

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARDWARE, INC.,
Patent Owner

Case No. IPR2025-01146
U.S. Patent No. 10,339,520

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

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	THE '520 PATENT.....	1
	A. BRIEF DESCRIPTION	1
	B. FIELD OF ENDEAVOR AND PROBLEM SOLVED BY THE INVENTORS	3
	C. SUMMARY OF THE PROSECUTION HISTORY	4
	D. LEVEL OF ORDINARY SKILL IN THE ART	5
III.	REQUIREMENTS FOR IPR.....	5
	A. STANDING UNDER 37 C.F.R. § 42.104(A)	5
	B. IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B)	6
	C. CLAIM CONSTRUCTION	6
IV.	SHOWING OF ANALOGOUS PRIOR ART	7
	A. GILL.....	7
	B. SMITH	10
	C. KAY	12
	D. GOMEZ.....	12
	E. ANALOGOUS ART.....	15
V.	GROUND 1: CLAIMS 18-21 AND 24 ARE OBVIOUS OVER GILL, SMITH, AND KAY	16
	A. CLAIM 18	16
	1. <i>18(Pre): A method of facilitating and authorizing an automated teller machine (ATM) transaction involving an electronic device, wherein an electronic device transacts wirelessly with an ATM, the method comprising:.....</i>	<i>16</i>
	2. <i>18(a): providing, by the electronic device, at least one of account information; identification; and authorization, for the ATM transaction; and,</i>	<i>18</i>
	a) Gill's Teachings	18
	b) Smith's Teachings	20
	c) Motivation to Combine	21

3.	<i>18(b): wherein the electronic device comprises a user interface comprising: displays; touch sensors; and buttons; and,</i>	<i>27</i>
4.	<i>18(c): recording a user selection from the user interface of the electronic device of a user selected account from which the electronic device is operable to wirelessly convey with an ATM; and,</i>	<i>29</i>
	a) Gill's Teachings	29
	b) Smith's Teachings	30
5.	<i>18(d): recording a user selection from the user interface of the electronic device of a user selected account operation, wherein said user selected account operation is selected from a list of funds transfer operations; and,</i>	<i>31</i>
	a) Gill's Teachings	31
	b) Kay's Teachings	33
	c) Motivation to Combine	35
6.	<i>18(e): wherein user input information from the user interface includes at least one of a set comprising: identification, account, amount of currency, operation and authorizing information; and,</i>	<i>37</i>
	a) Gill's Teachings	37
	b) Kay's Teachings	39
	c) Motivation to Combine	40
7.	<i>18(f): wherein the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC; and,</i>	<i>41</i>
8.	<i>18(g): wherein the ATM is configured for performing the user selected account operation using the identification and authorizing information; and,</i>	<i>43</i>
9.	<i>18(h): wherein the identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions; and,</i>	<i>45</i>

10.	<i>18(i): wherein said static and dynamic information is combined to perform the user selected ATM operation.</i>	<i>48</i>
B.	CLAIM 19	49
1.	<i>19. A method of claim 18, wherein the identification and authorizing information is generated from at least one of a set identification and data comprising: ATM accounts; user identification; biometric user identification; device-identifiers; email address; username; transactional information; merchant identifiers; facility location; user accounts; cryptocurrency address; cryptocurrency keys; merchant accounts; online accounts; bank accounts; device account numbers; payment numbers; card issuing authority; and payment-issuer; and wherein further the data includes at least one of time; duration; passwords; passcodes; device position; device motion; device specifics; secrets; keys; a currency; currency amounts; cryptocurrency amount; transaction limits; transaction records; usage duration; and usage sequence counts.....</i>	<i>49</i>
C.	CLAIM 20	52
1.	<i>20. A method of claim 18, wherein user entered identification and authorizing information is recorded through the user interface of the electronic device from at least one of set including: a plurality of button-press actions; a swipe gesture received at a touch sensor of the electronic device; a key press sequence received at the touch sensor; a passcode sequence received at the buttons; a plurality of swipe gestures received at a touch sensor of the electronic device; a key press PIN sequence received at the touch sensor; a passcode sequence received at the touch sensor; an accelerometer sensor indicating a user motion of the electronic device; an action and sequence of motions of the electronic device as performed by a user; an action of the user to move the electronic device into a specific orientation; a biometric sensor confirming the electronic device is in a grip of the user; and a biometric sensor confirming the electronic</i>	

	<i>device has remained in the possession of the user from activation to transaction.</i>	52
D.	CLAIM 21	53
1.	<i>21. A method of claim 18, wherein the identification and authorizing information is recorded responsive to the user inputting information using input methods provided by the ATM to record at least one of a PIN number; a passcode; a password; a biometric identification; and user known secrets.</i>	53
E.	CLAIM 24	54
1.	<i>24. The method of claim of 18, wherein the amount of currency information can be a unit of value from at least one of a set of comprising: a cash amount, an amount of a debit account, an amount of credit, a maximum spending amount, a merchant account, a bank account amount, a unit of cryptocurrency, an online account funds, an payment issuer unit of funds, and a merchant account points.</i>	54
VI.	GROUND 2: CLAIMS 18-24 AND 24 ARE OBVIOUS OVER GILL, SMITH, KAY, AND GOMEZ	55
A.	CLAIM 18	55
1.	<i>Gomez's Teachings</i>	56
2.	<i>Motivation to Combine</i>	58
B.	CLAIMS 19-21, 24	60
C.	CLAIM 22:	61
1.	<i>22. The method of claim 18, wherein the limited-use number dynamically generated in the device is based on cryptographically combining data selected from the group consisting of an ATM information, the locality of an ATM reader facility, information regarding the facility performing the transaction, bank information, a time of day, a date, a transaction amount, a count of past transactions, a sequence count, a historical record of transactions, a merchant account, a user's location, an online address, a device-internal secret, a device unique identifier, a payment authority key, a payment issuer</i>	

	<i>authority secret, a method and direction of payment, deposit, transfer and receipt, a cryptocurrency server, a cryptocurrency type, a cryptocurrency private key, a cryptocurrency public key, a cryptocurrency address, a touch gesture, a biometrically sensed user information, a user's private information, a user key, a user email, password, passcode, a PIN, a user secret, and a user input.</i>	61
D.	CLAIM 23:	63
1.	23. <i>The method of claim of 18, wherein the payment information comprises combining a plurality of static portions, and a plurality of dynamically generated limited-use portions, and wherein the static portion is a token account number with a limited-duration expiration date, to be used in place of issuer provided information.</i>	63
VII.	DISCRETIONARY CONSIDERATIONS	65
VIII.	CONCLUSION	66
IX.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)	67
A.	REAL PARTY-IN-INTEREST	67
B.	RELATED MATTERS	67
C.	LEAD AND BACK-UP COUNSEL	67
D.	37 C.F.R. § 42.8(B)(4) – SERVICE INFORMATION	68

I. INTRODUCTION

Apple Inc. (“Petitioner” or “Apple”) respectfully requests *inter partes* review (“IPR”) of claims 18-24 (“Challenged Claims”) of U.S. Patent No. 10,339,520 (“’520 patent”).

II. THE ’520 PATENT

A. Brief Description

The ’520 Patent specification describes an electronic payment card capable of generating a “**limited-duration number**”¹ for use in a payment transaction. ’520 *Patent*, 2:24-28, 2:49-62, 10:3-11:55, Fig. 7. Figure 7 depicts a process for generating and using a limited-duration number in a transaction:

¹ All emphasis added unless otherwise noted.

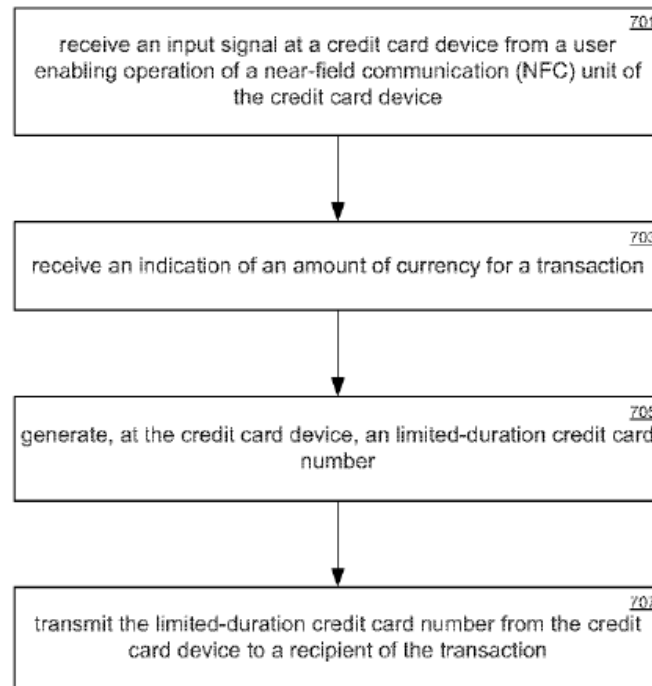


FIG. 7

'520 Patent, Fig. 7.

According to the specification, “[t]he credit card device comprises a real-time clock that is able to produce a cryptographically protected timestamp for each interaction.” *Id.*, 10:7-9. “The power source is able to activate the processor unit such that a unique number may be generated by the credit card device and verified by the credit authority according to the timestamp and the transmitted user information.” *Id.*, 10:9-13. “The limited duration credit card number is able to be produced at the time the credit card device is performing a transaction, and is able to be generated according to the user’s private information, a bank information, information regarding the facility performing the transaction, and the time of day.” *Id.*, 10:13-18. Further, the “limited-duration credit card number is able to be limited

to only one transaction, a finite number of transactions, or may be limited to a specified period of time—e.g., 2 minutes, 10 minutes, 3 hours—after which time that particular limited-duration number would become invalid.” *Id.*, 10:18-23.

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. “For example, the first four and last four digits of the credit card number are able to be fixed, while the remaining eight digits can be dynamically generated.” *Id.*, 10:38-41.

In some cases, the disclosed credit card device is used to conduct transactions with an automated teller machine (ATM). *'520 Patent*, 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.*, ¶¶33-35.²

The *'520 Patent* is reasonably pertinent to the problem of security in financial transactions. *'520 Patent*, 1:32–2:4. *Dec.*, ¶¶36-37. Existing credit card device types

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

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 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. Summary of the 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 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.

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.

The only rejection made during original examination was based on statutory double patenting. *'520 Patent File History* (Ex. 1002), 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 1-2—the application never should have been allowed.

D. Level of Ordinary Skill in the Art

A POSITA at the time of the *'520 Patent* would have had a bachelor's degree in computer science, computer engineering, electrical engineering or the equivalent, and one or two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless and online technologies. *Dec.*, ¶¶28-30. 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 FOR IPR

A. 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)

The Challenged Claims are unpatentable on the following grounds under 35 U.S.C. § 103:

Ground	Claim(s)	Basis Under 35 U.S.C. § 103
1	18-21, 24	Gill (EX1004), Smith (EX1005), and Kay (EX1006)
2	18-24	Gill, Smith, Kay, and Gomez (EX1007)

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	Prior Art Basis
Gill	05/06/2011	08/04/2015	§ 102(a)
Smith	03/01/2013	09/05/2013	§ 102(a)
Kay	11/15/2011	05/16/2013	§ 102(a)
Gomez	06/22/2012	03/21/2017	§ 102(a)

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

C. Claim Construction

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., 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 purposes of this

proceeding, Petitioner applies the plain and ordinary meaning of all claim terms as understood by a POSITA.⁴

IV. SHOWING OF ANALOGOUS PRIOR ART

A. Gill

Gill describes systems and methods for performing contactless transactions at an ATM: “An ATM machine is provided that has been equipped with a contactless interface for interacting with an external apparatus such as a debit/credit card, mobile device, and/or contactless transmission equipped stickers.” *Gill*, Abstract; *see also* 3:56-63 4:28-34, 5:13-27, 9:63-10:4, Figs. 1, 5. Figure 7 depicts example interactions between an external apparatus 120 and an ATM in performing a contactless transaction (e.g., via NFC), as taught in Gill:

⁴ Petitioner’s application of prior art to the Challenged Claims is not a waiver of any argument in litigation that any claim is indefinite, invalid, or requires claim construction.

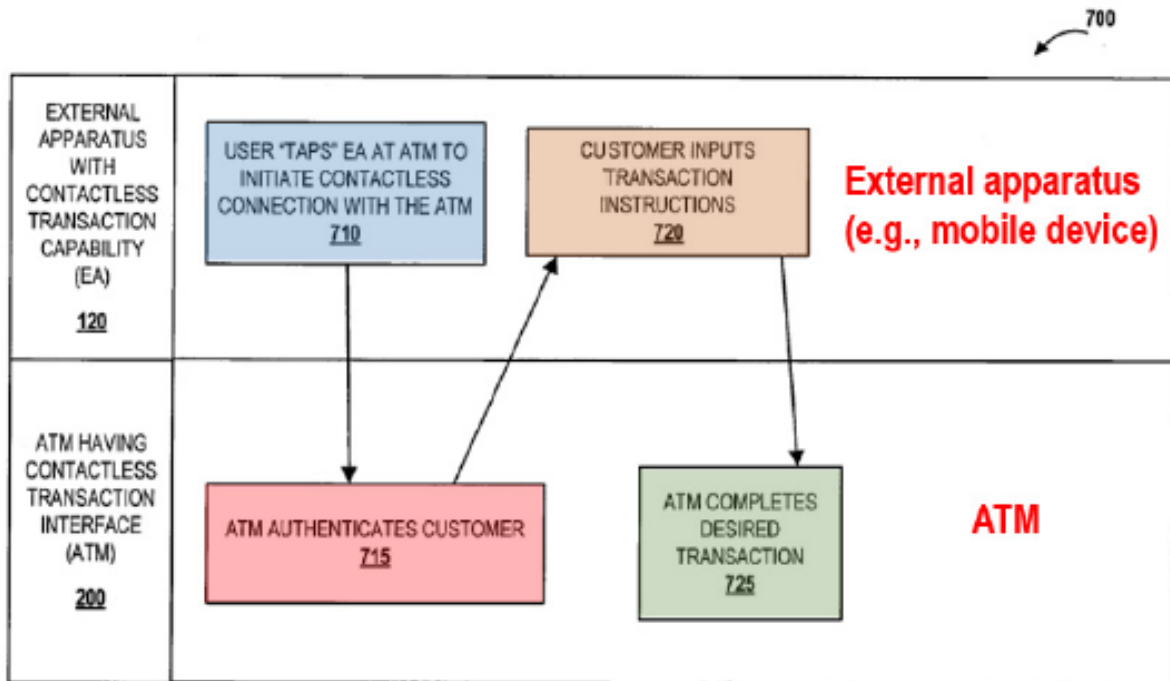


FIG. 7

Id., Fig. 7 (annotated).

As shown in Figure 7, a user (customer) “taps the external apparatus 120 at the ATM 200 to initiate a contactless connection with the ATM[,]” e.g., “by positioning the external apparatus 120 within close proximity of the contactless interface of the ATM 200[.]” *Id.*, 14:1-8. At block 715, the ATM 200 “authenticat[es] the customer” by requiring the user to present a valid credential such as a PIN. *Id.*, 14:9-13. In some embodiments, rather than directly entering credentials at the ATM after establishing a connection, “the customer may first authenticate himself prior to the contactless connection being established” by “input[ing] authentication information on his external apparatus 120 and such transfer such data

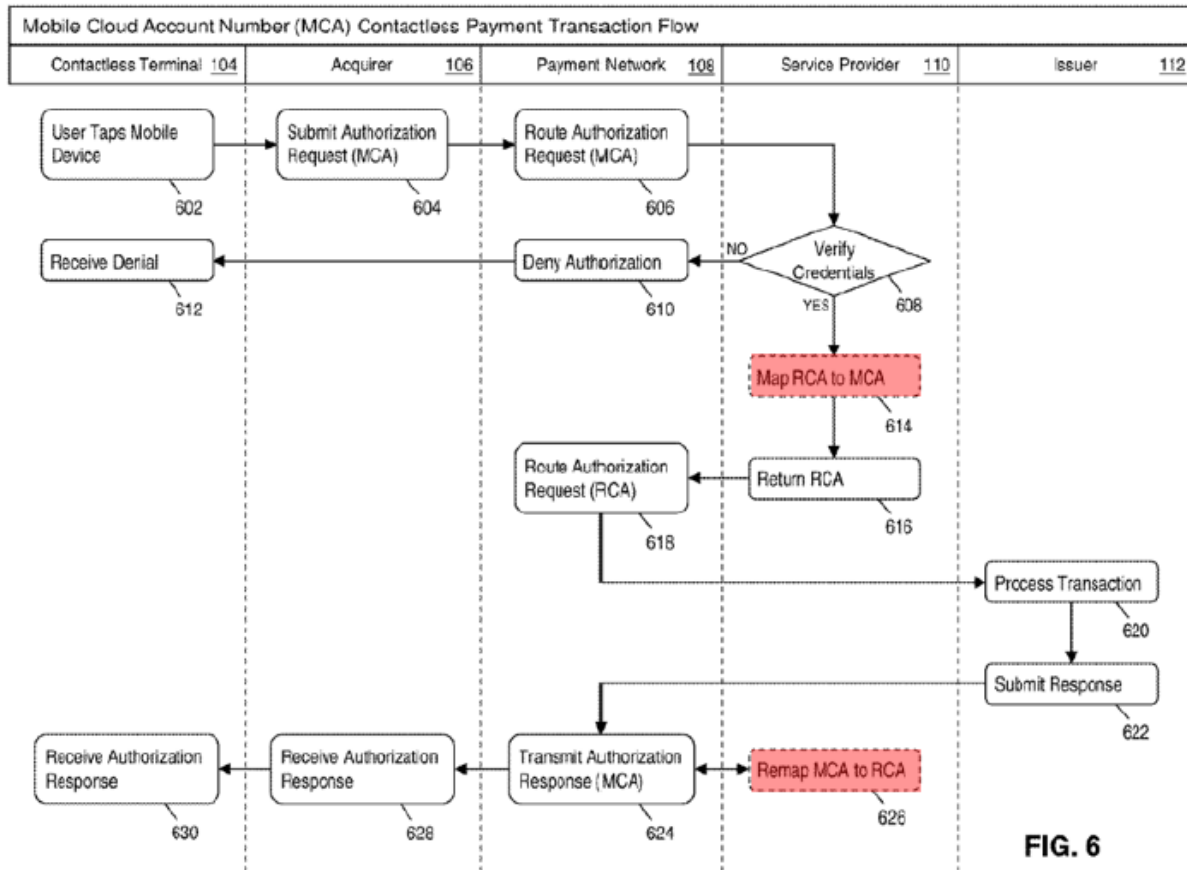
[sic] to the ATM 200 upon establishing the contactless connection.” *Id.*, 14:13-20.

This includes requiring that the user enter a valid PIN or otherwise be authenticated before initiating or otherwise carrying out a transaction. *Gill*, 5:11-20 (“the ATM is configured to ... require further security authorization in order to access the desired financial account at the ATM” and “[g]enerally speaking, the further security authorization will require at least the input of the proper PIN associated with the account”), 7:29-46 (“require users to identify and/or authenticate themselves ... before the ATM 200 will initiate, perform, complete, and/or facilitate a transaction”), 13:23-31, 13:47-51, 14:9-30, Figs. 6 (614), 7 (715). The customer can further input instructions for the transaction at the external apparatus 120 (block 720), and the apparatus 120 in turn transmits the instructions to the ATM over the contactless connection (e.g., NFC). *Id.*, 14:31-38, 17:56-62.

As part of the transaction, *Gill* describes the mobile device transmitting, and the ATM receiving, account information relating to the transaction, such as “account number, name, expiration date, debit/credit, etc.” and a “security code[.]” *Id.*, 5:11-18, 11:7-14, 12:29-32. *Gill* describes a range of possible transactions that can be performed with a mobile device and ATM, including withdrawals, deposits, and fund transfers. *Id.*, 14:32-36.

B. Smith

Smith describes techniques for conducting contactless payment transactions with a mobile device. *Smith*, [0002]. Smith teaches a mobile device that maintains “mobile cloud accounts” in a virtual wallet, where any of the mobile cloud accounts can be used to conduct a contactless transaction. *Smith*, [0032]-[0037]; *see also id.*, [0029] (“Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.”). “A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA).” *Id.*, [0034]. “The RCA may correspond to a payment account issued to the user by an issuer 112,” and “[t]he MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.” *Id.* “As a result, the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.” *Id.*



Smith, Fig. 6 (annotated).

As shown in Figure 6, *Smith* discloses that a user initiates a contactless transaction by tapping his/her mobile device at a terminal. *Id.*, [0066]-[0067]. The mobile device then transmits to the terminal “payment credentials” for the transaction, where the “payment credentials” include the “MCA” for the account desired for the transaction, a “payment cryptogram” such as “an authorization request cryptogram or dynamic card validation code ... [and] a mobile personal identification number (PIN).” *Id.*, [0067]-[0068]. The payment credentials are received by an acquirer, which in turn forwards the credentials to a service provider

that “verif[ies] (e.g., validate[s]) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art.” *Id.*, [0067], [0069]-[0070].

C. Kay

Kay generally describes techniques to “allow greater access to a banking platform via a mobile device.” *Kay*, Abstract. For example, “the customer can initiate a financial transaction using a mobile device,” and the mobile device provides a user interface with which the user can interact to facilitate the transaction, such as an ATM transaction. *Id.*, [0004]; *see also id.*, [0038]-[0043], [0051]-[0052], Figs. 3, 4A-4E.

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

D. Gomez

Gomez describes a payment card system that purports to address “[t]he problems of fraud and identity theft that result from the use of payment cards, such as credit and debit cards” when cardholders conduct a payment transaction that

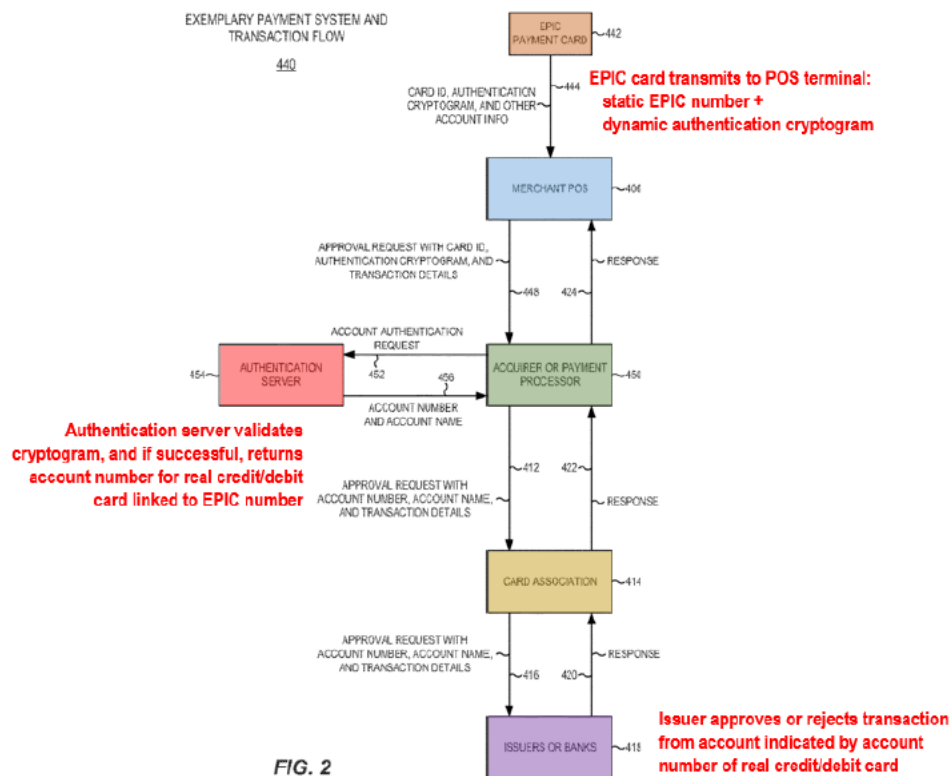
“leaves behind all the information necessary for another person to be able to make an unauthorized payment card transaction.” *Gomez*, 1:31-48. To address this problem, Gomez describes an improved payment system for conducting financial transactions. *Gomez*, 5:7-13. Gomez teaches “[a] payment card system uses a static payment card identifying number and generates, for each attempted transaction, an authentication cryptogram based at least upon a seed value stored within the payment card and further based upon a temporal signal value that changes for each attempted use of the payment card.” *Gomez*, Abstract. Gomez describes that its payment card can communicate the identifying number and cryptogram to the payment processing system via NFC. *Gomez*, 7:49-59, 8:3-24, Figs. 3-4. Because the authentication cryptogram is time-limited, “the information that can be gleaned from a payment card ... is rendered useless for making an unauthorized subsequent transaction.” *Id.*, 5:7-11, Fig. 7.

In Gomez, customers of the system are issued an electronic payment card, referred to as an “EPIC” card, which has a static card identifying number corresponding to the customer’s EPIC account. *Id.*, 2:19-39, 5:13-24. The customer can link one or more actual credit/debit cards to his or her EPIC account by entering the account numbers and other pertinent information into an online EPIC portal, which the EPIC system then stores and links to the customer’s static EPIC payment

card identifying number. *Id.*, 20:1-29. The customer can then use the EPIC card to make payment transactions with any of the linked card accounts.

During a transaction, such as an NFC transaction, the customer card dynamically generates an “authentication cryptogram” from a seed value and temporal signal. *Gomez*, 7:17-48; *see also* 5:25-32, 8:3-10, 8:25-9:11, 14:3-7, Fig-5. The card number, cryptogram, and other account information are sent for authorization to a payment processor, authorization server, and/or issuer. *Id.*, 7:49-8:2, 8:3-24, 17:13-19:22, Figs. 3-4, 16-18.

An illustration of Gomez’s payment transaction approval process is shown in Figure 2, in an embodiment:



Gomez, Fig. 2 (annotated).

E. 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 Gill*, Abstract, 1:53-59, 3:6-15, 3:51-67, 4:28-34, 5:13-27, Figs. 1, 7; *Smith*, [0002], [0005], [0035], [0049], [0061], [0066]-[0073], Fig. 6; *Kay*, [0025], [0051]-[0052], Figs. 3, 4A-4E; *Gomez*, 7:49-59, 8:3-23, 10:53-57, 14:3-7; *Dec.*, ¶¶91-115.

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 Gill*, 1:32-40, 4:35-42; *Smith*, [0003], [0034], [0040]; *Kay*, [0003], [0050]; *Gomez*, 1:32-62, 2:19-25, 4:64-5:18, 17:15-18, 21:37-40; *Dec.*, ¶¶91-115.

V. GROUND 1: CLAIMS 18-21 AND 24 ARE OBVIOUS OVER *GILL, SMITH, AND KAY*⁵

A. Claim 18

- 1. 18(Pre): *A method of facilitating and authorizing an automated teller machine (ATM) transaction involving an electronic device, wherein an electronic device transacts wirelessly with an ATM, the method comprising:***

To the extent the preamble is a limitation, the Gill-Smith-Kay combination renders obvious the recited method, as detailed below. For example, Gill discloses “methods ... for receiving a contactless transmission from an external apparatus to an ATM.” *Gill*, 4:28-34; *see also id.*, Abstract. The external apparatus can be a mobile device (electronic device) having a contactless transmission interface that allows the mobile device to transact wirelessly with the ATM. *Id.*, 5:13-18 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received ...”), 3:56-63 (“[T]he term ‘tap’ or ‘tapping’ may refer to bringing an external apparatus close to or within the proximity of an ATM contactless interface so that information can be communicated wirelessly between the external apparatus and the ATM using short range wireless transmission technology, such [as] near-field communication (NFC) technology, radio-frequency (RF) technology, or the like.”), 9:63-10:4 (“A ‘mobile device’ 500 may be any mobile communication

⁵ Dr. Clifford Neuman addresses background technology as of the Critical Date at Ex. 1003, ¶¶45-92.

device, such as a cellular telecommunications device (i.e., a cell phone or mobile phone), personal digital assistant (PDA), ... or the like.”), Fig. 5. Gill describes a range of possible transactions that can be performed with a mobile device and ATM, including withdrawals, deposits, and funds transfers. *Id.*, 14:32-36.

Gill further describes techniques for authorizing an ATM transaction, e.g., by requiring that the user enter a valid PIN or otherwise be authenticated before initiating or otherwise carrying out a transaction. *Gill*, 5:11-20 (“the ATM is configured to ... require further security authorization in order to access the desired financial account at the ATM” and “[g]enerally speaking, the further security authorization will require at least the input of the proper PIN associated with the account”), 7:29-46 (“require users to identify and/or authenticate themselves ... before the ATM 200 will initiate, perform, complete, and/or facilitate a transaction”), 13:23-31 (“memory 520 may include such data as user authentication information to gain access to the mobile wallet application 521, user authentication information for each payment vehicle that is stored by or accessible via the mobile wallet application 521, user authentication information to access the secure module 581 of the mobile wallet chip 580, etc.”), 13:47-51, 14:9-30, Figs. 6 (614), 7 (715).

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

Gill-Smith-Kay renders obvious providing, by the mobile (electronic) device, account information, identification, and authorization for the ATM transaction.⁶
Dec., ¶121.

a) Gill's Teachings

Gill teaches the mobile device provides “payment vehicle data” to the ATM terminal via a contactless/wireless connection when a user “taps” the mobile device at the ATM. *Gill*, 5:11-20 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received (i.e. account information, for example, *account number, name, expiration date, debit/credit*, etc.) and require further security authorization in order to access the desired financial account at the ATM.”), 7:64-8:2, 11:7-14, 11:34-53, 12:19-32, 13:41-46 (“typical content to be transferred from the external apparatus 120 includes *data identifying the financial account associated with the external apparatus*”), Figs. 6-7.

“[P]ayment vehicle data” includes payment “vehicle type, the payment vehicle number, the name associated with the payment vehicle, the expiration date

⁶ Although Petitioner addresses all three recited items (i.e., account information, identification, and authorization), only one is required to satisfy this claim element.

of the payment vehicle, the security code associated with the payment vehicle, ... etc.” (*account information*). *Id.*, 12:29-32 (“the antenna and other hardware or software that **transmit payment vehicle data** from the secure module 581 of the mobile device 500 may be integrated into the secure module 581”); *see also* 7:64-8:2, 11:7-16 (“**payment vehicle data 571** for each payment vehicle that is stored in the secure module 581 may include the **payment vehicle type**, the **payment vehicle number**, the **name associated with the payment vehicle**, the **expiration date** of the payment vehicle, the **security code** associated with the payment vehicle, ... etc.”), 13:32-51. *Dec.*, ¶¶122-123. Gill additionally teaches that the user inputs authentication information, such as a “username, password, PIN, biometric information, and/or one or more other credentials,” to the ATM. *Gill*, 7:29-38; *see also* 5:15-20 (“security authorization will require at least the input of the proper PIN associated with the account”), 13:47-51, 14:9-30, Figs. 6-7.

Claim 20 of the '520 Patent describes “user entered identification and authorizing information” recorded through the user interface as including “a key press PIN sequence received at the touch sensor.” *See, e.g., '520 Patent (EX1001)*, Claim 20; *see also*, 11:27-42 (describing entry of a username and passcode to pre-authorize a user for a transaction), Claim 21 (“wherein the identification and authorizing information is recorded responsive to the user inputting information

using input methods provided by the ATM to record at least one of a PIN number”).

b) Smith’s Teachings

In the combination, and based on Smith, the mobile device providing account information via a contactless/wireless connection includes a mobile cloud account number (MCA) (*identification*) and a payment cryptogram and (*authorization*) *for the ATM transaction*, in addition to other payment credentials described by Smith and Gill. *Dec.*, ¶¶124-125. Smith teaches a mobile device providing payment credentials to a contactless terminal, such as a MCA, payment cryptogram, and online PIN. *Smith*, [0067]-[0068] (“The term ‘tapping’ may refer to the transmission of *payment credentials* via near field communication from the mobile device 102 to the contactless terminal 104[.] ... *The payment credentials may include a payment cryptogram* ... [.] The contactless terminal 104 may forward the *payment credentials, including the MCA and payment cryptogram*, to the acquirer 106[.] credentials may include a mobile personal identification number (PIN)”; *see also* [0034] (“A mobile cloud account may include a *mobile cloud account number (MCA)*, which may be associated with a *real card account number (RCA)*. The RCA may correspond to a payment account issued to the user by an issuer 112.”), [0035]-[0036], [0041], [0045], [0061], [0067]-[0068], [0086], Fig. 6; Section IV.B.. The payment credentials are forwarded to a service provider that validates the MCA,

payment cryptogram, and other credentials. *Smith*, [0037]-[0039], [0067], [0069]-[0071].

The MCA functions to identify the requested account, e.g., it is linked to a real card account number (RCA) by the service provider, and the RCA “correspond[s] to a payment account issued to the user by an issuer 112.” *Smith*, [0034], [0067]. The MCA and cryptogram are packaged as payment credentials in an “authorization request” and used by a service provider and/or issuer to validate the request or deny authorization for a transaction. *Id.*, [0067], [0070]-[0072], Fig. 6; *infra*, Claim 18(g). Thus, the MCA is information provided for identification of the account to be used and the cryptogram is provided for authorization of the transaction. *Dec.*, ¶125.

c) Motivation to Combine

As discussed above, Gill describes techniques for using a mobile device in a contactless transaction at an ATM. *Supra*, Section IV.A. When a user presents the mobile device to a contactless reader (e.g., one having an NFC interface) at the ATM, the mobile device in Gill wirelessly conveys transaction information to the ATM for a requested transaction. *Gill*, 5:11-20, 13:43-51, 14:31-37, Fig. 7. Gill notes that “typical content to be transferred ... includes data identifying [a] financial account” for the transaction, such as “account number, name, expiration date, debit/credit, etc.,” a security code, a username and a PIN (account information, identification and authorization). *Id.*, 5:13-20, 11:7-13, 13:41-51, Fig. 6. A POSITA

would have understood that the username and PIN in a payment vehicle is used to authenticate a user during the authorization process. *Dec.*, ¶126. The ATM and a backend payment infrastructure then processes the information conveyed from the mobile device to complete the transaction. *Id.*, 5:13-20, 11:7-13, 13:41-51, Fig. 6.

Gill does not provide much detail about the specific information conveyed by the mobile device in a transaction request, or how such information might be secured and deployed to identify a desired payment account and authorize a transaction. *Dec.*, ¶127. It would have been obvious to a POSITA to consider references with additional implementation details and modify Gill in view of Smith such that the mobile device in Gill would be adapted to convey to the ATM at least “payment credentials” for a requested transaction, as credit card, debit card and ATM transactions typically use a payment credential, such as the mobile cloud account number (MCA) and a payment cryptogram (identification and authorization), as taught in Smith, in addition to other account information described in Gill, such as the account name, expiration date, and identification of credit or debit (account information). *Dec.*, ¶127.

Applying Smith’s proposed use of payment credentials—including an MCA and payment cryptogram—in Gill’s system would have been obvious to a POSITA by the time of the ’520 patent. *Dec.*, ¶128. As an initial matter, Gill and Smith each describe mobile devices and systems that operate in highly similar contexts. *Dec.*,

¶129. Indeed, both Gill and Smith describe mobile devices adapted for contactless transactions, and the mobile devices described in the references are each configured with a virtual wallet to hold a collection of payment vehicles, cards, or accounts for use in a given transaction. *Gill*, 10:34-53, 11:3-16, 13:3-31, Fig. 5; *Smith*, [0041], [0075], Fig. 2. Gill further focuses on ATM transactions, and explains that an ATM transaction ordinarily involves (among other things) “debit” transactions—i.e., among the same types of transactions for which Smith’s device was specifically intended to support. *Gill*, 2:1-2 (“initiate a debit account transaction”), 4:62-63 (“with ATM transactions, the transaction is generally a debit account transaction”); *Smith*, [0029] (“Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.”), [0031] (“debit cards”).⁷ A POSITA thus would have understood Smith’s payment credentials and expected them to be operable in ATM transactions like those discussed in Gill. *Dec.*, ¶129.

Moreover, a POSITA would have sought to use payment credentials like Smith’s MCA and payment cryptogram in the combination with Gill (and Kay, as

⁷ Apart from debit account transactions, Gill and Smith both describe systems operable to perform transactions conducted with a credit card or credit account. *See, e.g., Gill*, Abstract, 2:4-5; *Smith*, [0029]-[0031]

described below) to realize predictable security improvements. *Dec.*, ¶130. For example, since the MCA is merely a token for the real card account number (RCA), per Smith, the mobile device can store the MCA without needing to store the RCA, thereby mitigating the risk of the RCA being leaked, hacked, or otherwise compromised from the mobile device itself, or even any transaction involving the mobile device. *See Smith*, [0034] (“As a result, the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.”), *id.*, (“A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA). The RCA may correspond to a payment account issued to the user by an issuer 112. The MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.”); *Dec.*, ¶129-133.

Conducting contactless transactions with the MCA, and generated cryptogram, rather than the RCA would also improve security by preventing unauthorized actors from exploiting the MCA in fraudulent transactions. *Dec.*, ¶134. Because the MCA must be paired with a valid cryptogram for each transaction, a stolen MCA would be insufficient by itself to conduct a fraudulent transaction without a new, validly generated cryptogram. *Smith*, [0070] (“In step 608, the service

provider 110 may receive the MCA and additional payment credentials if applicable and may verify (e.g., validate) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art.”), [0040] (“The use of the MCA may enable the user of the mobile device 102 to more securely conduct a contactless payment transaction without using an RCA.”); *Dec.*, ¶134.

Additionally, cryptograms in payment devices were common long before the ’520 patent. *Dec.*, ¶¶131, 135. A payment cryptogram like Smith’s provides additional security by enabling a transaction processor to verify that the payment credentials submitted in a transaction originated from an authorized device and/or user. *Dec.*, ¶135. For example, Smith teaches that the cryptogram is generated based on device secrets and other data stored on the mobile device (referred to as “mobile cloud account data”)—thereby ensuring that unauthorized actors who lack such secrets cannot fraudulently generate a valid cryptogram. *Smith*, [0007], [0067], [0077], [0086], [0103]. A POSITA likewise would have sought to require submission of a valid payment cryptogram in ATM transactions of the Gill-Smith-Kay combination to further improve security and reduce the likelihood of fraudulent transactions. *Id.* The security enhancements stemming from use of both an MCA and a cryptogram in contactless ATM transactions (e.g., credit/debit transactions at an ATM) would have furthered Gill’s objectives of providing for secure transactions

with an ATM. *See Gill*, 1:34-36 (“The absence of contactless functionality with ATMs in the marketplace is largely due to security issues ...”), 4:35-55; *Dec.*, ¶135.

Integrating Smith’s suggested use of payment credentials, including an MCA and payment cryptogram, in ATM transactions like Gill’s would have amounted to an obvious application of known techniques to improve a similar system in substantially the same way as described in Smith, and would have achieve merely predictable results (e.g., more secure transactions). *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (a supposed invention that “simply arranges old elements with each performing the same function it had been known to perform” is obvious); *Dec.*, ¶136. Indeed, Gill recognizes that ATMs had not “enjoyed the benefits of contactless transactions, while numerous point-of-sale (POS) contactless terminals have been made available” and notes that financial institutions “do not wish to institute contactless ATM terminals that do not utilize any security verification.” *Gill (EX1004)*, 4:35-384:51-55. Thus, a POSITA would have been motivated to combine Gill and Smith to provide more secure contactless ATM transactions. As noted, Gill and Smith each describe mobile devices for contactless transactions (both including credit and debit transactions), and the system in the resulting combination would utilize such payment credentials in substantially the same way taught by Smith. *Dec.*, ¶136; *Smith*, [0011], [0029], [0067], [0096], Fig. 6; *Gill (EX1004)*, 14:1-37, Fig. 7. For each of these reasons, the combination would have been obvious and a POSITA

would have expected a high likelihood of success in pursuing its implementation to yield the predictable result of more secure payment transactions. *Dec.*, ¶136.

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

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

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

Gill teaches that “the mobile device 500 may have a *user interface* that includes user output devices 536 and/or user input devices 540.” *Gill*, 12:33-44, Fig. 5. “The user output devices 536 may include a *display 530* (e.g., a liquid crystal display (LCD) or the like)” *Id.* “The user input devices 540, which may allow the mobile device 500 to receive data from a user 110, may include any of a number of devices allowing the mobile device 500 to receive data from a user, such as a *keypad, keyboard, touch-screen, touchpad*, microphone, mouse, joystick, other pointer device, *button, soft key*, and/or other input device(s).” *Id.*, 12:33-44. A POSITA would have understood that a touch-screen and touchpad would include

touch sensors to permit positional detection of a user's contact with the touch-screen or touchpad, respectively. *Dec.*, ¶139. The “touch sensor array” of ’520 Patent refers to a “touchscreen panel” or “keypad.” *’520 Patent (EX1001)*, 6:31-33 (“A user input may be made via the touch sensor array 245, which may comprise a touchscreen panel, a keypad, or a combination thereof.”), 9:19-25, Figs. 2B, 4A. A keypad and keyboard would each include mechanical buttons, while a graphical user interface on a touchscreen would include virtual or soft buttons such as the buttons 415, 420 and buttons 440 like those depicted in the GUIs disclosed in Kay (and applied to the Gill-Smith-Kay combination). *Kay*, Figs. 4B, 4D; *see* Claims 18(d)-(e). A POSITA would have known of mobile devices as of the Critical Date of the ’520 patent whose user interfaces commonly included such physical display elements, including touch sensors and buttons for a touchscreen display. *Dec.*, ¶¶140-141.

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

Even if Claim 18(b) is interpreted to require multiple physical displays, a POSITA would have known that mobile devices like Gill's and Smith's can include multiple displays, and it would have been obvious and beneficial to provide multiple displays in the mobile device of the Gill-Smith-Kay combination to expand options available for displaying information to a user. *Dec.*, ¶143. A POSITA would have

appreciated that the provision of multiple displays would allow for different sets of information to be presented to the user simultaneously or at different times thereby expanding viewing options for the user to interact with. *Dec.*, ¶143.

To the extent the term “displays” encompasses virtual display elements on a physical display, the combination also provides such features. *Dec.*, ¶144. Kay, for example, discloses a series of display screens that each depict multiple display elements allowing a user to input instructions for an ATM transaction, such as displays of elements 415, 420 for selecting a desired transaction type and other displays. *Kay*, Figs. 4A-4; *see also* Claims 18(d)-(e). Smith similarly describes having multiple display elements corresponding to accounts that can be selected for a transaction. *Smith*, [0075], Fig. 7.

4. ***18(c): recording a user selection from the user interface of the electronic device of a user selected account from which the electronic device is operable to wirelessly convey with an ATM; and,***

Gill-Smith-Kay renders obvious recording a user selection from the user interface of the mobile device (*electronic device*) of a user-selected account from which the device is operable to wirelessly convey with an ATM. *Dec.*, ¶145.

a) Gill’s Teachings

For example, Gill discloses that “the GUI for the mobile wallet application 521 may *allow the user 110 to enter input to select a payment vehicle*” (*user selection from the user interface ... of a user selected account*) for a transaction. *Gill*,

13:9-17; *see also id.*, 4:1-6 (“the term ‘payment vehicle’ may refer to an electronic payment vehicle, such as an ‘electronic credit or debit card’” or other “account identifying information stored electronically in a mobile device”), 10:41-46. The mobile device is operable to convey data corresponding to the selected payment vehicle (*user selected account*) to an ATM over a wireless or contactless interface such as NFC (*wirelessly convey with an ATM*). *Id.*, 5:13-16 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received (i.e. account information, for example[] ...)”), 6:42-49 (“The contactless interface 300 is configured to contactlessly and/or wirelessly send and/or receive information over relatively short ranges[.]”), 10:47-53, 13:33-46.

b) Smith’s Teachings

In the combination, Smith also discloses that the user can select a particular account from a GUI to cause the mobile device to wirelessly convey payment credentials corresponding to the selected account (including an MCA and payment cryptogram). *Smith*, [0035] (“The user may indicate, using the mobile device 102, one of the MCAs to be used to fund a financial transaction ... The mobile device may then transmit payment credentials for the indicated mobile cloud account data to a contactless point-of-sale terminal via near field transaction.”), [0045], [0067]-[0068], [0075] (“The wallet 202 may store the mobile cloud account 704 and related data (e.g., MCA, post issuance scripts, etc.) for selection by the user 302 for use in

a contactless payment transaction.”), Figs. 6-7; *Dec.*, ¶147. The payment credentials are conveyed wirelessly via NFC. *Smith*, [0035], [0049], [0059], [0061], [0067] Fig. 5.

A POSITA further would have understood and/or it would have been obvious for the mobile device to record the user’s selection from the user interface. *Dec.*, ¶148. This is evident, for example, from the fact that the mobile device properly acts on the user’s selection by conveying information to the ATM for the correct account in accordance with the user’s selection. *Id.*; *Smith*, [0035], [0049], [0059], [0061], [0067]-[0068], [0075]; *Gill*, 5:13-16, 13:9-17, 14:31-37; *Dec.*, ¶148.

5. *18(d): recording a user selection from the user interface of the electronic device of a user selected account operation, wherein said user selected account operation is selected from a list of funds transfer operations; and,*

a) Gill’s Teachings

Based on *Gill*, it would have been obvious for the device to present a GUI that allows the user to enter transaction instructions “indicating what type of financial transaction the authenticated user wants to conduct at the contactless ATM.” *Gill*, 18:19-22; *Dec.*, ¶149.

Gill discloses that a customer can “input[] instructions to [an] ATM 200 to execute [a] desired transaction.” *Gill*, 14:31-36. “The desired transaction may be any type of ATM transaction such as, for example, withdrawing funds, depositing funds, transferring funds, balance checks, ordering products such as checks, and the like.”

Id.; see also *id.*, 4:1-3, 5:14-16, 9:15-25 (disclosing a “credit card” as another payment vehicle for an ATM transaction in lieu of a “debit card”). Gill teaches the user can select among transaction types that include “***withdrawing funds, depositing funds, transferring funds, balanc[ing] checks, ... and the like.***” *Id.*, 14:31-37; 19:12-19 (“***[R]eceive financial transaction instructions*** from an authenticated user associated with the external apparatus via the connection between the contactless ATM and the communication sticker affixed to the external apparatus, ***wherein financial transactions include withdrawing, depositing, or transferring funds and ordering financial institution products***”). Figure 7 shows the user inputting transaction instructions at the mobile device (external apparatus 120):

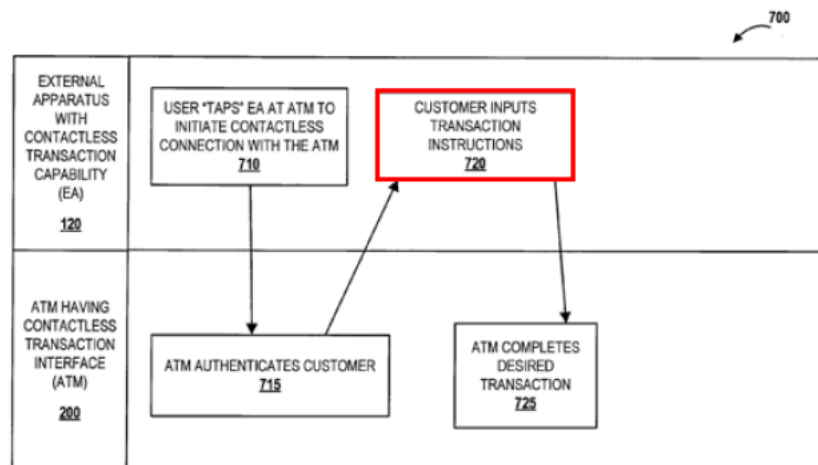


FIG. 7

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

Gill also indicates that the user can input instructions for an ATM transaction (including selecting the desired type of transaction) at the mobile device rather than the ATM, and the user's instructions are then communicated from the mobile device to the ATM via NFC or another short-range wireless connection. *Id.*, Fig. 7 (depicting instructions input at box 720 through the external apparatus (mobile device) 120), 16:58-64, 18:19-22. The mobile device can also include a "graphical user interface (GUI) that allows the user to perform various transactional processes" and that "allow[s] the user to set certain payment preferences or mobile wallet preferences." *Id.*, 10:42-46; *see also id.*, 13:9-17, Fig. 5.

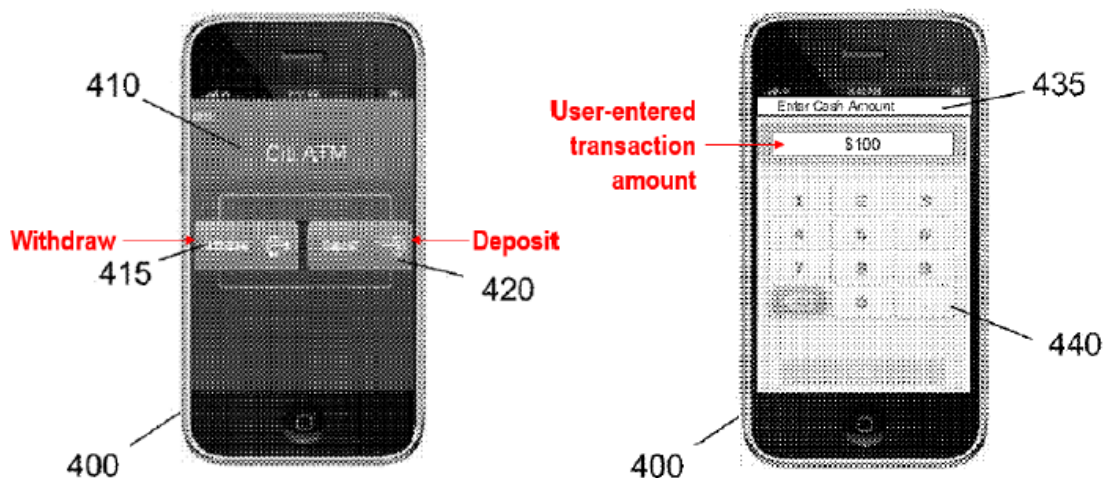
Nonetheless, Gill does not expressly depict the GUI and lacks detail as to how the user would specifically interact with the GUI to input instructions or select a particular type of ATM transaction.

b) Kay's Teachings

Based on Kay, it would have been obvious for the user to select from the GUI a desired ATM funds transfer operation from a list that includes, for example, depositing and withdrawing funds from an account. *Dec.*, ¶153. Kay demonstrates such GUIs adapted to receive user instructions for ATM transactions on a mobile device were known well before the '520 Patent. *Dec.*, ¶154.

Kay, like Gill, discloses a method of conducting ATM transactions using a mobile device including a touchscreen. *Kay*, [0017]-[0021], [0038]-[0052], Figs. 1,

3, 4A-4F. The mobile device includes a mobile banking and wallet application that “allow[s] a user to wirelessly conduct transactions (e.g., payments, account transfers) using one or more accounts of the customer without a credit card or debit card present” *Id.*, [0039], [0035]. The application includes a user interface that allows a user to “choose a category of instructions or transactions.” *Id.*, [0040]. As shown in Figure 4B (reproduced below), the user interface “present[s] options for ‘withdraw’ 415 and ‘deposit’ 420.” *Id.*, [0040]. “The customer can select withdraw 415 to withdraw cash from the financial transaction terminal,” or select deposit 420 to deposit funds into an account. *Id.* The GUI also allows a user to enter a PIN or other credentials for authentication, and to input an amount for the transaction such as a withdrawal amount as shown in Figure 4D:



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

Kay's teachings in this regard would have been obvious to apply to the combination with Gill and Smith for the reasons described below. *Dec.*, ¶156. In the combination, the GUI would predictably allow the user to select from a list of funds transfer operations such as "withdrawing funds, depositing funds, transferring funds, ... and the like." *Id.*; *Gill*, 14:31-37.

c) Motivation to Combine

A POSITA would have understood and/or it would have been obvious that the mobile device records the user's election of the user's indicated operation, including funds transfer options. *Dec.*, ¶156. This is evident, for example, from the fact that the mobile device properly acts on the user's selection by proceeding to carry out the indicated operation. *Id.*; *Gill*, 5:13-16, 13:9-17, 14:31-37, Fig. 7; *Kay*, [0040]-[0041]; *Smith*, [0067]-[0068], [0075].

It would have been obvious to a POSITA to apply in the combination Kay's teaching of a graphical user interface (GUI) on a mobile device, which would allow a user to select a particular type of transaction, such as those described in Gill and Smith, from a list of available transaction types. *Dec.*, ¶157. Multiple reasons would have motivated a POSITA to implement a GUI like Kay's in the mobile device of the Gill-Smith-Kay combination, in particular a GUI adapted to receive user input for an ATM transaction including a user's selection of a desired transaction type (e.g., withdrawing, depositing, or transferring funds) and an indication of a desired

amount for the transaction. *Id.* To start, such a GUI would have facilitated the user's ability to interact with a mobile device to carry out ATM transactions in the manner described in Gill and Smith, which already teach a GUI and touchscreen display. *Id.* As noted above, Gill's original solution already contemplated that the mobile device would include a GUI for the user to input instructions for ATM transactions. *Gill*, 10:41-46, 13:9-17, 14:31-36, Figs. 5, 7. Kay's GUI provides concrete design elements for a GUI in a similar context, which would allow a user to enter instructions for aspects of the desired transaction (e.g., the transaction amount and type) in a logical and intuitive layout on a small screen of a mobile device (e.g., by guiding the user through a series of interface screens for different stages of the transaction and providing selectable elements in a list of available transaction types). *Kay*, [0038]-[0052], Figs. 1, 3, 4A-4F; *Dec.*, ¶157. By providing a list of selectable transaction types and allowing the user to progress through different interface screens, the user could conveniently enter instructions on the mobile device without needing to separately enter instructions through the ATM. *Dec.*, ¶157.

Additionally, integrating a GUI like Kay's into the resulting combination would have involved no more than a predictable use of a known GUI as taught in Kay to improve similar devices (i.e., devices with GUIs) in substantially the same way, and would have achieved merely predictable results (e.g., more secure transactions). *KSR*, 550 U.S. at 417; *Dec.*, ¶158. Kay's GUI is designed for ATM

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

6. ***18(e): wherein user input information from the user interface includes at least one of a set comprising: identification, account, amount of currency, operation and authorizing information; and,***

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

a) Gill’s Teachings

Gill teaches a user can input identification, account, operation and/or authorizing information to perform an ATM transaction. For example, Gill teaches that “the ATM 200 may require users to identify and/or authenticate themselves to the ATM[.]” *Gill (EX1004)*, 7:29-32. For example, the user may be authenticated based on a username and PIN. *Gill (EX1004)*, 7:32-38; *see also*, 14:15-21 (“the customer may input authentication information on his external apparatus 120 and [] transfer such data to the ATM 200 upon establishing the contactless connection.”), 13:23-31, 7:29-44 (“[T]he ATM 200 may require users to identify and/or authenticate themselves to the ATM[.]”), 14:9-20. For example, the user inputs identification and authentication information, such as a “username, password, PIN,

biometric information, and/or one or more other credentials,” to the ATM. *Gill* (EX1004), 7:29-38; *see also* 5:13-20 (“[T]he ATM is configured to process the data received (i.e. account information, for example, **account number**, **name**, expiration date, debit/credit, etc.) and require further security authorization in order to access the desired financial account at the ATM. Generally speaking, the further security authorization will require at least the input of a PIN associated with an account”), 13:47-51, 14:9-20, Figs. 6-7. As discussed in Claim 18(a), the ’520 Patent describes that “user entered identification and authorizing information” includes “a key press PIN sequence.”

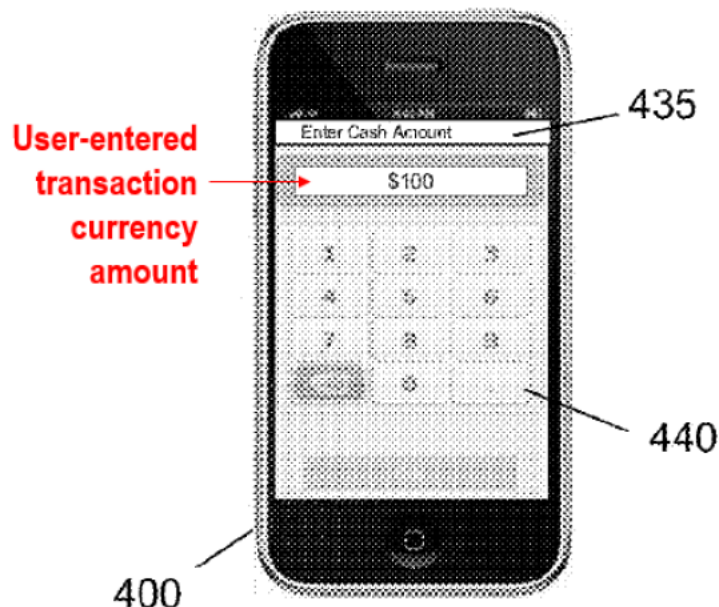
Gill further describes user inputs from the user interface regarding a payment vehicle (account information). *Gill*, 13:14-15 (“The GUI for the mobile wallet application 521 may allow the user 110 to enter **input to select a payment vehicle**”), 12:33-35, 13:9-17; *supra*, Claim 18(a). Gill similarly teaches the user provides inputs authentication information, e.g., password or biometric information, to the ATM. *Gill*, 7:29-38; *see also* 5:15-20 (“the security authorization will require at least the input of a PIN associated with an account”), 13:47-51, 14:9-30, Figs. 6-7. Thus, to the extent such information is “authorizing information” under the claim, Gill teaches it.

Gill also describes user inputs received at the mobile device directed to operations of the device, including withdrawing, depositing and transferring funds.

Gill, 13:12-16, 14:9-37, Fig. 7 (715-720) (depicting the user inputting instructions to the external apparatus 120 to execute the desired transaction); *see also*, 14:31-37.

b) Kay's Teachings

In the combination, Kay also discloses the mobile device receiving user input information from a user interface indicating an amount of cash to withdraw (*amount of currency*) for a transaction. *Kay*, [0043] (“In 340, the customer enters the amount of cash to withdraw and confirms the transaction. A shown in FIG. 4D, a mobile device 400 has a user interface that prompts the customer to ‘Enter Cash Amount’ 435 using a keypad 440 on a touchscreen of the mobile device 400 ...”); *Dec.*, ¶163; *see also* Claim 18(d).



Kay, Fig. 4D (annotated).

c) Motivation to Combine

A POSITA would have understood and/or it would have been obvious that Gill's mobile device would allow for the input of a currency amount. *Dec.*, ¶164; *see also* Claim 18(d). Gill already teaches that the customer inputs instructions to the mobile device to, for example, withdraw funds. *Gill*, 14:31-36, Fig. 7. It would have been obvious to a POSITA to apply Kay's teachings of allowing for input of a currency amount for such withdrawal because, absent such input, the ATM would not know how much money to disperse. *Dec.*, ¶164. A POSITA would have been motivated to implement this functionality in order to make the mobile device carry out the functionality described by Gill on the mobile device. *Id.* Kay's GUI allowing entry of a currency amount provides a concrete design element for a GUI similar in context to Gill that would allow a user to enter such instructions in a logical and intuitive way. *Id.* This combination would have involved the predictable use of a known GUI, as taught by Kay, to improve similar devices with GUIs in and would have achieved a predictable result of a payment device that guides a user various steps of a transaction. *Dec.*, ¶165. A POSITA would have had a reasonable expectation of success combining the teachings of Kay with those of Gill and Smith in this manner. *Id.*

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

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

Gill discloses that information exchanged between the mobile device and the ATM, such as the PIN and transaction information occur wirelessly via near-field communications (NFC) (*exchanged wirelessly between the electronic device and the ATM via NFC*). *Gill*, 3:56-67 (“the term ‘tap’ or ‘tapping’ may refer to bringing an external apparatus close to or within the proximity of an ATM contactless interface so that information can be communicated wirelessly between the external apparatus and the ATM using short range wireless transmission technology, such ***nearfield communication (NFC) technology***”), 4:28-34, 14:13-20, 5:11-18, 6:43-50, 13:41-46 (“typical content to be transferred from the external apparatus 120 includes data identifying the financial account associated with the external apparatus”). For example, as shown in FIG. 7, “the customer taps the external apparatus 120 at the ATM 200 to ***initiate a contactless connection with the ATM***,” and proceeds to exchange wirelessly the identification, selection, information and authorizing operations as described above with respect to Claims 18(a) and (c)-(e). *Gill*, 13:51-14:37; *see also*, 13:32-51, Figs. 1-3, 5-6.

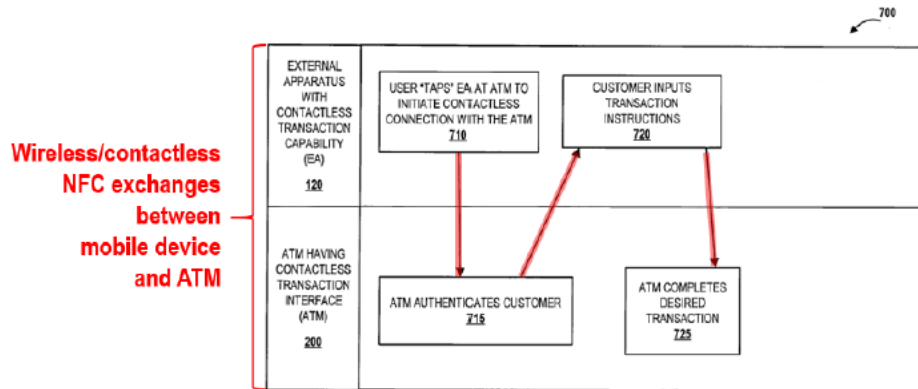


FIG. 7

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

Smith also discloses, and the combination provides, for the exchange of payment credentials (including an MCA, payment cryptogram and PIN) via NFC between the mobile device and a terminal. *Supra*, Claim 18(a); Section VII.B. The payment credentials are useful to identify and authorize the device for a transaction, and they correspond to an account indicated by a user's selection. *Smith*, [0067] ("The term 'tapping' may refer to the transmission of **payment credentials** via near field communication from the mobile device 102 to the contactless terminal 104 due to the close proximity of the mobile device 102 to the terminal 104. The **payment credentials may include a payment cryptogram** The contactless terminal 104 may forward the **payment credentials, including the MCA and payment cryptogram**, to the acquirer 106[] ..."); *see also* [0034]), [0045], [0058]-[0059] (describing user's selection of a payment account for a transaction), Figs.5- 6; *supra*, Claim 18(a).

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

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

Gill-Smith-Kay renders obvious configuring the ATM to perform the user selected account operation using identification and authorization information received wirelessly from the mobile device. *Dec.*, ¶171; *supra*, Claims 18(a), (c)-(f). For example, Gill teaches that the ATM authenticates the customer based on credentials (e.g., account name, expiration date, security code, username, and/or PIN) received wirelessly from the mobile device. *Gill*, 14:17-20 (“the customer may input authentication information on his external apparatus 120 and such transfer such data to the ATM 200 upon establishing the contactless connection”), 13:47-51 (“ATM 200 authenticates the user”), Figs. 6 (612, 614), 7 (715). Once the ATM receives further transaction instructions, Gill discloses that the ATM is configured to “execute the desired transaction.” *Id.*, 14:31-37, Fig. 7 (720, 725); *see also*, 5:11-20, 7:29-46 (“ATM 200 will initiate, perform, complete, and/or facilitate a transaction”).

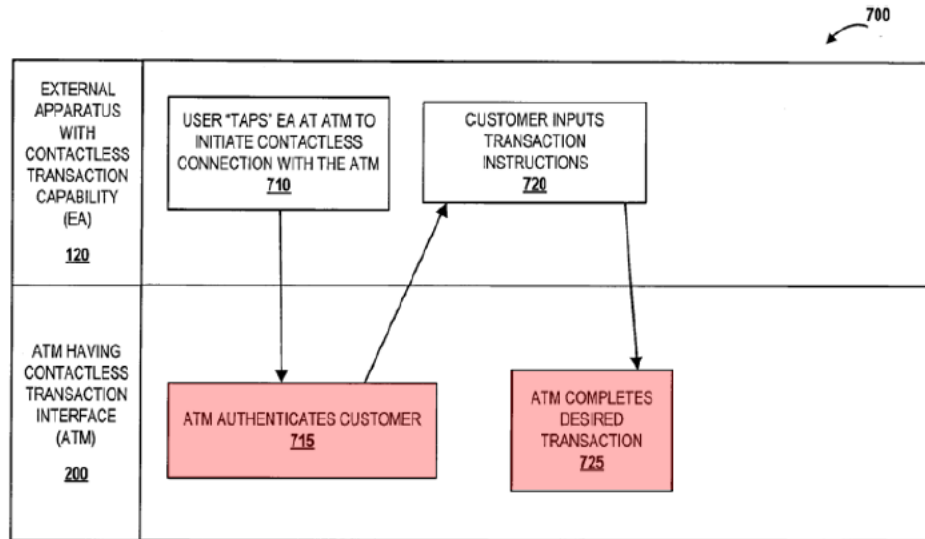


FIG. 7

Gill, Fig. 7 (annotated).

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

In the combination, the ATM is configured to perform the user selected account operation using the MCA, payment cryptogram, username and PIN (*identification and authorizing information*), such as the MCA, payment cryptogram, and/or PIN, as discussed above in Claim 18(a). *See Smith*, [0035], [0041], [0045], [0049], [0061], [0067]-[0068]; *Dec.*, ¶173; *supra*, Claim 18(a).

9. ***18(h): wherein the identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions; and,***

Gill-Smith-Kay renders obvious exchanging wirelessly with an ATM transaction data including account, identification, and authorizing information, as discussed above. *Supra*, Claims 18(a), (b)-(f); *Dec.*, ¶174.

Based on Smith, it would have been obvious for the wireless exchange to involve transmission of a mobile card account number (MCA) and a payment cryptogram (*identification and authorizing information*) from a mobile device to a terminal. *Smith*, [0067]-[0068] (“In step 602, the user 302 may ‘tap’ the contactless terminal 104 using the mobile device 102 with payment credentials loaded into the mobile card let in the secure storage 210. ... The *payment credentials may include a payment cryptogram*, such as an authorization request cryptogram or dynamic card validation code[] ... The contactless terminal 104 may forward the payment credentials, *including the MCA and payment cryptogram* ... The mobile device 102 may also transmit additional credentials to the contactless terminal ... includ[ing] a mobile personal identification number (PIN)[.]”), Fig. 6; *see also*, [0035]-[0036], [0045], [0051] (“MCAs for use in conducting contactless payment transactions”), [0061]; Claim 18(a); *Dec.*, ¶175.

The MCA is a *statically generated limited-use number portion* of the payment credentials provisioned to the mobile device, and is linked by a service provider to

a real card account number (RCA) for an actual account of the user. *Smith*, [0040] (“The use of the MCA may enable the user of the mobile device 102 to more securely conduct a contactless payment transaction without using an RCA.”), [0034] (“The RCA may correspond to a payment account issued to the user by an issuer 112. The MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.”). The MCA remains unchanged and static across transactions initiated by the mobile device, but has a limited period of use defined by an expiration date assigned to the MCA. *Id.*, [0086] (“the generated MCA may include an expiration date”); *Dec.*, ¶176.

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

The significance of the cryptogram having a dynamic, limited-use would have been apparent to a POSITA, as it was commonly understood that updating the cryptogram, such as a dynamic card validation code, on a frequent basis (e.g., with each transaction or some other period of time) protects against the risk of payment credentials (including the MCA and cryptogram) from a prior transaction being reused by an illicit actor to conduct a fraudulent transaction with the same credentials. *Dec.*, ¶178. Smith explains that the service provider can identify and authorize a transaction request by verifying the cryptogram using known techniques. *Smith*, [0070] (“the service provider 110 may receive the MCA and additional payment credentials if applicable and may verify (e.g., validate) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art”). The service provider’s verification of the MCA and associated cryptogram identifies that the transaction request was initiated from an authorized user’s device, and can be used to validate the request or deny authorization for the transaction. *Id.*, [0070] (“If the verification of the credentials fails, then, in step 610, the payment network 108 may receive an indication from the service provider 110 to deny the authorization”), [0071]-[0072]. It would have been obvious to apply Smith’s suggested use of statically and dynamically generated limited-use number portions, including an MCA and

cryptogram, in the resulting combination for the reasons discussed above. *Supra*, Claims 18(a), (f)-(g); *see also Dec.*, ¶178.

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

Smith discloses, and the combination renders obvious, that the MCA and payment cryptogram (said static and dynamic information) are combined into “payment credentials” to form an authorization request for performance of a user selected operation. *Smith*, [0067] (“the payment credentials, **including the MCA and payment cryptogram**”; “‘tapping’ may refer to the transmission of payment credentials via near field communication from the mobile device 102”), Fig. 6 (602); *see also*, [0035]-[0036], [0045], [0059] (“the user 302 may (e.g., via the display UI 204), select an MCA for use in funding a contactless payment transaction”), [0061]; *Dec.*, ¶179.⁸

⁸ Smith alternately refers to the MCA and payment cryptogram being combined to form “transaction data.” *Smith*, [0011] (“The receiving device is configured to receive transaction data related to a financial transaction, wherein the transaction data includes at least an MCA and a payment cryptogram.”), [0096] (“In step 1104, a receiving device may receive transaction data related to a financial transaction, wherein the transaction data may include at least an MCA and a payment cryptogram.”).

In the combination as described above, the MCA and cryptogram are combined into payment credentials, with additional information, to perform a user-selected ATM operation such as a deposit, withdrawal, or funds transfer operation like those described in Gill, Smith, and Kay. *Gill*, 14:34-37; *see also*, *Smith*, [0029] (“Transactions that may be performed via a payment network include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.”), [0031] (“Payment cards may include ... debit cards”); *Kay* (*EX1006*), [0017] (“Financial transactions include ... deposits, withdrawals, account transfers[.]”), [0031], [0040]; *supra*, Claims 18 (a), (c)-(g); *Dec.*, ¶180.

B. Claim 19

1. ***19. A method of claim 18, wherein the identification and authorizing information is generated from at least one of a set identification and data comprising: ATM accounts; user identification; biometric user identification; device-identifiers; email address; username; transactional information; merchant identifiers; facility location; user accounts; cryptocurrency address; cryptocurrency keys; merchant accounts; online accounts; bank accounts; device account numbers; payment numbers; card issuing authority; and payment-issuer;***

and wherein further the data includes at least one of time; duration; passwords; passcodes; device position; device motion; device specifics; secrets; keys; a currency; currency amounts; cryptocurrency amount; transaction limits; transaction records; usage duration; and usage sequence counts.

Gill teaches that “account information” and/or “payment vehicle data” that includes an account name (*user identification* or *username*), an account number

(*payment numbers, ATM accounts, bank account*), and an expiration date and debit/credit account (*transaction information*) is provided to the ATM. *Gill*, 5:11-20 (“Upon tapping the external apparatus at the ATM, the ATM is configured to process the data received (i.e. *account information*, for example, *account number, name, expiration date*, debit/credit, etc.)”), 11:7-16, 12:29-32, 13:12-16.

Gill further describes identification and authentication information provided through user input, such as a username and PIN (*secrets, passwords, passcodes*) or biometric information (*biometric user identification*). *Id.*, 5:18-20 (“the further security authorization will require at least the input of the proper *PIN* associated with the account”), 7:34-40 (“authenticate an ATM user based at least partially on an ATM debit card, smart card, token ..., username, password, PIN, biometric information, and/or one or more other credentials”), 14:13-20; *Dec.*, ¶182. This information is *identification and authorizing information* used by the ATM in performing the transaction. *Dec.*, ¶182.

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

1. The cryptogram is generated based on secret mobile cloud account data stored on the mobile device, including the MCA, secrets and a key. *Smith*, [0067] (“The payment credentials may include a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code, generated based on at least a portion of the mobile cloud account data stored in the secure element 210.”), [0086] (“The mobile cloud account data 802 may include at least the issuer public key certificate, the ICC public key certificate, and the MCA. In some embodiments, the generated MCA may include an expiration date, which may be further included in the mobile cloud account data 802. In one embodiment, the mobile cloud account data 802 may further include static track data and initialization vectors”); *Dec.*, ¶184. A POSITA would have been aware of the benefits of using multiple data elements to generate a dynamic cryptogram, unique to the transaction, device, and account, as described in Hammad, for use in a financial transaction and, therefore, would have been motivated to do the same in order to make the transaction and the user’s account information more secure. *Dec.*, ¶184.

Accordingly, the MCA and cryptogram (identification and authorizing information) are generated from at least a device account number/payment number/bank account/device identifier, secret and a key. The PIN is a passcode. In the combination, the complete transaction data or payment credentials are generated from these pieces of information. *Dec.*, ¶185.

C. Claim 20

1. ***20. A method of claim 18, wherein user entered identification and authorizing information is recorded through the user interface of the electronic device from at least one of set including: a plurality of button-press actions; a swipe gesture received at a touch sensor of the electronic device; a key press sequence received at the touch sensor; a passcode sequence received at the buttons; a plurality of swipe gestures received at a touch sensor of the electronic device; a key press PIN sequence received at the touch sensor; a passcode sequence received at the touch sensor; an accelerometer sensor indicating a user motion of the electronic device; an action and sequence of motions of the electronic device as performed by a user; an action of the user to move the electronic device into a specific orientation; a biometric sensor confirming the electronic device is in a grip of the user; and a biometric sensor confirming the electronic device has remained in the possession of the user from activation to transaction.***

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

Kay similarly teaches that the user enters a “PIN,” “username and password, or a biometric credential” to the mobile device. *Kay*, [0041]-[0042], Figs. 3, 4C (discussing one example of a user interface on a mobile phone adapted to receive a user’s entry of a PIN to authorize an ATM transaction).

A POSITA would have understood and/or it would have been obvious that the user’s entry of a PIN, passcode, or like credentials (*user entered identification and authorization information*) recorded through the user interface would include at least one of *a plurality of button-press actions, a key press sequence received at the touch sensor, a passcode sequence received at the buttons, a key press PIN sequence received at the touch sensor, or a passcode sequence received at the touch sensor.* *Dec.*, ¶¶187-188; *see also* Claims 18(c)-(e).

D. Claim 21

1. ***21. A method of claim 18, wherein the identification and authorizing information is recorded responsive to the user inputting information using input methods provided by the ATM to record at least one of a PIN number; a passcode; a password; a biometric identification; and user known secrets.***

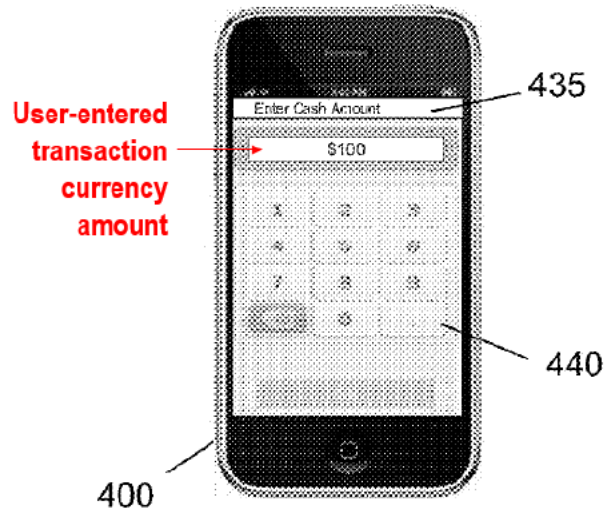
As discussed in Claims 18(e) and 20, *supra*, Gill discloses, and the combination renders obvious, identification and authorization information recorded responsive to the user inputting information using input methods provided by the ATM to record a *PIN number, password, and biometric information (biometric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

E. Claim 24

1. ***24. The method of claim of 18, wherein the amount of currency information can be a unit of value from at least one of a set of comprising: a cash amount, an amount of a debit account, an amount of credit, a maximum spending amount, a merchant account, a bank account amount, a unit of cryptocurrency, an online account funds, an payment issuer unit of funds, and a merchant account points.***⁹

As discussed with respect to Claim 18(e), Kay discloses and the combination renders obvious a mobile device that receives user input information from a user interface indicating an “amount of currency” (*cash amount*) for a transaction. *Kay*, [0043] (“In 340, the customer enters the amount of cash to withdraw and confirms the transaction. Figure 4D, for example, shows a mobile device 400 with a user interface that prompts the customer to ‘Enter Cash Amount’ 435 using a keypad 440 on a touchscreen of the mobile device 400 ...”); *Dec.*, ¶¶190-191.

⁹ The additional features recited in this claim are not limiting as they do not define further limitations of the recited method; they are nonetheless obvious.



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

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

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

A. Claim 18

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

Although Smith discloses that the payment cryptogram can be dynamic in the form of an authorization request cryptogram or a dynamic card validation code generated based on at least a portion of the mobile cloud account data (e.g., issuer public and private key and MCA) securely stored on the mobile device, Smith does not expressly disclose all details as to how the payment cryptogram would be made to change across transactions or how the cryptogram would be calculated. *Dec.*, ¶194. Nonetheless, the use of dynamic cryptograms in electronic transaction systems had been known for many years before the Critical Date of the '520 Patent. *Id.*; see also Claims 18(h), 19. A POSITA would have known many ways in which a cryptogram like Smith's could be generated so as to provide a unique value for each transaction, and to permit a service provider or issuer to use the cryptogram in authenticating and authorizing transaction requests, such as described by Gomez. *Id.*

1. Gomez's Teachings

Gomez teaches computing an authentication cryptogram based on a "temporal signal" that changes from transaction to transaction. See, e.g., Gomez, 1:58-2:1 ("[A] payment card systems that utilizes a secure authentication cryptogram which is *generated uniquely for each attempted used of the payment card*, and which expires within a short period of time thereafter. The authentication cryptogram is generated based upon a seed value stored within the payment card, and further based upon a *temporal signal which changes for each attempted use of the payment*

card[] ...”), 7:17-27 (“a temporal signal is generated which corresponds to the instance of attempted use”; “a temporal signal value may reflect the date/time of the attempted use”; “a temporal signal value may reflect the sequence value (or sequential number) of the attempted use”), 8:36-41. In Gomez, the temporal signal is combined with other data stored on the device (e.g., a seed value, such as a “unique customer key”) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. *Id.*, 2:45-50, 7:26-48, 8:25-51, 16:64-17:12, Figs. 3, 5. The cryptogram is then formed by encoding the output of the hash function. *Id.*, 2:14-17, 8:52-9:11; *Dec.*, ¶195. Gomez further teaches that the cryptogram can be transmitted with other account information (e.g., EPIC card number) in an NFC transaction. *Id.*, 7:47-57, 8:11-24, 10:54-57, 14:3-7.

Because the temporal signal changes with each attempted use, the output of the hash function and the ultimately encoded cryptogram changes with each transaction, even if the seed value remains constant. Gomez explains that “[t]he encoding of the authentication cryptogram renders it extremely difficult for an unauthorized party, without knowledge of the seed value corresponding to the payment card, to generate a new authentication cryptogram in attempt to authorize a future fraudulent transaction.” *Gomez*, 5:43-47; *see also id.*, 2:21-25 (“fraudulent use would not be possible because any attempted transaction would not be approved

without an appropriate authentication cryptogram generated uniquely for such transaction”), 1:58-63, 13:63-14:2, 14:37-39, 21:37-48; *Dec.*, ¶196.

2. *Motivation to Combine*

In the Gill-Smith-Kay combination of Ground 1, the mobile device generates for a contactless ATM transaction payment credentials that include a mobile card account number (MCA) and a payment cryptogram as taught in Smith. *Supra*, Claim 18. In the Gill-Smith-Kay-Gomez combination, the payment cryptogram is dynamically generated based on a temporal signal as taught in Gomez, in addition to mobile cloud account data of Smith, and constitutes “dynamically generated limited use number portions” as recited in Claim 18(h). *Gomez*, 1:64-2:1 (“The authentication cryptogram is generated based upon ... *a temporal signal which changes for each attempted use of the payment card* [...] ...”), 7:17-27 (“a temporal signal is generated which *corresponds to the instance of attempted use*”; “a temporal signal value may reflect the date/time of the attempted use”; “a temporal signal value may reflect the sequence value (or sequential number) of the attempted use”), 2:21-25 (“fraudulent use would not be possible because any attempted transaction would not be approved without an appropriate *authentication cryptogram generated uniquely for such transaction*”).

It would have been obvious and a POSITA would have been motivated to further modify the Gill-Smith-Kay combination of Ground 1 in view of Gomez such

that the payment cryptogram would be generated using a temporal signal and cryptographic methods like those described in Gomez. *Dec.*, ¶¶197-198. The cryptogram in the resulting combination with Gomez could be formed, for instance, by combining at least a portion of the mobile cloud account data stored on the mobile device (as taught in Smith) with a temporal signal (as taught in Gomez), hashing the combined data, and encoding the output of the hash function in a manner suitable for transmission in a contactless connection between the mobile device and the ATM. *Id.*

A POSITA would have sought to use a dynamically changing temporal signal in calculation of the cryptogram (along with a cryptographic technique such as hashing) to ensure that the cryptogram produced in each transaction would vary from prior cryptograms in an unpredictable manner, thereby frustrating the ability of illicit actors to exploit an MCA and cryptograms from prior transactions to later consummate a fraudulent transaction. *See Gomez*, 1:58-63, 2:21-25, 5:43-47, 13:63-14:2; *Dec.*, ¶199.

The application of Gomez's cryptogram techniques to the combination as described above further would have been obvious as a predictable use of known techniques (e.g., using multiple data elements to generate a cryptogram) that would have achieved no more than predictable results (e.g., increased transaction security). *KSR*, 550 U.S. at 417; *Dec.*, ¶200. Smith and Gomez each describe contactless

transactions from which the user's device submits a token account number (e.g., an MCA in Smith or an EPIC number in Gomez) paired with a cryptogram that is specifically generated to facilitate validation or authorization of a requested transaction. *See, e.g., Smith*, [0070]-[0071]; *Gomez*, 8:11-23, 14:3-11, 18:20-25, 18:54-59. The obviousness of the combination is also underscored by Smith, which expressly treats the specific manner of verifying transaction requests with a payment cryptogram as something that would have been well within the capabilities and knowledge of a POSITA. *Smith*, [0070] (“service provider 110 ... may verify (e.g., validate) the MCA and/or payment cryptogram or other credentials *using cryptography methods and systems apparent to persons having skill in the relevant art*”). Accordingly, a POSITA would have expected a high likelihood of success implementing the combination with Gomez given the similarities in the systems. *Dec.*, ¶200.

B. Claims 19-21, 24

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

C. Claim 22:

1. ***22. The method of claim 18, wherein the limited-use number dynamically generated in the device is based on cryptographically combining data selected from the group consisting of an ATM information, the locality of an ATM reader facility, information regarding the facility performing the transaction, bank information, a time of day, a date, a transaction amount, a count of past transactions, a sequence count, a historical record of transactions, a merchant account, a user's location, an online address, a device-internal secret, a device unique identifier, a payment authority key, a payment issuer authority secret, a method and direction of payment, deposit, transfer and receipt, a cryptocurrency server, a cryptocurrency type, a cryptocurrency private key, a cryptocurrency public key, a cryptocurrency address, a touch gesture, a biometrically sensed user information, a user's private information, a user key, a user email, password, passcode, a PIN, a user secret, and a user input.***

Smith discloses, and the combination renders obvious, that the payment cryptogram (i.e., the limited-use number dynamically generated in the device) is generated using cryptographic techniques based on at least portions of the mobile cloud account data securely stored on the mobile device. *Smith*, [0067] (“a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code, generated based on at least a portion of the mobile cloud account data stored in the secure element 210”). The mobile cloud account data comprises device-internal secrets such as the MCA, issuer public key certificate, and ICC public key certificate. *Id.*, [0086]. *Dec.*, ¶202.

In the combination, Gomez further teaches that the cryptogram can be generated based on a temporal signal including a “date/time of attempted use” (date, time of day,) or the instance of attempted use or “sequence value (or sequential number) of the attempted use (sequence count or count of past transactions). Gomez, 7:17-27, 8:36-41, 10:58-11:6, 17:5-12. In addition, the cryptogram is based on a seed value that is “unique for each payment card,” such as a “unique customer key” (user key). Gomez (EX1007), 7:27-43 (“This seed value is unique for each payment card, and corresponds to the payment card identifying number. ... [I]n certain embodiments, the seed value may include certain non-random customer specific information, such as a unique customer key, either alone or in addition to a pseudo-random bit string.”), Fig. 3; *see also supra*, Ground 2, Claim 18; Dec., ¶202-203. It would have been similarly obvious to use a sequence count as an additional data element in generating the cryptogram as the use of transaction sequence counters in this way was well-known at the time and a POSITA would have had a reasonable expectation of success in doing the same to generate the predictable result of increasing security given it is simply utilizing known techniques in a known way to improve similar systems (e.g., mobile payment systems). *Id.*

D. Claim 23:

1. ***23. The method of claim of 18, wherein the payment information comprises combining a plurality of static portions, and a plurality of dynamically generated limited-use portions, and wherein the static portion is a token account number with a limited-duration expiration date, to be used in place of issuer provided information.***

As discussed above in Ground 1, the mobile device in the Gill-Smith-Kay combination generates and transmits payment information that includes a mobile card account number (MCA) and a payment cryptogram as taught in Smith. *Supra*, Ground 1, Claims 18(h)-(j). Further, and as described above in Claim 18 of Ground 2, it would have been obvious to further modify the Gill-Smith-Kay combination in view of Gomez such that the duration of the cryptogram would be limited by generating it based on both a temporal signal that changes with each transaction and secret(s) stored on the device such as a seed value (as taught in Gomez) or mobile cloud account data (as taught in Smith). *Supra*, Ground 2, Claim 18; *Dec.*, ¶204.

In this context, the Gill-Smith-Kay-Gomez combination provides the additional features recited in Claim 23. For example, Smith discloses that the MCA is formed by combining a first set of digits that are different from the corresponding RCA and a second set of digits taken directly from the corresponding RCA. *Gill*, [0095] (“In one embodiment the MCA may include at least a portion of the RCA. In a further embodiment, the portion of the RCA may include at least the last four digits of the RCA.”), [0091]. Both portions of the MCA are static (plurality of static

portions), as the corresponding digits from the RCA are fixed and the remaining digits likewise unchanged for the lifetime of the MCA. *Id.*, [0086]. The MCA is a token account number with a limited-duration expiration date for use in place of the RCA (i.e., issuer-provided information). *Id.*, (“the generated MCA may include an expiration date”), [0034] (“The MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.”), [0040] (“The use of the MCA may enable the user of the mobile device 102 to more securely conduct a contactless payment transaction without using an RCA.”); *Dec.*, ¶25.

Moreover, Gomez teaches and the combination renders obvious that the cryptogram can be generated by combining a “date” and a “time” (a plurality of dynamically-generated limited use portions) to form a temporal signal used in calculating the cryptogram. *Gomez*, 7:17-24 (“At step 256 a temporal signal value is generated which corresponds to the instance of attempted use. In some embodiments such a temporal signal value may reflect the date/time of the attempted use. The ***date and time*** may be determined by a real-time clock device included within the payment card[]”), 7:41-48; *Dec.*, ¶206.

As another example, Gomez describes techniques for encoding the cryptogram into a sequence of characters (e.g., 32 characters). *See generally id.*,

14:36-17:13. With this encoding, each character represents a different portion of the message digest, and the characters (a plurality of dynamically generated limited-use portions) are combined to form the complete cryptogram. *Id.*, 15:43-51 (describing a radix-64 numbering system in which each character of the cryptogram represents 6 bits of the message digest), 15:61-65 (describing a radix-32 numbering system in which each character of the cryptogram represents 5 digits of the message digest); *Dec.*, ¶207. It would have been obvious to encode the cryptogram with higher-order characters rather than mere binary digits in order to convey more information in fewer characters, as taught by Gomez. *Gomez*, 15:17-60; *Dec.*, ¶207. Fewer numbers of higher-order characters would thus be needed to achieve the same level of security from the cryptogram as a greater number of lower-order characters, thereby permitting more secure cryptograms to be transmitted from the mobile device in fewer numbers of characters (e.g., in a fixed-length field with a limited number of characters). *Id.*; *see also id.*, 15:57-58 (“Such a code could be useful in a NFC environment”); *Dec.*, ¶208.

VII. DISCRETIONARY CONSIDERATIONS

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.

VIII. CONCLUSION

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

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
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

IX. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)

A. Real Party-In-Interest

Petitioner is the real party-in-interest. 37 C.F.R. § 42.8(b)(1).

B. Related Matters

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. The grounds of the present petition rely on identical prior art to that presented in IPR2023-00211, which was instituted but terminated prior to a final written decision. IPR2023-00211, Papers 13, 24.

Petitioner is concurrently filing a second petition challenging a different subset of claims of the '520 patent in IPR2025-01145.

C. Lead and Back-Up Counsel

Petitioners provide 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	Mark Lang (Reg. No. 55,356) Mark.Lang@eriseip.com
Postal and Hand-Delivery Address: ERISE IP, P.A.	Lydia Raw (Reg. No. 76,436) Lydia.raw@eriseip.com PTAB@eriseip.com

7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	<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. Petitioner consents 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	Excerpts from the Prosecution History of the ’520 patent (“the Prosecution History”)
Exhibit 1003	Expert Declaration of Dr. Clifford Neuman
Exhibit 1004	U.S. Patent No. 9,098,846 (“Gill”)
Exhibit 1005	U.S. Pub. No. 2013/0232083 (“Smith”)
Exhibit 1006	U.S. Pub. No. 2013/0124410 (“Kay”)
Exhibit 1007	U.S. Patent No. 9,600,808 (“Gomez”)
Exhibit 1008	Intentionally Left Blank
Exhibit 1009	Intentionally Left Blank
Exhibit 1010	Intentionally Left Blank
Exhibit 1011	Intentionally Left Blank
Exhibit 1012	Intentionally Left Blank
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 . (“IBM”)
Exhibit 1021	<i>Vedat Coskun, Near Field Communication: Theory to Practice</i> (John Wiley & Sons, 1st ed. 2012) (“Coskun”)
Exhibit 1022	<i>MagTek, Magnetic Stripe Card Standards</i> , (MagTek Inc. eds., 2011) (“MagTek”)
Exhibit 1023	<i>EMVCo, LLC, EMV Integrated Circuit Card Specifications for Payment Systems: Book 2 – Security and Key Management</i> (EMVCo, LLC eds., Version 4.3 2011) (“EMV”)
Exhibit 1024	<i>Klaus Finkenzeller, RFID Handbook</i> (John Wiley & Sons, 3rd ed. 2010) (“Finkenzeller”)
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 . (“PayPass”)

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_Approved_Mobile_Devices.pdf , [https://web.archive.org/web/20120906234255/http://www.mastercard-mobilepartner.com:80/docs/MasterCard_Approved_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	<i>Alessandro Vizzarri et al., 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. Patent No. 8,462,133 (“Lynch”)
Exhibit 1045	U.S. Patent No. 7,740,168 (“Hammad”)
Exhibit 1046	“ <i>A Note on the Use of Timestamps as Nonces</i> ,” B. Clifford Neuman, et al., ACM SIGOPS Operating Systems Review, Volume 27, Issue 2, pp. 10 – 14 (April 1993)
Exhibit 1047	U.S. Pub. No. 2002/0174075 (“Mirlas”)
Exhibit 1048	U.S. Patent No. 5,903,721 (“Sixtus”)
Exhibit 1049	WO 2010/039337 (“Lin”)
Exhibit 1050	U.S. Publn. No. 2009/0307132 (“Phillips”)

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 13,197 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**

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

IPR2025-01146

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

(913) 777-5600 Telephone

(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER