NFC to interact, such as those involving payment. *Griffin*, [0001], [0003]. When an NFC connection is established between two devices, data, such as security codes, IDs or PINs, are exchanged. *Id.*, [0023], [0039].

I. Analogous Art

Each of the applied prior art references discloses conducting secure payment transactions and is in the same field of endeavor as the '520 Patent. *Compare '520 Patent*, Abstract, 1:26-28, Fig. 1 *with Toomer*, Abstract, [0001], [0004]-[0008], Fig. 7; *Grigg*, Abstract, [0005]-[0006], Fig. 1; *Hammad*, Abstract, 2:12-20, Fig. 6; *with Mullen '449*, [0003]-[0005]; *Lin*, Abstract, 3:16-4:5, Figs. 1, 3-4, 11A-B; *Casey*, Abstract, 1:6-9, 3:10-19; *Mullen '760*, Abstract, [0002]-[0005], [0016], [0021]-[0034], Figs. 1, 6-7; *Griffin*, Abstract, [0001], [0003]; *Dec.*, ¶¶92-113.

Further, each of the applied prior art references is reasonably pertinent to problems addressed by the '520 Patent such as increasing security of payment transactions. *Compare '520 Patent*, 1:26-28, 1:63–2:4, 9:9-15 *with Toomer*, Abstract, [0004], [0024], [0038]; *Grigg*, [0003]-[0004], [0008], [0048]; *Hammad*, 1:17-2:6; *Mullen '449*, [0008], [0091]; *Lin*, 26:27–27:14; *Casey*, 3:35-37, 10:35-46, 17:15-38; *Mullen '760*, [0210], [0299]; *Griffin*, [0003], [0037]; *Dec.*, ¶¶92-113.

V. 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:

Toomer teaches methods and systems for “authorizing financial transactions initiated by or otherwise involving the use of a contactless or mobile device.” *Toomer*, [0019], [0038]. A “mobile device” may be “any small, likely handheld, electronic device that can be used to initiate or otherwise participate in a financial transaction[,]” including cellular telephone, PDA, smart card or other contactless device. *Toomer*, [0023].⁵ Toomer’s mobile device “can store and/or execute a mobile wallet application adapted to maintain account numbers and/or other information, i.e., electronic payment credentials, related to one or more financial accounts” (e.g., such as credit or debit accounts) “maintained by one or more

⁵ Claim language identified with *italics* and underline for clarity.

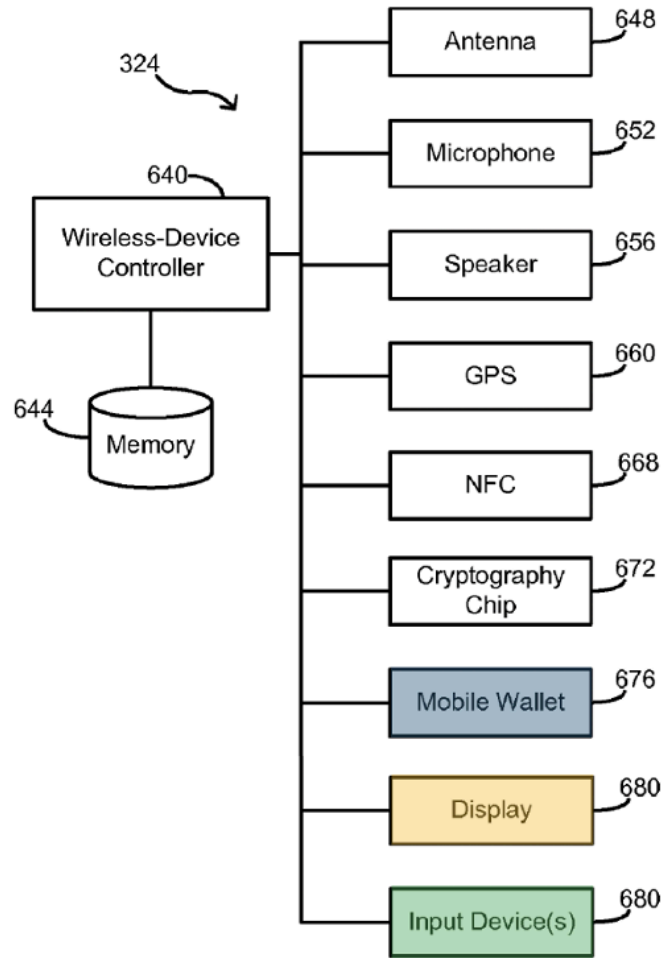
financial institutions 316-318.” *Toomer*, [0052]. The mobile wallet application “may store or generate a unique identifier for use by other systems in identifying one or more accounts associated with the mobile wallet.” *Toomer*, [0038], [0059]. Thus, *Toomer*’s mobile device executing a mobile wallet application to store and/or generate payment credentials and related information performs a method of storing and generating payment information in an electronic device, as described below.

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

Toomer teaches using a mobile wallet application on a mobile device (electronic device) “to maintain account information related to one or more financial accounts[,]” which may include “information such as a bank name, account number, account type, etc” (issuer provided payment information). *Toomer*, [0038], [0053]. The mobile wallet application can “store payment vehicle information, i.e., an electronic payment credential and/or other information identifying one or more financial accounts[,]” such as credit or debit accounts. *Toomer*, [0063]. A “payment vehicle” is a method of payment, such as a “credit, debit, stored-value” or other account. *Toomer*, [0027]. The mobile wallet allows “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*, [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[.]” *Id.*, [0003]. A POSITA would have understood that in order for Toomer’s mobile device to maintain information such as an account number, it would first need to be entered into the device using the touchscreen display. *Dec.*, ¶¶115-117. Thus, Toomer teaches or renders obvious a 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. *Dec.*, ¶115.



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

To the extent Patent Owner argues that *Toomer* does not teach “accepting a user input of issued payments information input[,]” it would have been obvious to modify *Toomer* to allow the mobile device to accept user input of payment account information when setting up accounts for the mobile wallet, as taught by *Grigg*.

b) Grigg's Teachings

Grigg teaches a user device (e.g., mobile phone or PDA) that includes a mobile payment application for a mobile wallet, which are similar to Toomer's mobile device and mobile wallet application. *Grigg*, [0005], [0043], [0070], Fig. 2. The mobile payment application on Grigg's user device mobile wallet stores in memory mobile wallet account numbers and payment device (e.g., credit card) account numbers. *Id.*, [0029], [0073], Fig. 2. The user application allows a user to add or "input payment devices onto his/her mobile wallet" by providing information associated with the payment device, e.g., credit card number, to a financial institution server. *Id.*, [0087], [0072], Figs. 3, 5; *see also*, [0008], [0048], [0078]-[0079]. The financial institution server receives and stores the payment device account numbers and associated mobile wallet account numbers. *Id.*, [0073]. Thus, Grigg teaches a mobile electronic device accepting a user input of issued payment information input comprising issuer provided payment information. *Dec.*, ¶¶118-119.

c) Motivation to Combine

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. *Dec.*, ¶120. Toomer even describes such manual entry of payment

information into an electronic device. *Toomer*, [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. *Dec.*, ¶¶120-122. A POSITA would have further found it obvious to allow for adding payment devices to Toomer's wallet application through the touchscreen. *Id.* 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. *Id.* Moreover, touchscreen input was well-known and predictable long before the '520 Patent, including for adding financial accounts to a transaction application. *Id.* Therefore, a POSITA would have been motivated to combine 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. *Id.* 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. *Id.*

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. Dec., ¶123.

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

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

Toomer teaches that mobile device 324 includes a memory comprising a unique static identifier. *Toomer*, [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[.]" *Id.*, [0059]. Per dependent claim 12 of the '520 Patent, "device-specific information" includes "device identifiers[.]" '520 Patent, 17:41-43.

Toomer also teaches that memory stores the payment vehicle information utilized by mobile wallet application. *Toomer*, [0024], [0027], [0063]. Payment vehicle information includes "information identifying one or more financial accounts such as credit accounts [or] debit accounts[.]" *Toomer*, [0063]. Toomer also teaches mobile device 324 storing "information such as a bank name, account number, account type, etc[.]" *Toomer*, [0038], [0053]. Per dependent claim 13 of the '520 Patent, "user-specific information comprises at least one of a set comprising: [. . .] **bank accounts; payment information**[.]" '520 Patent, 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. Dec., ¶¶125-126. Therefore, Toomer's teaches user-specific information.

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

Toomer teaches mobile device 324 being a cellular phone capable of “a cellular or other wireless communications service[.]” *Toomer*, [0022]-[0023]. Toomer similarly teaches that its system can include 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.” *Id.*, [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].” *Id.*, [0042]. The network 115 includes a “wireless network[.]” *Id.*, [0041].

Like Toomer, Grigg's 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*, [0087]. Similarly, Grigg teaches that “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.” *Id.*, [0072]. The network 201 is a “wireless” connection “between devices on the network[,]” e.g., the user device and financial institution server. *Id.*, [0042], Fig. 2.

For the reasons discussed with regard to 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. *See* Claim 10(a). This includes wirelessly communicating the issuer provided payment information. *Dec.*, ¶¶127-129.

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

a) **Toomer’s Teachings**

Toomer teaches the use of either “a **unique static identifier**” or “a unique dynamic identifier” as “information identifying the electronic device presenting the payment credential[.]” *Toomer*, [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.” *Id.*, [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. *Id.*, [0021]-

[0023].

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. *Id.*, [0038], [0052]-[0053], [0063].

b) Grigg’s Teachings

As discussed in Claim 10(c), Grigg teaches that a user device and financial institution server are wirelessly connected. *See* Claim 10(c); *Grigg*, [0042].

Grigg teaches that “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*, [0043]. 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*, [0006], [0047], [0051]. Grigg’s mobile wallet account number “may be permanently associated with the mobile wallet.” *Grigg*, [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*, [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*, [0006], [0011]. The mobile wallet number is provided by the

financial institution to the mobile wallet application of the device over a network.
Id., [0042], [0053].

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*, [0043], [0047], [0051]; *Dec.*, ¶¶132-135.

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

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[.]" *Id.*, [0073]. The financial institution server also stores the mobile wallet account number and associated payment device account numbers. *Id.* Grigg teaches that 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*, [0074], Fig. 6. 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) and stored on an electronic device. *Dec.*, ¶137.

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. *Dec.*, ¶139. Thus, Grigg's mobile wallet account number is static device account number payment information. *Id.*

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

c) Motivation to Combine

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, akin to Toomer's "unique identifier for use by other systems in identifying" an account. *Dec.*, ¶141; *Toomer*, [0038]. As noted by Grigg, 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*, [0002]-[0004]; *Dec.*, ¶141. Thus, this modification prevents bad actors from obtaining access to the actual account number if a user device is stolen. *Id.* A POSITA would have appreciated storing a mobile

wallet account number is safer than storing the actual account number on Toomer's device. *Id.* Thus, a POSITA would have been motivated to use Grigg's mobile wallet account number in place of Toomer's account number. *Dec.*, ¶142. Toomer even 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*, [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. *Dec.*, ¶142. 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. *Id.*

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 and a POSITA would have been familiar with using account number alternatives when making mobile payments. *Dec.*, ¶143. 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. *Id.*; *Grigg*, [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. *Id.*; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007).

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. *Dec.*, ¶144. A POSITA would recognize that the electronic device of Toomer could be beneficially modified to incorporate Grigg's mobile wallet number into device memory. *Id.*

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*, [0038]-[0039], [0052], [0063]; *Dec.*, ¶145. 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. *Id.* The mobile wallet account number would be used instead of the account number when making payment transactions, as taught by Grigg. *Grigg*, [0051]; *Dec.*, ¶145. 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. *Dec.*, ¶145.

This modification is a substitution of one known element for another predictably resulting in increased security of Toomer's payment system. *Dec.*, ¶146. 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 of increasing transaction security. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007); *Dec.*, ¶146.

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*, [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*, [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*, [0054], [0084], [0089]) and still receive the increased security benefits from not storing traditional account information. *Dec.*, ¶147. 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. *Id.*

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*, [0051]; *Dec.*, ¶148. It is also a more simple solution requiring less system resources. *Dec.*, ¶148. 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. *Id.*

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. *Dec.*, ¶149.

6. 10(e): and wherein

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

Grigg's mobile wallet account number is a limited-use number in that it is only able to be used by the device mobile wallet and is cancelled by the user if the

device is stolen. *Dec.*, ¶150. 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). *Dec.*, ¶150.

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***

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. *Dec.*, ¶150.

a) Toomer’s Teachings

Toomer teaches the mobile device stores payment credentials, which includes information representing an account (e.g., bank name, account number, account type, etc.). *Toomer*, [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.” *Id.*, [0038]. The payment credentials are used in authorizing a transaction. *Id.*, [0052]-[0054].

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*, [0002], [0062]; *Hammad*, 1:35-45, 3:60-67, 4:7-20; *Dec.*, ¶¶152-153.

b) Hammad's Teachings

Hammad describes dynamically generating a card verification value (“dCVV”) using a mobile device application for use in a mobile payment transaction. *Hammad*, 2:66-3:11, 3:51-4:6. Hammad teaches generating a dCVV from multiple dynamic and static data elements. *Id.*, 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.” *Id.*, 4:21-56, 4:61-7:3, Fig. 1. 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. *Id.*, 4:52-60, 5:2-5. The dCVV is generated by combining these data elements with multiple encryption keys, including a master derivation key, resulting in a 3-digit dCVV. *Id.*, 5:34-6:39, Figs. 1-3. The master derivation key is

provided by the service provider and used to generate the dCVV. *Id.*, 5:38-57, Fig. 2.

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*, 6:40-42, 6:49-7:28, 7:55-61, Figs. 4-5. The service provider uses the dCVV to determine the authenticity of the payment service. *Id.*, 7:29-38, 7:61-8:50, Fig. 6.

A dCVV is generated for “each transaction” and included with other payment data. *Id.*, 4:61-65; *see also id.*, 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. *Id.*, 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. *Dec.*, ¶156.

c) Motivation to Combine

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*. *Dec.*, ¶157.

Hammad recognizes the risk of fraud in using a static CVV in a contactless transaction. *Hammad*, 1:20-23, 1:35-45, 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*, 4:46-60. These 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. *Id.*, 4:21-5:5, 5:38-58.

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. *Dec.*, ¶159. Indeed, Hammad recognizes that only including one dynamic data element, such as a counter, is susceptible to fraud. *Hammad*, 1:66-2:4. Hammad, therefore, teaches including at least three or four dynamic data elements and static data elements (set of information). *Dec.*, ¶159. 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 this information for fraudulent purposes. *Id.* 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. *Id.*

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. *Dec.*, ¶160. This modification of known techniques would have yielded the predictable result of increasing security of the transaction. *Id.*

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 making mobile payments. *Dec.*, ¶161. 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. *Id.*; *Grigg*, [0051]. Such a modification is combining known prior art elements according to known methods to yield the predictable result of increased security. *Dec.*, ¶161; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007).

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 components is largely the same. *Dec.*, ¶162.

Thus, 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. *Dec.*, ¶163.

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.***

Toomer teaches completing a contactless financial transaction using a payment credential, which includes making “a request to authorize the transaction.” *Toomer*, [0006], [0039]. The mobile device transmits payment credentials to a financial institution, via a point-of-sale device and acquirer, during a transaction. *Toomer*, [0038]-[0039], [0051]-[0054], Fig. 4. The payment credentials include “information and/or credential related to a financial account in the mobile wallet[.]” *Toomer*, [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 the information or credential has been provided.” *Id.*, [0054].

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

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. *Dec.*, ¶166. 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 and Grigg. *Id.*; see also Claim 10(f), *supra*.

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. *Dec.*, ¶167.

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;

As discussed in Claim 10(a), Toomer teaches that mobile device 324 allows a user to interface with the mobile device 324 “by manipulating a **keypad**, wheel, **touch screen**, or other input device 682[.]” *Toomer*, [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[.]” *Id.*, [0003]. A POSITA would have understood that the user input, e.g., manual entry of account information, would be 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. *Dec.*, ¶168.

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 associated with the device, such as a credit card number. *See* Claim 10(a); *Grigg*, [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 the modification. *Dec.*, ¶169.

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.

For the reasons discussed in Claim 10(b), Toomer teaches that the device-specific information comprises [. . .] device identifiers. See Claim 10(b). As discussed in Claim 10(d), Grigg teaches storing the mobile wallet account number (device account numbers) on the payment device. As discussed in Claim 10(f), Hammad teaches storing an ATC (device usage sequence counters) on the mobile device.

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). *Dec.*, ¶¶170-171.

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***

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

discussed in Claim 10(f), Hammad teaches using birthday or home address (*user information*) to generate a dCVV.

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). *Dec.*, ¶¶172-173.

VI. 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.*

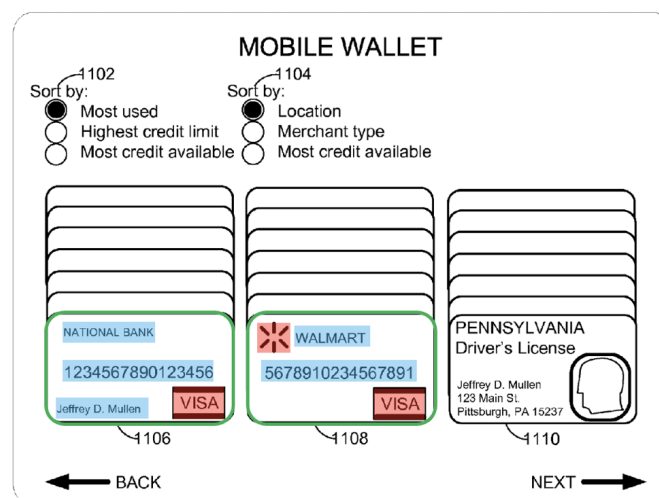
a) Toomer's Teachings

Toomer teaches that “the 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*, [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.” *Id.*, [0052], [0063]. “[P]ayment vehicles” are *payment method*

types, such as “credit, debit, ... and other types of accounts.” *Id.*, [0027]. Thus, Toomer teaches *rendering on the display* of the mobile device (*electronic device*) payment vehicles (*payment method types*) *stored in the* mobile device.

b) Mullen '449's Teachings

Mullen '449 teaches a mobile device 100 configured to display a mobile wallet. *Mullen '449*, [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*, [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*, [0064]. Figure 11 below illustrates the GUI of a mobile device and depicts payment method types as *images* of payment cards (annotated in green), the images including *alphanumeric characters* (blue) and *iconography* (red) on the cards.



Mullen '449, Fig. 11; *see also*, [0112], [0114] (“One or more payment cards, for example, may be rendered onto GUI 1100[.]”). As shown in Figure 11, alphanumeric characters and iconography includes card network icons (e.g., VISA icons), an issuer logo (e.g., Walmart logo), a portion of the account number, and a cardholder name. *Mullen*, Fig. 11.

c) Motivation to Combine

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. Dec.*, ¶176. 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. *Id.* 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. *Id.*

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. *Dec.*, ¶177.

Further, the teaching of Mullen '449 would enhance the user experience of displaying accounts for selection. *Id.*

In combination, Toomer's mobile device is configured to store payment method types and render the payment methods on its display device, the renderings comprising images, alphanumeric characters and iconography relating to the virtual cards, as taught by Mullen '449. *Dec.*, ¶178.

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 [on] the display and using a touch screen interface for the user selection.***

a) Toomer's Teachings

Toomer's mobile device "allow[s] storage of multiple payment vehicles" and "provide[s] 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 [...] touch screen[.]" *Toomer*, [0063]. 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 in view of Grigg. *Grigg*, [0054], [0084]; *Dec.*, ¶179.

Toomer's 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." *Toomer*, [0052]. 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) using a touch screen interface for the user selection. See Claim 14; Dec., ¶179.

b) Mullen '449's Teachings

It would have been obvious to a POSITA based on the teachings of Mullen '449. 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*, [0112], Fig. 11. “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.” *Id.*, -[0120], Fig. 13; *see also* [0119], Fig. 12.

c) Motivation to Combine

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 available for user selection on the touch screen display, as taught in Mullen '449. See Claim 14; Dec., ¶181. A POSITA also would have had a reasonable expectation of success in the combination. See Claim 14; Dec., ¶181.

C. Claim 16

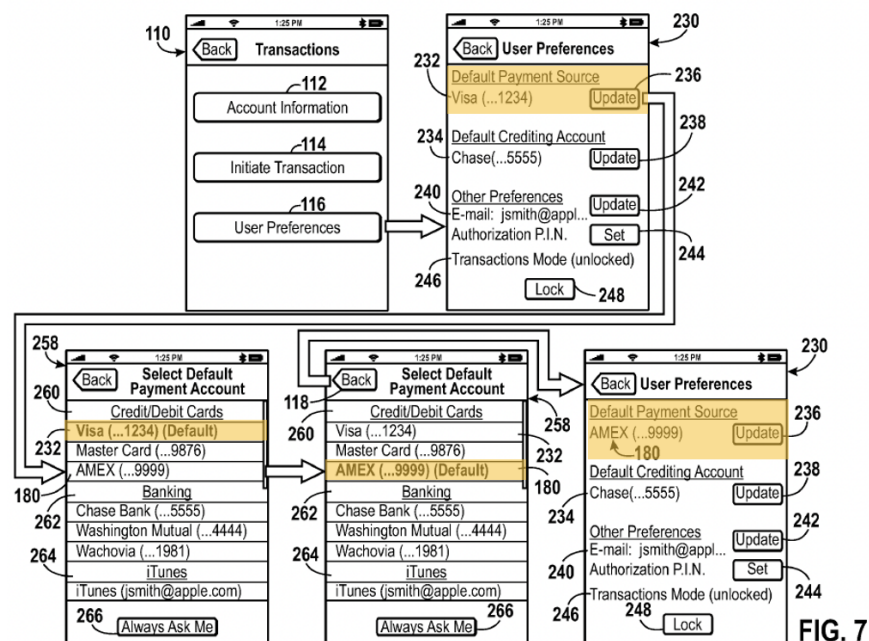
1. **16. The method of claim 15, wherein the user selection is a default payment method to be used in transactions.**

a) Toomer's Teachings

As discussed with regard to Claim 15, Toomer teaches a user selection of a payment method to be used in transactions. See Claim 15.

b) Lin's Teachings

Lin teaches a similar mobile wallet application that “may include a user-specified preferred or **default payment account** or source[.]” *Lin*, 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). *Id.*, 37:22-25, 40:1-7, 47:1-2.



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

c) Motivation to Combine

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. *Dec.*, ¶184. 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. *Id.* 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. *Id.* 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. *Id.*

Thus, in combination, Toomer's mobile device is configured to permit a user to select a payment method stored on its mobile wallet application, the selected payment method being a default payment method to be used in transactions as taught by Lin. *Dec.*, ¶185.

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;

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, [0038]; *see also* [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).

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. *Dec.*, ¶186.

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

A. Claim 1

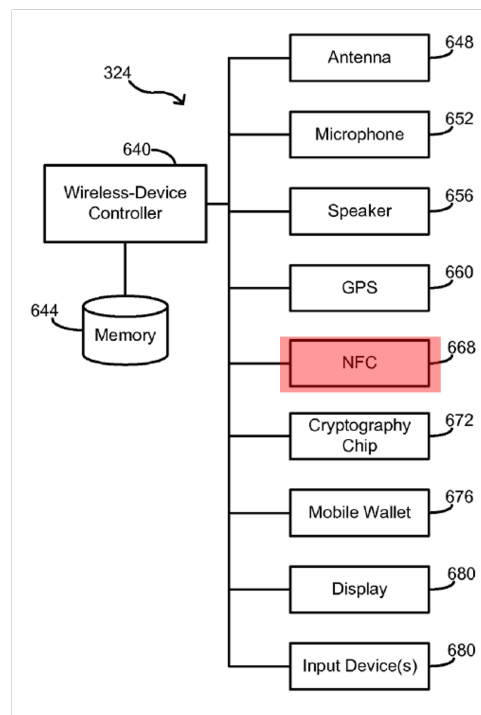
1. 1(pre): An electronic device comprising:

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

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

Toomer teaches a mobile device including 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[.]”

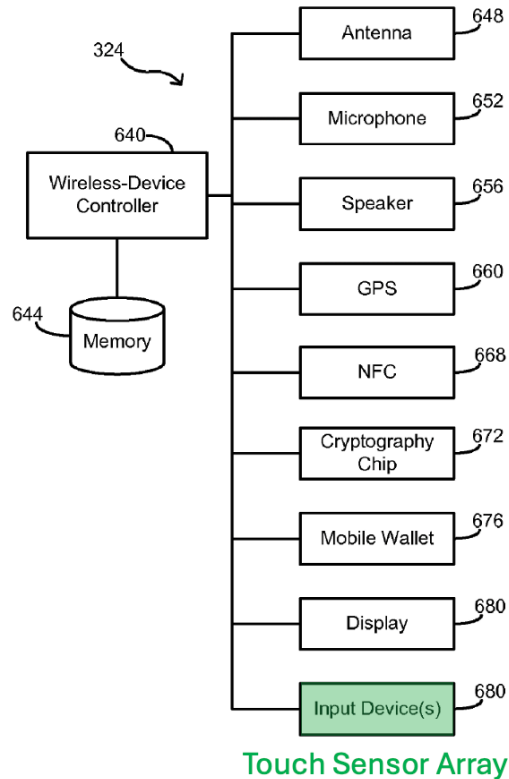
Toomer, [0062]; *see also* [0023], [0025], [0051]-[0052], [0055], [0063].



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

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

As discussed in Claim 10(a), Toomer teaches the 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*, [0063], Fig. 6.



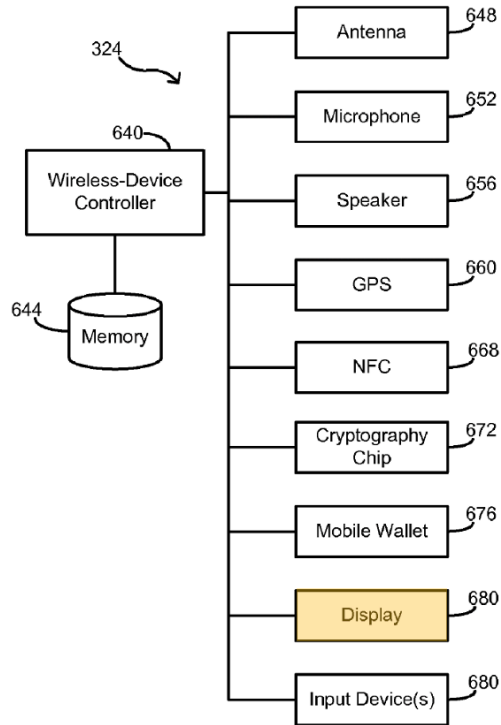
Toomer, Fig. 6 (annotated).⁶

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

4. 1(c): a display;

Toomer teaches that the mobile device includes a “screen or display device 680[.]” *Toomer*, [0063]; *see also* [0044].

⁶ Figure 6 incorrectly identifies the input device as 680.



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

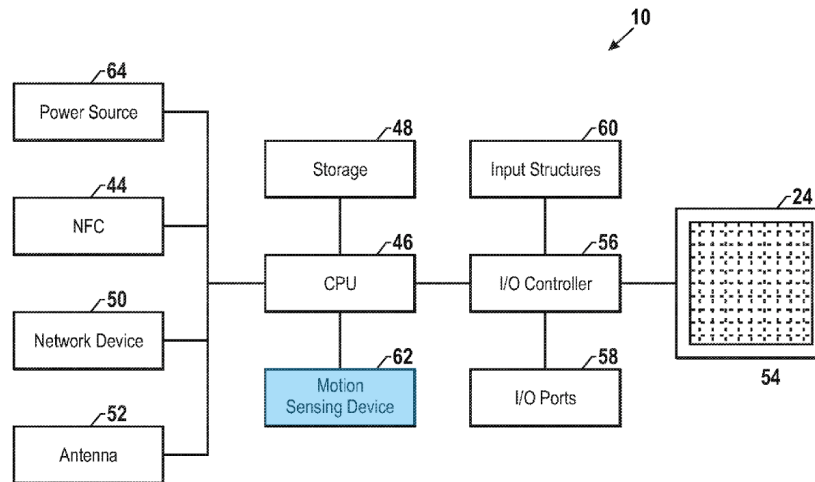
5. 1(d): a motion rate detection array;

a) Toomer's Teachings

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

b) Casey's Teachings

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



Casey, Fig. 2 (annotated).

The motion sensing device is “any device configured to measure motion or acceleration,” including a three-axis accelerometer. *Id.*, 7:61-8:3. A POSITA would understand a three-axis accelerometer includes an array of three accelerometers measuring accelerations in the X, Y, and Z axes. *Dec.*, ¶¶195-197. Per dependent claim 2, a motion rate detection array includes a plurality of accelerometers. Thus, Casey teaches a motion rate detection array.

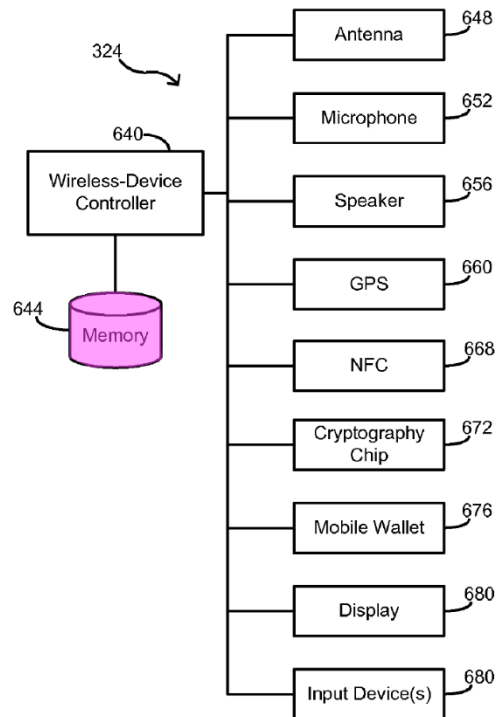
“Motion data acquired by the motion sensing device 62 may be used to confirm a payment transaction.” *Casey*, 8:4-13. Specifically, “[t]he device 10 may sense motion through ... the motion sensing device[,]” such as user may move the device to the right to confirm or left to deny a transaction. *Id.*, 9:47-10:2; *see also* 18:39-19:10, Figs. 12-13.

c) Motivation to Combine

Based on the teachings of Casey, it would have been obvious, and a POSITA would have been motivated to include Casey's motion sensing device in Toomer's mobile device. *Dec.*, ¶¶199-200. A POSITA would have appreciated that mobile devices at the time of the '520 Patent typically included inertial sensor arrays, such as accelerometers. *Id.* 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, as taught by Casey. *Id.* 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. *Id.* 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. *Id.*

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

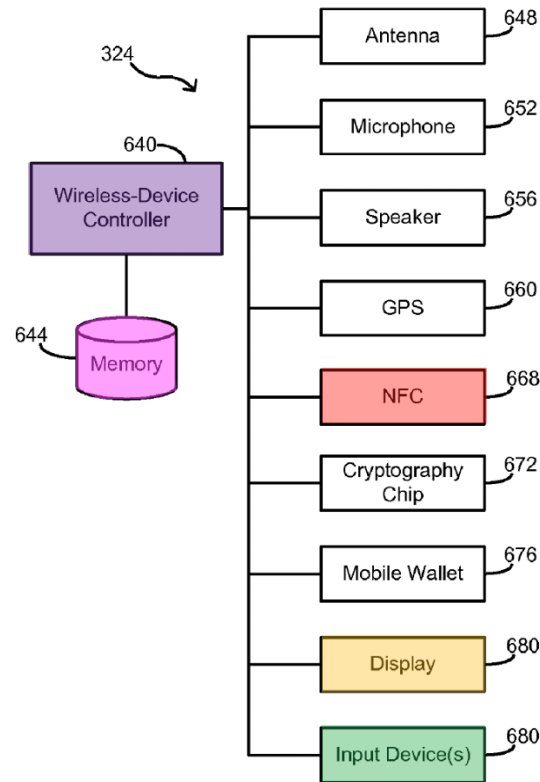
Toomer's mobile device includes a memory 644. *Toomer*, [0061]; *see also* [0044]. Toomer's memory is used to store payment information, which includes "ownership details of the account" (i.e., a user data) and "current balance levels for the account" (i.e., a currency amount). *Toomer*, [0052]-[0053];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



Toomer, 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;***

Toomer's 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*, [0061]; *see also* [0044]-[0045]. As shown in Fig. 6, processor 640 is operatively coupled to the NFC unit, the touch sensor array (input device 682), the display, and the memory.



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

As discussed in Claim 1(d), it would have been obvious to a POSITA to modify Toomer's mobile device to include a motion rate detection array. 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 of the array. Dec., ¶203.

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:***

Toomer's mobile device includes a computer readable medium having software (i.e., instructions) stored thereon that, responsive to execution by the electronic device, cause the electronic device to perform operations, including those

associated with a mobile wallet application. *Toomer*, [0061], [0063]; *see also*, [0008], [0036], [0047], [0072], Claim 26; *Dec.*, ¶¶204-205. Specifically, Toomer teaches a mobile wallet application software stored in memory that executes to cause the mobile device to perform payment operations, including those required by limitations 1(i)-(n) (as modified by the references discussed therein). *See Toomer*, [0024], [0047], [0052], [0055], [0063]; *see also* Claims 1(i)-(n).

9. 1(h)-(n):

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

Casey teaches user input comprising a confirmation or a denial of an indicated transaction. In particular, 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*, 13:39-43; *see also* 13:46-48, Fig. 5. “[A] user may drag the slide bar to the left to the decline position 186 to decline the payment or the user may drag the slide bar 182 to the right to the

confirmation position 188 to confirm the payment transaction.” *Id.*, 13:48-51, Figs. 5-6.

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

b) Motivation to Combine

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. *Dec.*, ¶¶207-209. 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. *Dec.*, ¶209. A POSITA would have further understood that requiring a PIN to access the payment method would increase the security of the transaction. *Id.* 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. *Id.* These modifications would have been minimal and required routine skill given the prevalence and ways for interacting with a mobile device in a transaction at the time. *Id.*

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.***

As discussed above, 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*, 4:22-26. Hammad further teaches that the time of day can be used in generating a dCVV. *Id.*, 3:9-11, 4:37-40. The time of day, if within a predetermined range of times, can be used in the authorization process. *Id.*, 8:11-14, 8:28-36.

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 and include the same

in the payment information. *Dec.*, ¶211. As combined with teachings of Grigg, Toomer's mobile device would transmit the mobile wallet account number and dCVV generated from the time of day, in addition to other static and dynamic data elements to an authorizing server. *See* Claims 1(n), 10(g). A POSITA would understand the mobile wallet account number and dCVV 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. *Dec.*, ¶211. A POSITA would have been motivated to include the time of day, in addition to other data elements, as an additional mechanism to secure the transaction. *Id.*; *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. *Dec.*, ¶211; *see also* 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.**

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). A POSITA would have understood that Hammad's dCVV

would also not be used in another transaction (*limited recurrence*) because the ATC changes for each transaction. *Dec.*, ¶212.

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

As discussed in Claim 10(f), Hammad teaches generating a dCVV from various dynamic and static data elements. *See* Claim 10(f). Hammad further teaches that, in addition to a ATC, a “hash value based on transaction data” may be used in generating the dCVV. *Hammad*, 4:33-36. Thus, when payment data is transmitted to a financial institution, the cryptographic hash, like the ATC, would be stored and included in the payment data. *Hammad*, 6:49-7:3, 7:4-28, Figs. 4-5. A POSITA would have understood that the cryptographic hash is processed by the processor and stored in memory, like the ATC, prior to being used to generate a dCVV and embedded in payment data for transmission. *Dec.*, ¶213.

b) Motivation to Combine

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 for the same reasons discussed in Claim 10(f). *Dec.*, ¶214.

F. Claim 9

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

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*, 5:35-43. Thus, Casey's device includes a USB connector for connection to a standard computing device.

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. *Dec.*, ¶216. 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. *Id.* 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. *Id.*

VIII. 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***

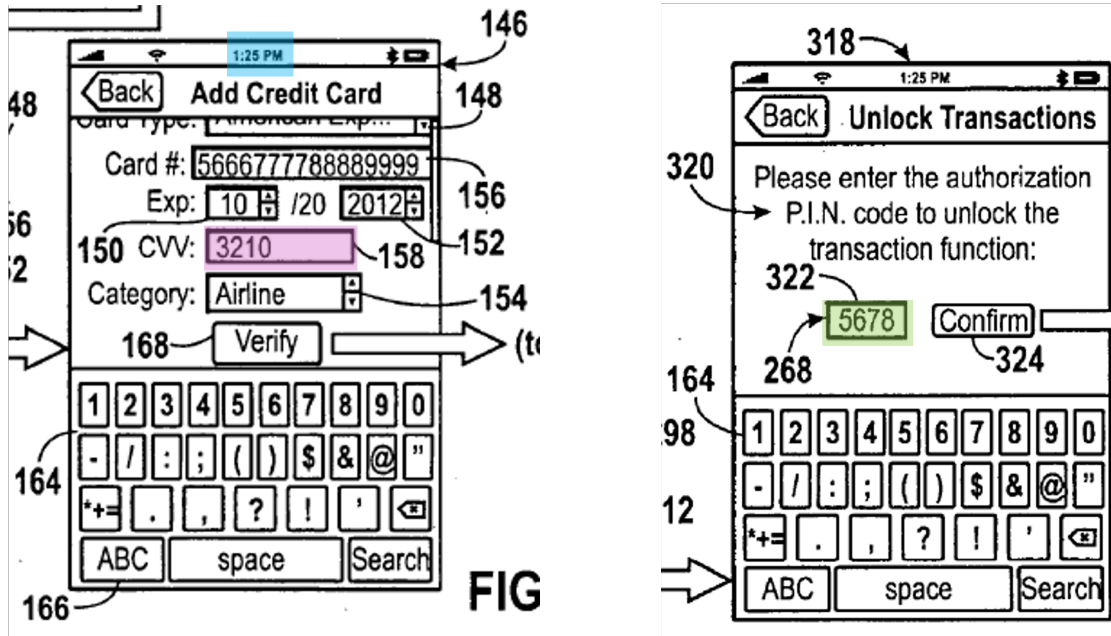
other credit card transaction information of the user, a merchant, a bank or a credit card authority.

a) Toomer and Grigg's Teachings

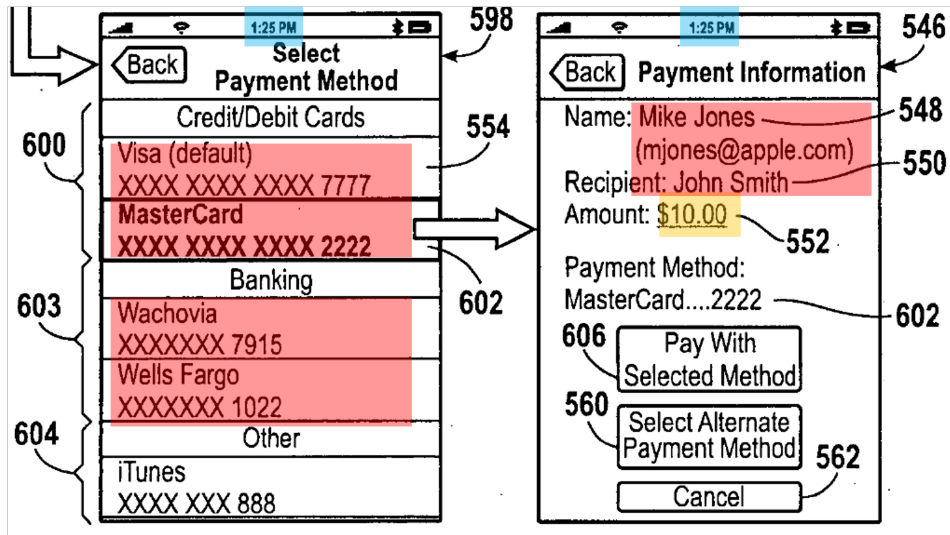
Toomer teaches a mobile wallet application on a mobile device that allows for entry, display, and selection of an account for a particular transaction. *Toomer*, [0052]. Alternatively, in combination with Grigg, this includes accepting user input and displaying information associated with adding card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

b) Lin's Teachings

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*, 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 limited-use 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).



Id., Figs. 5A, 10B.



Id., Fig. 14E.

c) Motivation to Combine

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.

Dec., ¶¶217-222. 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. *Dec.*, ¶219. It was well-known that such a device could display various pieces of information related to entering card information and a payment transaction. *Id.* 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. *Id.*

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

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. *Dec.*, ¶221. Like Toomer, Lin describes using the mobile device to conduct a transaction via NFC. *Lin*, 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.

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. *Dec.*, ¶222. In the combined system, Toomer would display on its touchscreen display the information depicted in Lin. *Id.*

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

A. Claim 1

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

See 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

As discussed in Claim 1(pre), Toomer discloses that its mobile device may be a smart card. *Supra*, Ground 3, Claim 1(a); *Toomer*, [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”).

b) Mullen 760's Teachings

Mullen '760 teaches a smart credit card capable of communicating payment information for a transaction through a magnetic stripe or in a contactless manner (e.g., RFID). *Mullen '760*, [0002]-[0003], [0016], [0021], [0023], [0245], [0300]-[0301], Figs. 11, 22. The card can include inertial movement sensors, such as one or more accelerometers. *Id.*, [0019], [0245]. A POSITA would have understood that using multiple accelerometers, as taught by Mullen '760, is an array of accelerometers. *Dec.*, ¶225; *see also* Ground 3, Claim 1(d). As discussed below in

Claim 2, Mullen '760 also teaches a plurality of inductor coils and companion magnetic-field pickup coils and an optical sensor array. *See* Claim 2. Per dependent claim 2 of the '520 Patent, 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. Thus, Mullen '760 teaches a motion rate detection array.

Mullen '760's inertial movement sensor may "detect a swipe in order to initiate one or more [magnetic] emulators." *Mullen '760*, [0245]; *see also*, [0019] ("[T]he swiping motion of a card may be detected via one or more inertial sensors such as accelerometers and/or gyroscopes."). 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." *Id.*, [0014]; *see also*, [0013], [0016], [0021], [0023].

c) Motivation to Combine

Based on the teachings of Mullen '760, it would have been obvious, and a POSITA would have been motivated to include Mullen '760's motion sensing device in Toomer's contactless device, such as a smart card. *Dec.*, ¶227. A POSITA would have appreciated that smart cards at the time of the '520 Patent often included inertial sensor arrays including accelerometers. *Id.* 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. *Id.* Providing more than one way to initiate transactions would have enhanced the user experience by making transaction initiation easier and more efficient. *Id.* 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. *Id.*

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.***

As discussed in Claim 1, Toomer-Grigg-Hammad-Mullen '760 discloses that a contactless device may include a plurality of accelerometers. *Supra*, Ground 5, Claim 1(d). Based on Patent Owner's apparent interpretation of this claim language, Toomer-Grigg-Hammad-Mullen '760 render Claim 2 obvious, as described in Ground 5, Claim 1(d). *Dec.*, ¶228.

In any event, 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

Mullen '760 teaches that a magnetic emulation circuit may be a coil. *Mullen '760*, [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. *Id.*, [0007], [0028], [0036]-[0041], [0088], [0240], [0247], [0295], [0302], [0305], [0348] (“a magnetic emulator (or multiple magnetic emulators) may magnetically communicate financial data”).

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. *Id.*, [0295], [0363]; *see also* [0030], [0035], [0253], [0300], [0302], [0347], [0354]-[0355], [0362]-[0363], Figs. 22-23, 43 (elements 4310, 4320, 4330), 44-45, 51 (elements 5170, 5180, 5185). 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 a card.” *Id.*, [0375], Fig. 53. The card also includes an RFID antenna and RFID field detector. *Id.*, [0301], [0304]. A POSITA would understand an RFID antenna and/or field detector includes coils for magnetic-field pickup from an RFID reader. *Dec.*, ¶231. 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, [0305]; *see also* [0029], [0308], [0321].

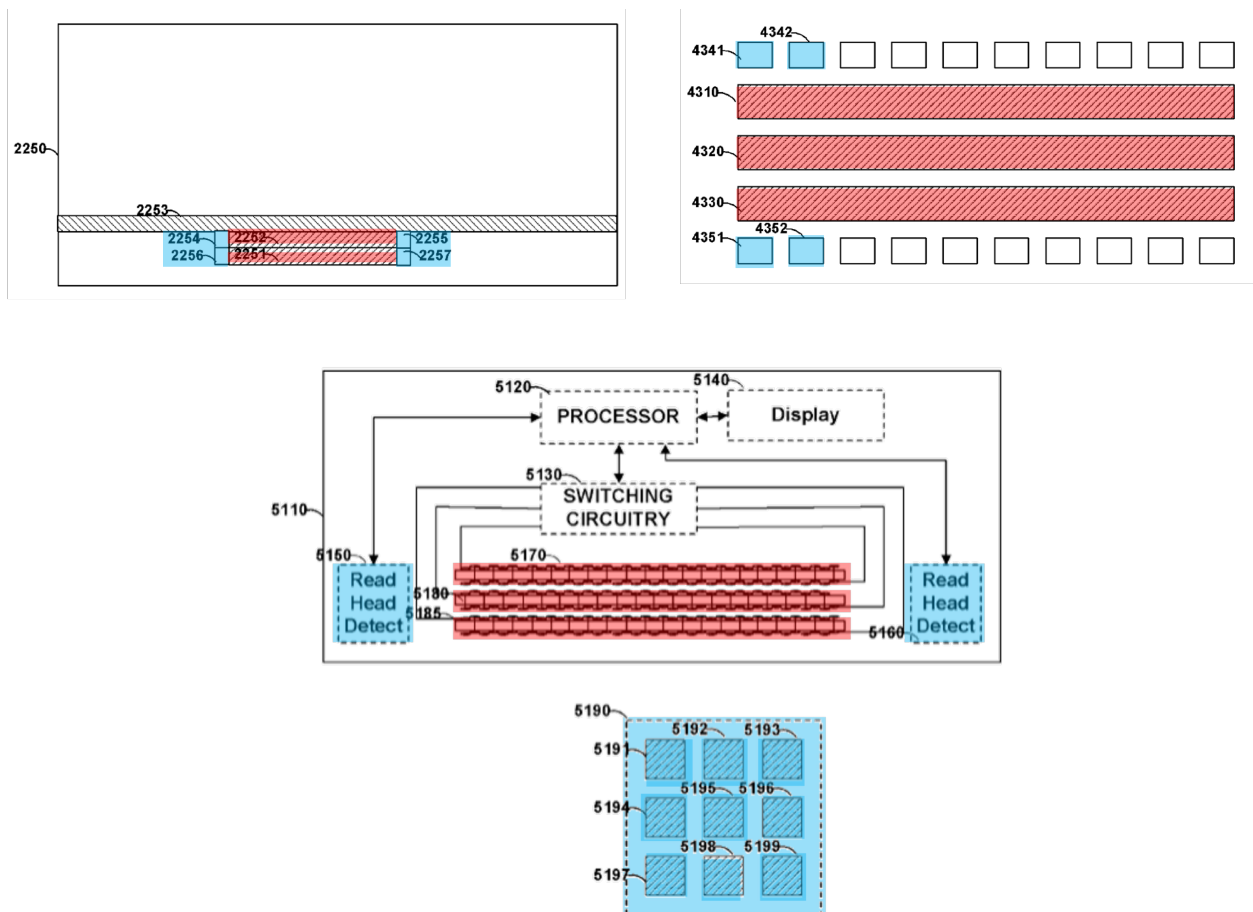
A POSITA would understand the magnetic emulators, RFID antenna and field detector of *Mullen* ’760, therefore, are a plurality of inductor coils and companion magnetic-field pickup coils.

Mullen ’760 also teaches that a card includes a read-head detector for detecting a read-head “of a magnetic stripe reader.” *Mullen* ’760, [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.” *Id.*, [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]. A read-head detector may comprise a “cluster” of read-head detectors, including “optic” detectors (optical sensor array) that “determine the presence of a read-head. *Id.*, *also* [0338], [0364], Fig. 51 (5190), Fig. 37. The optical detector can “determine the presence of a read-head[.]” *Id.*, [0338]; *see also* [0041], [0295].

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. *Id.*, [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*). Dec., ¶232. Accordingly, the optical and/or emulator of the card (*electronic device*) detects the presence (*detected proximity*) of the magnetic stripe reader's read-head (*second electronic device*).

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:



Figs. 22, 43, 51 (annotated).

b) Motivation to Combine

As discussed in Ground 4, Claim 1(d), it would have been obvious to include a plurality of accelerometers in Toomer's smart card.

It would have been obvious and a POSITA would have been motivated to include Mullen '760's magnetic emulators and an optical detector in Toomer's smart card. *Dec.*, ¶¶236. Based on Mullen "'760's teachings, the optical detector would determine that the read-head is being swiped in a particular reader. *Id.* An emulator used as a read-head detector would similarly detect the presence of the read-head upon detecting a phase-shift. *Id.*

Moreover, 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. *Id.* 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. *Id.* 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. *Id.*

X. 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.

Based on Patent Owner's apparent interpretation of this claim language, Toomer-Grigg-Hammad-Mullen '760 render Claim 3 obvious, as described in Ground 5, Claim 1(d). *Dec.*, ¶238. Alternatively, the proposed combination in view of Griffin renders Claim 3 obvious.

Mullen '760 teaches that the accelerometers “detect a swipe in order to initiate one or more emulators.” *Mullen* '760, [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[.]” *Id.*, [0305], Fig. 25; *see also*, [0029]-[0030], [0319], [0321], Fig. 29.

a) Griffin's Teachings

Griffin teaches mobile devices that use NFC, such as those involving payment. *Griffin*, [0001], [0003]. The mobile device includes an accelerometer, such as a 3-axis accelerometer. *Id.*, [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. *Dec.*, ¶¶195-197. “The accelerometer 137 recognizes the tapping of a communications device against ... another device, i.e., recognizes the vibrations.” *Id.*, [0049]. “[W]hen the device is tapped against another object,” the NFC circuit is woken up and communication is initiated. *Id.* Thus, the

accelerometers generate an indication of the proximity of the mobile device to another device. *Dec.*, ¶240.

b) Motivation to Combine

It would have been obvious to use Mullen '760's accelerometers in a similar way as described in Griffin. *Dec.*, ¶241. In the combination, Mullen '760's emulator would be initiated upon the accelerometers detecting the two devices have contacted. *Id.* This is a natural application of Griffin's teachings to Mullen '760's device and a POSITA would understand it would implement Mullen '760's teachings relating to using the inertial movement sensor to initiate one or more emulators. *Id.* A POSITA would have been motivated to combine such prior art elements according to known methods to yield the predictable result of increased options and user experience in performing a transaction. *Id.*

XI. DISCRETION UNDER 35 U.S.C. § 325(d)

Pursuant to the Office's Interim Process Concerning Institution published March 26, 2025, Petitioner reserves the right to address in further briefing any discretionary denial issues raised by CardWare.

XII. CONCLUSION

For the forgoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

ERISE IP, P.A.

BY: /s/ Adam P. Seitz

IPR2025-01145

U.S. Patent No. 10,339,520

Adam P. Seitz, Reg. No. 52,206

adam.seitz@eriseip.com

7015 College Boulevard, Suite 700

Overland Park, Kansas 66211

(913) 777-5600 Telephone

(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

XIII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

A. Real Party-in-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '520 patent is the subject of a civil action in *CardWare Inc. v. Apple Inc.*, 1:25-cv-00446 (W.D. Tex.). The '520 Patent is also the subject of a civil action in *CardWare Inc. v. Google Inc.*, 7:24-cv-00278 (W.D. Tex.).

The '520 patent was previously the subject of *inter partes* review petitions in *Samsung Electronics Co., Ltd., v. CardWare Inc.*, IPR2023-00210 and IPR2023-00211, which are no longer pending.

Petitioner is concurrently filing a second petition challenging a different set of claims of the '520 patent in IPR2025-01146.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Adam Seitz (Reg. No. 52,206) Adam.seitz@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	Mark Lang (Reg. No. 55,356) Mark.Lang@eriseip.com Lydia Raw (Reg. No. 76,436) Lydia.raw@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700

	Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601
--	---

D. 37 C.F.R. 42.8(b)(4) – Service Information

Please address all correspondence to the lead and back-up counsel as shown above. Petitioners consent to electronic service by e-mail at the e-mail addresses provided above.

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 10,339,520 to Wyatt (“the ’520 patent”)
Exhibit 1002	Prosecution History of the ’520 patent (“the Prosecution History”)
Exhibit 1003	Expert Declaration of Dr. Clifford Neuman
Exhibit 1004	U.S. Pub. No. 2009/0210308 (“Toomer”)
Exhibit 1005	U.S. Pub. No. 2014/0006276 (“Grigg”)
Exhibit 1006	U.S. Patent No. 7,740,168 (“Hammad”)
Exhibit 1007	U.S. Pub. No. 2012/0290449 (“Mullen”)
Exhibit 1008	WIPO Publication No. 2010/039337 (“Lin”)
Exhibit 1009	U.S. Patent No. 8,255,323 (“Casey”)
Exhibit 1010	WIPO Publication No. 2009/082760 (“Mullen ’760”)
Exhibit 1011	U.S. Pub. No. 2011/0070826 (“Griffin”)
Exhibit 1012	CardWare Inc.’s Preliminary Proposed Claim Constructions
Exhibit 1013	Intentionally Left Blank
Exhibit 1014	Intentionally Left Blank
Exhibit 1015	Intentionally Left Blank
Exhibit 1016	Intentionally Left Blank
Exhibit 1017	Intentionally Left Blank
Exhibit 1018	Intentionally Left Blank
Exhibit 1019	Intentionally Left Blank
Exhibit 1020	IBM, <i>The Magnetic Stripe</i> , IBM, https://www.ibm.com/history/magnetic-stripe . (“ <i>IBM</i> ”)
Exhibit 1021	Vedat Coskun, <i>Near Field Communication: Theory To Practice</i> (John Wiley & Sons, 1st ed. 2012) (“ <i>Coskun</i> ”)
Exhibit 1022	MagTek, <i>Magnetic Stripe Card Standards</i> , (MagTek Inc. eds., 2011) (“ <i>MagTek</i> ”)
Exhibit 1023	EMVCo, LLC, <i>EMV Integrated Circuit Card Specifications for Payment Systems: Book 2 – Security and Key Management</i> (EMVCo, LLC eds., Version 4.3 2011) (“ <i>EMV</i> ”)
Exhibit 1024	Klaus Finkenzeller, <i>RFID Handbook</i> (John Wiley & Sons, 3rd ed. 2010) (“ <i>Finkenzeller</i> ”)
Exhibit 1025	MasterCard, <i>MasterCard PayPass™ in Action</i> , MASTERCARD (Jun. 11, 5:35 PM), https://www.mastercard.com/us/company/en/ourbusiness/paypass_in_action.html#:~:text=MasterCard%20PayPass%E2%84%A2%20in%20Action&text=Developed%20to%20replace%20the%20need,the%20way%20they%20view%20cash . (“ <i>PayPass</i> ”)

Exhibit 1026	<i>Smart Card Alliance, EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value-Added Functionality</i> (Smart Card Alliance, Inc. eds., 2012) (“ <i>Smart</i> ”)
Exhibit 1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. (“ <i>Pitroda</i> ”)
Exhibit 1028	MasterCard, <i>MasterCard Approved Mobile Devices</i> , MASTERCARD (Aug. 3, 2012), http://www.mastercard-mobilepartner.com/docs/MasterCard_Aproved_Mobile_Devices.pdf , [https://web.archive.org/web/20120906234255/http://www.mastercard-mobilepartner.com:80/docs/MasterCard_Aproved_Mobile_Devices.pdf] (“ <i>MasterCard Mobile Partner</i> ”)
Exhibit 1029	U.S. Patent Publication No. 2013/0054474 to Yeager (“ <i>Yeager</i> ”)
Exhibit 1030	EMVCo, LLC, <i>EMV Chip At-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World</i> , EMVCo (2002), https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf (“ <i>EMVCo</i> ”)
Exhibit 1031	<i>Scoping SIG & Tokenization Taskforce PCI Security Standards Council, PCI Data Security Standard (PCI DSS) – Information Supplement: PCI DSS Tokenization Guidelines</i> (pci Security Standards Council eds., Version 2.0 2011) (“ <i>PCI SSC</i> ”)
Exhibit 1032	Alessandro Vizzarri et al., <i>Security in Mobile Payments</i> (2013) (“ <i>Vizzarri</i> ”)
Exhibit 1033	U.S. Patent Publication No. 2008/00110983 to Ashfield (“ <i>Ashfield</i> ”)
Exhibit 1034	Intentionally Left Blank
Exhibit 1035	“Smart Card Technology: New Methods for Access Control” (“ <i>Smart Card Tech.</i> ”)
Exhibit 1036	U.S. Patent No. 5,528,222 (“ <i>Moskowitz</i> ”)
Exhibit 1037	“The Electronic Purse” (“ <i>Wenninger</i> ”)
Exhibit 1038	U.S. Patent 5,594,233 (“ <i>Kenneth</i> ”)
Exhibit 1039	U.S. Patent No. 7,004,385 (“ <i>Douglass</i> ”)
Exhibit 1040	U.S. Pub. No. 2007/0265984 (“ <i>Sanantha</i> ”)
Exhibit 1041	U.S. Pub. No. 2012/0197691 (“ <i>Grigg</i> ”)
Exhibit 1042	U.S. Patent Publication No. 2010/0125509 (“ <i>Kranzley</i> ”)
Exhibit 1043	U.S. Pub. No. 2011/0140841 (“ <i>Bona</i> ”)
Exhibit 1044	U.S. Pub. No. 2009/0307132A1 (“ <i>Phillips</i> ”)

Exhibit 1045	“A Monolithic Three-Axis Silicon Capacitive Accelerometer with Micro-G Resolution,” J. Che, et al., <i>TRANSDUCERS '03. 12th International Conference on Solid-State Sensors, Actuators and Microsystems</i> . Digest of Technical Papers, Boston, MA, USA, 2003, pp. 81-84 vol.1
Exhibit 1046	U.S. Patent No. 8,351,910 (“Horodezky”)
Exhibit 1047	U.S. Patent No. 8,952,832 (“Nasiri”)
Exhibit 1048	U.S. Patent No. 6,938,484 (“Najafi”)
Exhibit 1049	U.S. Patent No. 7,258,012 (“Xie”)
Exhibit 1050	U.S. Patent No. 8,892,390 (“MacGougan”)
Exhibit 1051	Apple Presents iPhone 4, available at: https://www.apple.com/newsroom/2010/06/07Apple-Presents-iPhone-4/
Exhibit 1052	“Motion sensing in the iPhone 4: MEMS accelerometer,” MEMS Journal -- The Largest MEMS Publication in the World, available at: https://www.memsjournal.com/2010/12/motion-sensing-in-the-iphone-4-mems-accelerometer.html
Exhibit 1053	Handhelds and PDAs_ Motorola ES400, available at: https://www.ruggedpcreview.com/3_handhelds_motorola_es400.html
Exhibit 1054	Review of the Motorola Droid from Verizon Wireless — Digital Bits Technology Column, available at: https://www.andybrain.com/2009/review-of-the-motorola-droid-from-verizon-wireless/
Exhibit 1055	Top 10 HTC Smartphones of 2011 _ IBTimes, available at: https://www.ibtimes.com/top-10-htc-smartphones-2011-388788
Exhibit 1056	U.S. Pub. No. 2009/0320123A1 (“Yu”)
Exhibit 1057	U.S. Patent No. 9,721,319 (“Smets”)
Exhibit 1058	U.S. Pub. No. 2013/0087627A1 (“Marseille”)
Exhibit 1059	U.S. Patent No. 8,909,138 (“Rhelimi”)
Exhibit 1060	Cardware’s Preliminary Infringement Contentions, <i>CardWare Inc. v. Apple Inc.</i> , Civil Action No. 7:24-cv-00279-ADA

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,267 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: June 24, 2025

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

**CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105(a)**

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on June 24, 2025, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '520 patent:

David Wyatt
c/o Murabito, Hao & Barnes
1500 E Hamilton Ave, Suite 118
Campbell, CA 95008

A courtesy copy of the Petition for *Inter Partes* Review was emailed to counsel of record in the parallel litigation:

Caroline M. Walters (cwalters@reichmanjorgensen.com)
Navid Cyrus Bayar (nbayar@reichmanjorgensen.com)
Timothy A. Trost (ttrost@reichmanjorgensen.com)
Khue V. Hoang (khoang@reichmanjorgensen.com)
Matthew G. Berkowitz (mberkowitz@reichmanjorgensen.com)
Patrick R. Colsher (pcolsher@reichmanjorgensen.com)
Yue (Joy) Wang (ywang@reichmanjorgensen.com)
Eric H. Findlay (efindlay@findlaycraft.com)

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211

IPR2025-01145

U.S. Patent No. 10,339,520

(913) 777-5600 Telephone

(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER