

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC
Petitioner

v.

CARDWARE INC.,
Patent Owner

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.	MANDATORY NOTICES.....	1
III.	PAYMENT OF FEES UNDER 37 C.F.R. §§42.15 AND 42.103.....	3
IV.	GROUND FOR STANDING	4
V.	PRECISE RELIEF REQUESTED AND GROUNDS RAISED	4
VI.	LEVEL OF ORDINARY SKILL.....	5
VII.	OVERVIEW OF THE '520 PATENT	6
VIII.	CLAIM CONSTRUCTION	7
IX.	DETAILED EXPLANATION OF GROUNDS	8
A.	Ground 1A: Law and Gomez Render Claims 10-13 Obvious	8
1.	Law.....	8
2.	Gomez	11
3.	Law-Gomez Combination.....	13
4.	Claim 10	18
5.	Claim 11	34
6.	Claim 12	35
7.	Claim 13.....	36
B.	Ground 1B: Law, Gomez, and Spodak Render Claims 14-17 Obvious 37	
1.	Claim 14.....	37
2.	Claim 15.....	39
3.	Claim 16.....	39
4.	Claim 17.....	40
C.	Ground 2A: Gill, Smith, Kay, and Gomez Render Claims 18-24 Obvious.....	40
1.	Gill.....	40
2.	Smith	41
3.	Kay	44
4.	Gill-Smith-Kay-Gomez Combination.....	44

5.	Claim 18.....	55
6.	Claim 19.....	72
7.	Claim 20.....	73
8.	Claim 21	73
9.	Claim 22.....	74
10.	Claim 23.....	74
11.	Claim 24.....	76
X.	DISCRETIONARY DENIAL IS NOT APPROPRIATE.....	77
XI.	CONCLUSION	77
APPENDIX A (CLAIM LISTING)		

LIST OF EXHIBITS

EX1001	U.S. Patent No. 10,339,520 to Wyatt (“the ’520 patent”)
EX1002	Prosecution History of U.S. Patent App. No. 15/701,261
EX1003	Declaration of Dr. Michael Ian Shamos, Ph.D.
EX1004-1006	RESERVED
EX1007	U.S. Patent No. 9,600,808 to Gomez
EX1008	RESERVED
EX1009	U.S. Patent Publication No. 2012/0123937 to Spodak
EX1010-1013	RESERVED
EX1014	Curriculum Vitae of Dr. Michael Ian Shamos
EX1015-1016	RESERVED
EX1017	U.S. Patent No. 5,594,233 to Kenneth
EX1018	U.S. Patent No. 5,528,222 to Moskowitz
EX1019	Martha E. Haykin et al., Computer Science and Technology, NIST Special Publication 500-157, Smart Card Technology: New Methods for Computer Access Control (1988)
EX1020-1021	RESERVED
EX1022	PCI Data Security Standard (PCI DSS), Information Supplement: PCI DSS E-commerce Guidelines (January 2013)
EX1023	Z. Honig, A week with Google Wallet, Engadget (September 19, 2011)

EX1024	RESERVED
EX1025	Kadambi et al., Near-Field Communication-Based Secure Mobile Payment Service, ACM 11th International Conference on Electronic Commerce 2009
EX1026	PCI Data Security Standard, Navigating PCI DSS: Understanding the Intent of the Requirements, Version 2.0 (October 2010)
EX1027-1028	RESERVED
EX1029	Todd Wasserman, New Credit Card has LCD Screen, Touch Sensitive Buttons, The Sydney Morning Herald (Nov. 9, 2012)
EX1030	PCI Data Security Standard (PCI DSS), Information Supplement: PCI DSS Tokenization Guidelines, Version 2.0 (August 2011)
EX1031	History of Phones, Georgia Southern University.
EX1032	U.S. Patent Publication No. 2015/0134540 to Law
EX1033	U.S. Provisional Application No. 61/673,096 to Law (“Law Provisional”)
EX1034	U.S. Patent No. 9,098,846 to Gill
EX1035	U.S. Patent Publication No. 2013/0232083 to Smith
EX1036	U.S. Patent Publication No. 2013/0124410 to Kay
EX1037	Exhibit A to CardWare Inc.’s Preliminary Infringement Contentions, <i>CardWare Inc. v. Google LLC</i> , Case No. 7:24-cv-00278 (W.D. Tex. (Feb. 13, 2025) (‘520 Patent Infringement Contentions”)
EX1038	John Wenninger et al., The Electronic Purse, Federal Reserve Bank of New York, Current Issues in Economics and Finance, Vol. 1, No. 1 (April 1995)

EX1039	Tim Noonan, Barriers to Using Automatic Teller Machines: A Review of the Usability of Self-Service Banking Facilities for Australians with Disabilities (Feb. 2000)
EX1040	U.S. Patent No. 7,004,385 to Douglass
EX1041	Geoff Walker and Mark Fihn, LCD In-Cell Touch, Information Display (Mar. 2010)
EX1042-1045	RESERVED
EX1046	Claim Construction Memorandum and Order (Dkt. 101), <i>CardWare Inc. v. Google LLC</i> , Case No. 7:24-cv-00278 (W.D. Tex. August 28, 2025)

I. INTRODUCTION

Google LLC (“Petitioner”) respectfully requests *inter partes* review of claims 10–24 (“the challenged claims”) of U.S. Patent No. 10,339,520 (“the ’520 patent”) (EX1001) assigned to CardWare Inc. (“Patent Owner”).

II. MANDATORY NOTICES

Real Parties-in-Interest: Pursuant to 37 C.F.R. §42.8(b)(1), Petitioner identifies Google LLC¹ as the real party-in-interest.

Related Matters: The ’520 patent is asserted against Petitioner in *CardWare Inc. v. Google LLC*, Case No. 7:24-cv-00278 (W.D. Tex.), filed on November 4, 2024.

The ’520 patent originates from U.S. Patent Application No. 15/701,261, filed on September 11, 2017, which is a continuation of application No. 14/981,757 filed on December 28, 2015, now Pat. No. 9,760,884, which is a continuation of application No. 14/680,979, filed on April 7, 2015, now Patent No. 9,224,083, which is a division of application No. 14/217,261, filed on March 17, 2014, now Patent No.

¹ Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.

9,022,286, which claims priority to provisional application No. 61/794,891, filed on March 15, 2013, now expired (EX1001, Cover).

Additionally, U.S. Patent Nos. 10,810,579 (“the ’579 patent”), 11,176,538 (“the ’538 patent”), and 11,620,634 (“the ’634 patent”) are also at issue in *CardWare Inc., v. Google, LLC*, Case No. 7:24-cv-00278 (W.D. Tex.). The ’579 patent originates from U.S. Patent Application No. 16/459,150, filed on July 1, 2019, which is a continuation of application No. 15/701,261, filed on September 17, 2017, now Pat. No. 10,339,520. The ’579 patent is related to the ’538 patent and the ’634 patent. The ’634 patent originates from U.S. Patent Application No. 17/528,073, filed on November 16, 2021, which is a continuation of application No. 17/075,637, filed on October 20, 2020, now the ’538 patent, which is a continuation of application No. 16/459,150, filed on July 1, 2019, now the ’579 patent. Petitioner is concurrently filing IPR petitions challenging the ’579, ’538, and ’634 patents.

The ’579, ’520, and ’538 patents were asserted in *CardWare Inc., v. Samsung Electronics Co., Ltd. et al*, Case No. 2-22-cv-00141 (E.D. Tex), which was filed on May 11, 2022, and voluntarily dismissed on October 31, 2023. The ’634 patent was asserted in *CardWare Inc., v. Samsung Electronics Co., Ltd. et al*, Case No. 2-23-cv-00187 (E.D. Tex), which was filed on April 24, 2023, and voluntarily dismissed on October 31, 2023 before any substantive motions or orders. The ’579 patent was at issue in *Samsung Electronics Co., Ltd. v. CardWare Inc.*, IPR2023-00196

(PTAB); the '520 patent was at issue in *Samsung Electronics Co., Ltd. v. CardWare Inc.*, IPR2023-00210 (PTAB) and *Samsung Electronics Co., Ltd. v. CardWare Inc.*, IPR2023-00211 (PTAB); and the '538 patent was at issue in *Samsung Electronics Co., Ltd. v. CardWare Inc.*, IPR2023-00219 (PTAB). IPR2023-00196 and IPR2023-00211 were terminated after the parties settled after the decision on institution of trial, while IPR2023-00210 and IPR2023-00219 were denied institution.

The '579, '634, '520, and '538 patents are also at issue in *CardWare Inc. v. Apple Inc.*, Case No. 7:24-cv-00279 (W.D. Tex.), which was filed on November 4, 2024.

Counsel and Service Information: Lead counsel is Naveen Modi (Reg. No. 46,224). Backup counsel are Daniel Zeilberger (Reg. No. 65,349), Robert Laurenzi (Reg. No. 45,557), Jason Mikus (Reg. No. 71,911), Alexa Lowman (*pro hac vice* to be filed), and Maksim Mints (Reg. No. 78,507). Service information is Paul Hastings LLP, 2050 M Street NW, Washington, D.C. 20036, Tel.: 202.551.1700, Fax: 202.551.1705, email: PH-Google-Cardware-IPR@paulhastings.com. Petitioner consents to electronic service.

III. PAYMENT OF FEES UNDER 37 C.F.R. §§42.15 AND 42.103

The PTO is authorized to charge any fees due during this proceeding to Deposit Account No. 50-2613.

IV. GROUNDS FOR STANDING

Petitioner certifies under 37 C.F.R. §42.104(a) that the '520 patent is available for review and Petitioner is not barred or estopped from requesting review on the grounds identified herein.

V. PRECISE RELIEF REQUESTED AND GROUNDS RAISED

Petitioner respectfully requests review of claims 10-24 of the '520 patent. The challenged claims should be found unpatentable on the following grounds:

Ground 1A: Claims 10-13 are unpatentable under 35 U.S.C. §103 as being obvious in view of Law (EX1032) and Gomez (EX1007).

Ground 1B: Claims 14-17 are unpatentable under §103 as being obvious in view of Law, Gomez, and Spodak (EX1009).

Ground 2A: Claims 18-24 are unpatentable under §103 as being obvious in view of Gill (EX1034), Smith (EX1035), Kay (EX1036), and Gomez.²

Each of these references is prior art even assuming the earliest possible priority date of the '520 patent is March 15, 2013 (“the Critical Date”).³ Law

² The Gill-Smith-Kay-Gomez ground challenging claims 18-24 was previously instituted by the Board in IPR2023-00211, which settled before final decision.

³ Petitioner does not concede that the '520 patent is entitled to a March 15, 2013 priority date.

published from an application filed April 16, 2013, claims priority to provisional application No. 61/673,096 (“Law Provisional”) filed July 18, 2012 (EX1033, Cover), and qualifies under at least pre-AIA §102(e). Gomez issued from an application filed June 22, 2012 (EX1007, Cover); Gill issued from an application filed on May 6, 2011 (EX1034, Cover); Smith published from an application filed March 1, 2013 (EX1035, Cover); Kay published from an application filed November 15, 2011 (EX1036, Cover); and each qualifies under at least §102(e). Spodak published May 17, 2012 (EX1009, Cover), and qualifies under at least §102(a) and (e).

The above-listed prior art was not identified during prosecution. *See generally* EX1002.

VI. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) at the time of the alleged invention of the ’520 patent would have had an undergraduate degree in electrical engineering, computer engineering, computer science or a related field along with one to two years of work experience with payment processing and/or digital authentication systems, including familiarity with short-range wireless technologies.

EX1003, ¶¶38-43.⁴ More education can supplement practical experience and vice versa. *Id.*

VII. OVERVIEW OF THE '520 PATENT

The '520 patent describes electronic or smart card devices capable of generating a “limited-duration number” for use in a payment transaction. EX1001, 2:14-3:4, FIG. 7. Figure 7 illustrates a process for generating and using a limited-duration number:

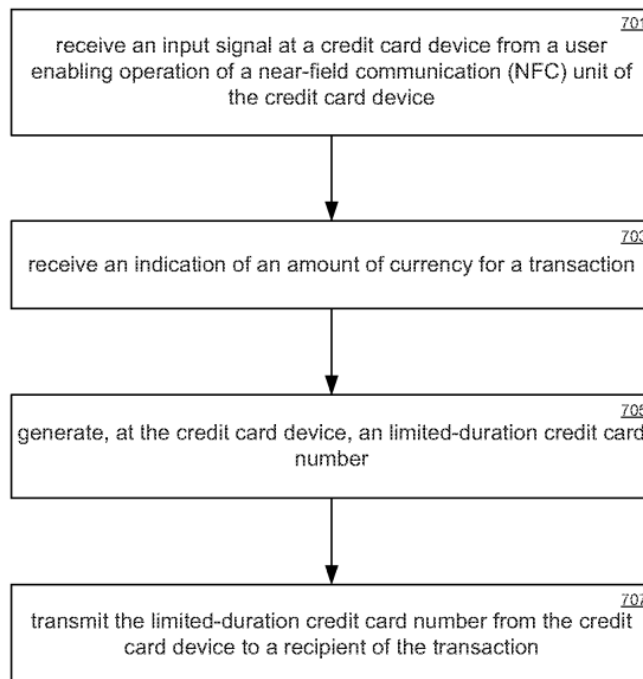


FIG. 7

EX1001, FIG. 7.

⁴ Petitioner submits the declaration of Dr. Michael Shamos (EX1003), an expert in the field of the '520 patent. EX1003, ¶¶38-43; EX1014.

“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.” *Id.*, 10:18-23.

VIII. CLAIM CONSTRUCTION

Given the correlation between the prior art references and the challenged claims of the ’520 patent, the Board need not construe any terms of the challenged claims to resolve the underlying controversy, as any reasonable construction reads on the prior art.⁵

On August 28, 2025, Magistrate Judge Gilliland issued a Claim Construction Memorandum and Order in the parallel litigation in the Western District of Texas. *See generally* EX1046. Nonetheless, because of the close parallel between the prior art and claims, Petitioner does not believe that the Board needs to construe any terms here.

⁵ Petitioners reserve all rights to raise claim construction and other arguments in other venues.

IX. DETAILED EXPLANATION OF GROUNDS

A. Ground 1A: Law and Gomez Render Claims 10-13 Obvious

1. Law

Law is entitled to the filing date of the Law Provisional because (1) at least one claim of Law is supported by the Law Provisional, and (2) the subject matter relied upon in Law is also described by the Law Provisional. The following chart demonstrates the enabling support found in the Law Provisional for claim 4 of Law. The analysis for each claim element in the Grounds also includes supporting citations to the Law Provisional.

Law Claim 4	Exemplary Disclosures of the Law Provisional (Ex. 1033)
4. A computer-implemented method comprising:	EX1033, [0033], [0034], [0063].
registering a funding card comprising storing a funding card number;	EX1033, [0050]-[0053], [0110], FIG. 10.
receiving a message from a mobile device indicating a desire to make a payment using the registered funding card;	EX1033, [0054], [0066]-[0072], [0079].

Law Claim 4	Exemplary Disclosures of the Law Provisional (Ex. 1033)
computing data for a virtual card, wherein the data for the virtual card comprises a virtual card number that is different than the funding card number;	EX1033, [0072]-[0073], [0076]-[0079], [0100], [0113]-[0114].
storing the data for the virtual card in association with the funding card number;	EX1033, [0051]-[0052], [0109]-[0114].
sending information related to the data for the virtual card to the mobile device;	EX1033, [0051]-[0052], [0062], [0070]-[0073], [0111]-[0113].
receiving a first payment authorization request from a merchant or a merchant acquirer, the first payment authorization request comprising the data for the virtual card and a requested payment amount;	EX1033, [0054], [0084]-[0088].

Law Claim 4	Exemplary Disclosures of the Law Provisional (Ex. 1033)
retrieving the funding card number based on the data for the virtual card;	EX1033, [0054], [0086]-[0091].
sending a second payment authorization request to a funding card issuer, the second payment authorization request comprising the funding card number and the requested payment amount;	EX1033, [0054], [0087]-[0093].
receiving a payment authorization response from the funding card issuer; and	EX1033, [0055], [0087]-[0093].
sending the payment authorization response to the merchant or the merchant acquirer.	EX1033, [0048], [0087]-[0093].

Law describes “facilitating a payment transaction at a merchant location using a virtual card on a mobile device.” EX1032, [0002]; EX1033, [0001]. Law describes that an “NFC-enabled mobile device can be equipped with a ‘software payment card’ (e.g. a software implementation of a contactless payment card) application running inside the mobile device. The software payment card uses the compatible contactless communication capabilities of the device to interact with contactless-enabled POS terminal to facilitate payment transactions.” EX1032, [0062]; EX1033, [0034].

Law explains that when “a contactless funding card credential is used to facilitate a payment transaction, the transaction most often includes dynamic data from the card to securely authenticate the payment credential.” EX1032, [0069]; EX1033, [0041]. Law further describes that a static number may be acquired by the mobile device and used in place of a user’s actual credit card number. *See* EX1032, [0082]; EX1033, [0052]. The Law system also describes use of transaction counters, key values and cryptographic hashing, among other values, in producing dynamic data for the payment transaction. EX1032, [0142]-[0155]; EX1033, [00109]-[00122].

2. Gomez

Gomez describes a mobile payment system “utiliz[ing] a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card,

and which expires within a short period of time thereafter.” EX1007, 1:58-63, 7:17-48. Customers of the system described in Gomez are issued an electronic payment card, referred to as an “EPIC” card. *Id.*, 2:19-39. The EPIC card has a static payment card identifying number which identifies the payment card. *Id.*, 2:25-31. The customer can link a credit card account to the EPIC account by entering the account number and other pertinent information of the credit card account into an online EPIC portal. *Id.*, 2:19-39; *see also id.*, 20:1-29. The customer can then use the EPIC card to make payment transactions. *Id.*, 2:35-37.

When a customer initiates a transaction with an EPIC card, the card dynamically generates an “authentication cryptogram” based on a unique “seed value” stored securely in the card and a “temporal signal” that changes with each attempted use or transaction. *Id.*, 7:17-48. The payment card transmits the static EPIC number (i.e., static payment card identifying number) and the dynamically-generated authentication cryptogram to the point-of-sale (POS) terminal, which is then conveyed to an authentication server (e.g., EPIC) before the transaction request is sent to an issuer or bank for approval. *Id.*, 7:49-8:82, FIG. 2. The authentication server authenticates the transaction using the cryptogram, and if successful, the authentication server returns the actual account number for the customer’s linked credit/debit card to the acquirer or payment processor, which information is then

forwarded to the appropriate card association and issuer or bank for approval. *Id.*, 18:4-42, FIGS. 2, 17-18.

3. Law-Gomez Combination

A POSITA would have beneficially applied the teachings of Gomez to Law to modify Law's mobile payment system to include multiple improvements, as explained below, that complement Law's focus on secure cryptogram generation for payment transactions. EX1003, ¶¶126-133. The teachings of Law and Gomez would have rendered obvious and provided each element of claims 10-13 for the reasons discussed below. EX1003, ¶¶126-133.

It would have been obvious and beneficial to augment the payment information communicated by the device in a contactless transaction as taught in Law with a tokenized static payment card identifying number like that taught in Gomez (such that the presented payment information would include both a static number and limited-use authentication cryptogram dynamically generated for each transaction). EX1003, ¶127; EX1007, 1:58-63, 6:23-38, 7:17-65, 8:3-41, FIGS. 2-5, 17-18. Law discloses wirelessly receiving a funding card identifier (i.e., a tokenized static account number which identifies a user's actual credit card account). EX1032, [0082]; EX1033, [0052]; EX1003, ¶127. Law's funding card identifier is held on the payment application on a user's mobile device in place of the user's actual credit card number for security purposes. *Id.* During the payment transaction

process, Law uses the funding card identifier to create limited-use payment information such as a cryptographically hashed one-time use number. EX1032, [0147], [0149]-[0154]; EX1033, [0114]. Law does not expressly disclose that the funding card identifier is sent as part of the complete payment information when performing a payment transaction. Gomez describes a “static payment card identifying number”—also referred to as an “EPIC” number—stored on the electronic device. EX1007, 2:25-39; *see also id.*, 1:63-64, 13:45-14:2, 22:49-51, 6:10-12, 18:57-59. The EPIC number “identifies the payment card, but does not represent a live account.” *Id.*, 5:13-18. Gomez uses this static payment card identifying number in combination with an authentication cryptogram when performing a payment transaction. *Id.*, 7:9-8:51. Multiple reasons would have led a POSITA to apply Gomez’s suggested use of a static payment card identifying number in combination with an authentication cryptogram with Law before the Critical Date of the ’520 patent. EX1003, ¶127.

The addition of the tokenized static number with an authentication cryptogram would have improved transaction security by preventing fraudulent use of a substituted or incorrect account number. EX1003, ¶128. By requiring both a tokenized static number and authentication cryptogram as part of the complete payment information, an additional layer of security would be realized to prevent unauthorized actors from exploiting any compromised portion of the payment

information. EX1003, ¶128. Additionally, a payment processing authority would more easily identify the user's actual account number for processing a transaction with the presence of the user's tokenized static account number in the payment information because that tokenized static account number is linked to the user's actual account. EX1032, [0082]; EX1033, [0052]; EX1007, 5:13-18; EX1003, ¶128.

Further, a POSITA would have seen the addition of Gomez-like payment information (i.e., a static number and cryptogram used together) as a useful technique to improve security in a manner that would still be compatible with existing merchant payment infrastructure, particularly since that payment information would be capable of transmission in ordinary account name fields, security code fields, or both. EX1007, 2:4-13, 2:40-44, 7:52-57; EX1032, [0075] (“additional infrastructure . . . is not required”); EX1033, [0046]; EX1003, ¶129. Further, the fact that Gomez is directed to a smart payment card while Law is directed to a mobile device does not teach away from the proposed combination. Indeed, Gomez's payment card is not a traditional credit card but instead contains a processor that functions to compute dynamic payment information based on seed values and/or temporal signals, like Law. EX1007, 1:58-2:1, 2:14-17, 2:21-25, 5:43-47, 7:17-27, 8:42-9:11, 13:63-14:2. Therefore, a POSITA would have implemented

Gomez's payment information generation technique with a smartphone, as in Law. EX1003, ¶129.

Additionally, a POSITA would have recognized the benefits of hashing functions in payment transactions. EX1003, ¶130. Law discloses an algorithm and hashing functions used in generating the payment information. EX1032, [0146]-[0155]; EX1033, [0113]-[0122]. Law specifically states that SHA256 and HMAC are known cryptographic hash functions that are used in discretionary data generation. *Id.* Gomez discloses use of a cryptographic hash function to generate a message digest, from which the authentication cryptogram is ultimately derived for a payment transaction. EX1007, 8:42-43; *see also id.*, 8:44-48, 9:58-10:3, 21:55-59. A POSITA would have understood and it would have been obvious that the discretionary data/message digest would be stored in a memory of the device for at least some time to allow processing to form the cryptogram. EX1032, [0095], [0155]; EX1033, [0065], [0122]; EX1007, 11:7-9; *infra*, [10.f]; EX1003, ¶130. The cryptogram itself would also be processed and stored on the device for at least some time to permit its inclusion in the payment message(s) transmitted from the device to a terminal in a transaction. *Id.* A POSITA would have recognized that the cryptographic hashing functions described in Gomez would be beneficially applied to Law as a useful technique to improve security in payment transactions. EX1003, ¶130.

Moreover, a POSITA would have recognized that Law and Gomez each disclose communicating payment information via NFC communication, and a POSITA would have recognized that integrating Gomez's payment card functionality into a mobile device such as a smartphone would have reduced the number of devices that a user needs to carry while also improving the user experience due to the improved user interfaces and processing power of smartphone devices of the time. EX1032, [0088]; EX1033, [0058]; EX1007, [14:3-7]; EX1003, ¶131. Among other considerations, use of a multi-functional payment device in lieu of a card was known to be desirable to increase the convenience of retail and other payment transactions to users. EX1003, ¶131.

Additionally, given that the use of dynamic payment information in electronic transaction systems had been known for many years before the Critical Date, the combination amounts to a predictable use of a known technique for improving transaction security (i.e., Gomez's payment information) to improve a similar system as taught in Law in a similar way, and would have achieved predictable results. *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); EX1003, ¶132.

In the combination, the teachings of Law in view of Gomez would have rendered obvious claims 10-13, and the combination would have provided each element of these claims for the reasons described below. EX1003, ¶133.

4. Claim 10

i) [10.pre]

To the extent limiting, Law discloses an electronic device capable of storing and generating payment information. EX1003, ¶134. For example, Law discloses “facilitating a payment transaction at a merchant location using a virtual card on a mobile device.” EX1032, [0002]; EX1033, [0001]. Law explains that “contactless payment is well suited for a mobile device. For example, some mobile devices have a near-field communication (NFC) system that allows data to be transferred wirelessly” with another contactless-enabled device “by touching them together or keeping them into close proximity.” EX1032, [0061]; *see also id.*, [0062]; EX1033, [0033]-[0034].

ii) [10.a]

Law discloses a device in which issuer provided payment information is entered at a touch screen display. EX1003, ¶¶135-136; EX1032, [0092]; EX1033, [0062]. Law discloses “cardholder 101 registers one or many funding cards and their mobile device with a virtual card issuer 401” and the “cardholder’s mobile device includes a payment application that can interact with the virtual card issuer 401.” EX1032, [0081]; EX1033, [0051]. Law further describes the process

of registering a funding card with a virtual card issuer. EX1032, [0082] (“[T]he user enters in (e.g. types in) card details into the mobile device (e.g. card details include the name printed on the funding card, the PAN⁶ printed on the funding card, the expiry date printed on the funding card, and the static security code printed on the funding card). The mobile device sends this data, plus a user provided PIN and the mobile device ID to the payment gateway server.”), [0142]; EX1033, [0052], [0109].

Figure 10 of Law illustrates these steps:

Registration process

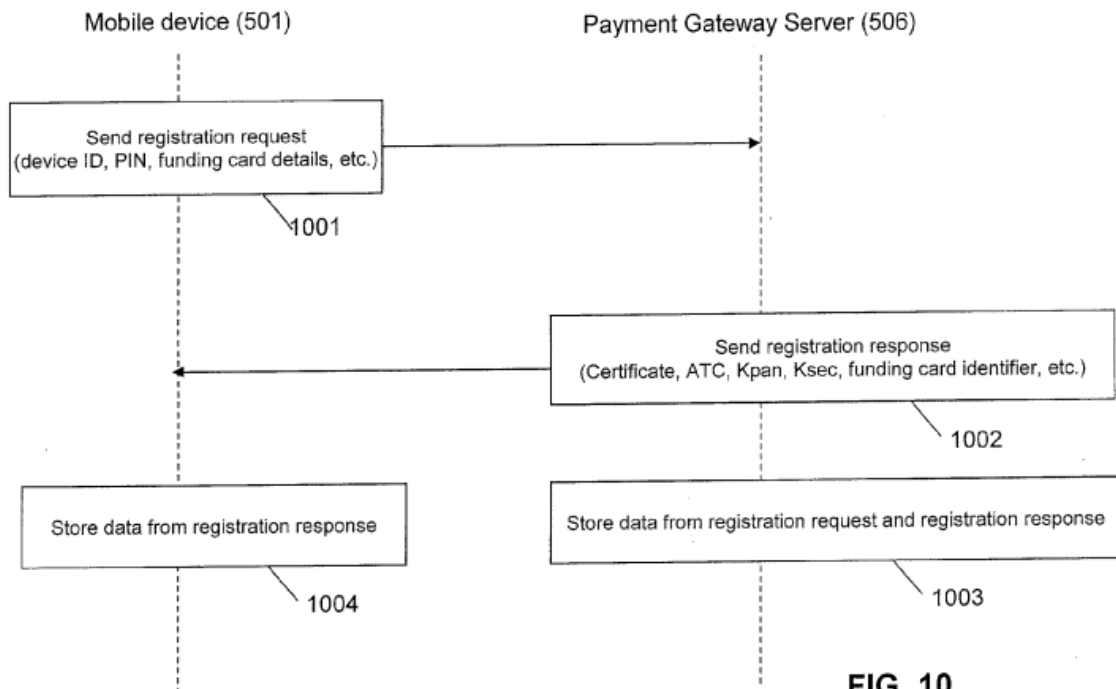


FIG. 10

⁶ Law describes the PAN as a primary account number (i.e., the user’s actual credit card number). EX1032, [0043]; EX1033, [0023].

EX1032, FIG. 10; EX1033, FIG. 10. Law's disclosure of user input of a PAN would constitute at least [10.a]'s "issued payment information." EX1003, ¶135. Law's disclosure of user input of an expiry date and/or static security code would constitute at least [10.a]'s "an issuer provided payment information." *See* EX1037, 71-78; EX1003, ¶135.

Gomez additionally describes inputting issuer provided payment information on a payment device. For example, Gomez teaches that "[a]n EPIC account may be established online to link one or more actual payment card accounts with the EPIC account." EX1007, 20:2-3; *generally id.*, 20:1-28; EX1003, ¶136. Through this process, the user "enter[s] all credit cards information" for cards that are to be linked to the EPIC account. EX1007, 20:12-13. This setup allows an EPIC authentication server later to look up the "actual payment card account number" and "account name" linked to the EPIC account number while processing a transaction. EX1007, 18:20-25, 18:54-59, 20:30-53. A POSITA thus would have understood that the information entered by the user to link issued payment cards to his/her EPIC account would include, for each card, at least the "actual payment card account number" (i.e., "issued payment information") and other credit card details such as expiration date and issuer-provided card security code (i.e., "an issuer provided payment information"). EX1003, ¶136.

iii) [10.b]

Law describes that during the funding card registration process, the mobile device sends card details as well as “a user provided PIN and the mobile device ID to the payment gateway server.” EX1032, [0082]; *see also id.*, [0092], [0099]; EX1033, [0052], [0062], [0069]. Information such as a mobile device ID and a user’s PIN constitute device-specific and user-specific information, respectively. EX1032, [0165]; EX1033, [0132]; EX1003, ¶137. In response to the information sent, “the payment gateway server computes a funding card identifier which identifies the given funding card.” *Id.*; *see also id.*, [0142]-[0143]; EX1033, [0109]-[0110]. Thus, the memory of the device stores the funding card identifier (i.e., device-specific information). *Id.*; EX1003, ¶137. Law discloses that the device stores key values for use in generation of the dynamic data used in the payment transaction. EX1032, [0142] (describing a “Kpan” and “Ksec”), [00146]; EX1033, [0109], [0113].

Additionally, the payment device according to Gomez stores in memory a “seed value,” a “customer key,” and a “reference credential.” EX1003, ¶138. The “seed value,” which the device uses to generate an authentication cryptogram, “is unique for each payment card, and corresponds to the payment card identifying number.” EX1007, 7:27-34. Further, “the seed value may include certain non-random customer specific information, such as a unique customer key.” *Id.*, 7:34-

41. Gomez further describes how the device can store “reference credentials” against which user-entered credentials are compared for authentication. *Id.*, 9:30-39. The reference credentials limit use of the device to a specific user and provide another example of “user-specific information” stored in memory of the electronic payment device. EX1003, ¶138; *see also* EX1007, 10:34-36 (describing memory for storage of information on the device), 10:43-46, 11:7-9.

iv) [10.c]

As described above (*supra* [10.b]), Law describes that the issuer provided payment information is communicated wirelessly by the device which includes payment information that the user inputs to the device (e.g., funding card details that the user links to a funding card identifier (EX1032, [0082]; EX1033, [0052])) and an issuer-provided payment card account number and account name. Law discloses that payment gateway server 506 communicates with the mobile device 501 through a wireless network (EX1032, [0089]) and the “mobile device 501 uses a communication system 613 to interact with a wireless network 612” (*id.*, [0092]) as part of the funding card registration process. *See also* EX1033, [0059]-[0062]. Law also describes communication user provided payment information using NFC, which is wireless. EX1032, Abstract; EX1033 [0002]; EX1003, ¶139.

Gomez describes an “online” account portal that allows a user to enter and submit information about his/her EPIC account using a mobile phone through a

“browser interface” or a “native application” (iPhone, Android, Blackberry, Windows Phone, Windows Mobile, webOS, etc.).” EX1007, 20:2, 20:43-59. The online account portal specifically allows the user to enter and submit information about each of the live/actual payment cards that he/she desires to link (or has linked) to his/her EPIC account. EX1007, 20:1-21:3. In this context, a POSITA would have understood that information the user enters and submits through a native application or browser interface of the payment device for online account setup and configuration—i.e., information constituting and rendering obvious “issuer provided payment information”—would be communicated wirelessly to an EPIC server. EX1003, ¶¶139-140. Further, Gomez describes communicating payment card information via NFC, which is wireless. EX1007, 7:49-54. Gomez also describes communicating an account name field via NFC. *Id.*, 14:3-11.⁷

v) [10.d]

Law describes the process of receiving a static device account number payment information (i.e., a funding card identifier) for storage on the electronic

⁷ The Law-Gomez disclosure of issuer provided payment information communicated wirelessly aligns with Patent Owner’s interpretation of limitation [10.c]. In its infringement contentions, Patent Owner identifies a Wi-Fi or cellular network communication as [10.c]’s wireless communication. *See* EX1037, 81.

device. EX1032, [0082]; EX1033, [0052]. Law explains that “[f]or each funding card, the payment gateway server computes a funding card identifier which identifies the given funding card.” *Id.* The payment gateway server “stores the funding card identifier in association with the funding card details, mobile device ID and PIN, and it sends the funding card identifier to the mobile device for storage.” *Id.* Law further discloses that “the funding card identifier is a value that is different from the PAN, expiry date or static security code of the funding card” and “is a random value so that, if intercepted by an adversary, would not be able to recognize any funding card details.” *Id.* Law explains how the mobile device uses a communication system to interact with a wireless network during the registration process. EX1032, [0092]; EX1033, [0062]. Figure 10 of Law illustrates the process of receiving a funding card identifier (i.e. a static device account number payment information) for storage on the device:

Registration process

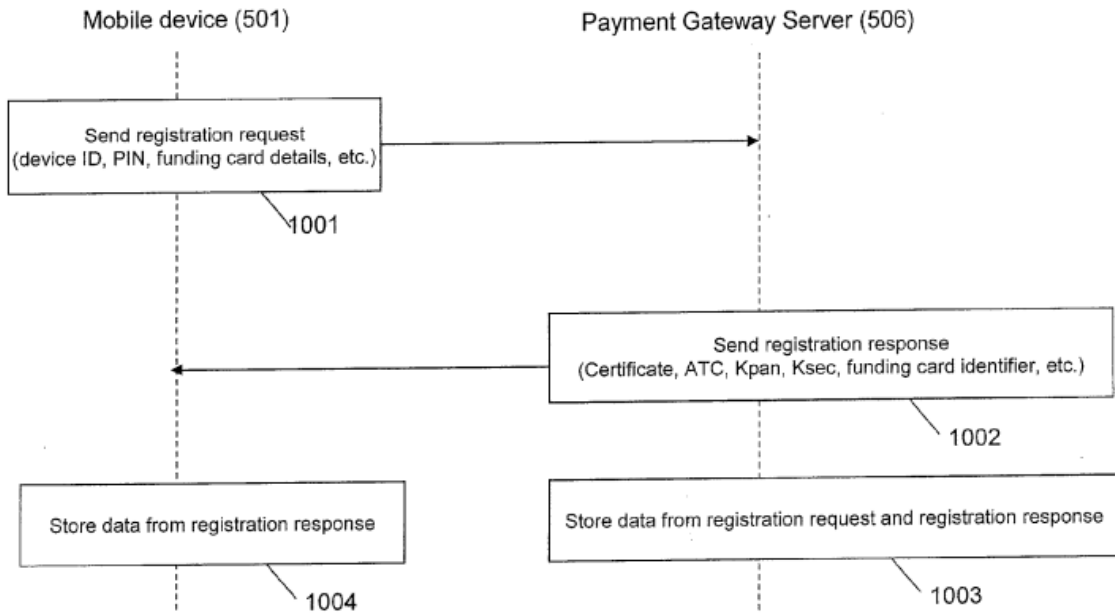


FIG. 10

EX1032, FIG. 10; EX1033, FIG 10. Law also describes communicating user provided payment information using NFC, which is wireless. EX1032, Abstract; EX1033, [0002]; EX1003, ¶¶141-143.

Gomez describes communicating payment card information via NFC, which is wireless. EX1007 7:49-54. Gomez details that the static payment card identifying number—also referred to as an “EPIC” number—“identifies the payment card” and is stored on the device. EX1007, 2:25-27; *see also id.*, 5:13-15, 1:63-64, 13:45-14:2, 22:49-51, 6:10-12, 18:57-59. The EPIC number “identifies the payment card, but does not represent a live account.” *Id.*, 5:13-18; *see also id.*, 13:49-56; EX1003, ¶¶141-143. Thus, Gomez’s EPIC number, or static payment card identifying

number, is a device-specific number identifying the payment card itself. EX1003, ¶¶141-143.⁸

vi) [10.e]

Law and Gomez disclose that at least a portion of the payment information is a limited-use number used in place of issuer provided payment information. EX1003, ¶¶144-145. EX1032, [0082]; EX1033, [0052]. As part of this registration process, the device also receives “a certificate, an Application Transaction Counter (ATC), a key value (called Kpan) for generating a PAN, [and] a secure element key value (called Ksec).” EX1032, [0142]; *see also id.* (“The certificate is a client certificate for the mobile device 501 and, in an example embodiment, it is configured to according to the RSA algorithm and has a 2048 bit length. The ATC is a counter that is initially set to a random value between “0” or “1000” and increments with each transaction. The initialized ATC value is a random value to prevent adversaries from predicting the ATC values. Copies of the ATC are stored

⁸ The Law-Gomez disclosure of wirelessly receiving a static device account number payment information for storage on the electronic device aligns with Patent Owner’s interpretation of limitation [10.d]. In its infringement contentions, Patent Owner identifies the reception of a tokenized account number over a wireless connection as meeting [10.d]. *See* EX1037, 88-95.

and synchronise on both the payment gateway server and the mobile device. In an example embodiment, the ATC is a 10 digit value. In an example embodiment, the Kpan is 128 bits long, and the Ksec is 128 bits long.”); EX1033, [0109]. In creating payment information, Law describes the process with reference to Figure 11.

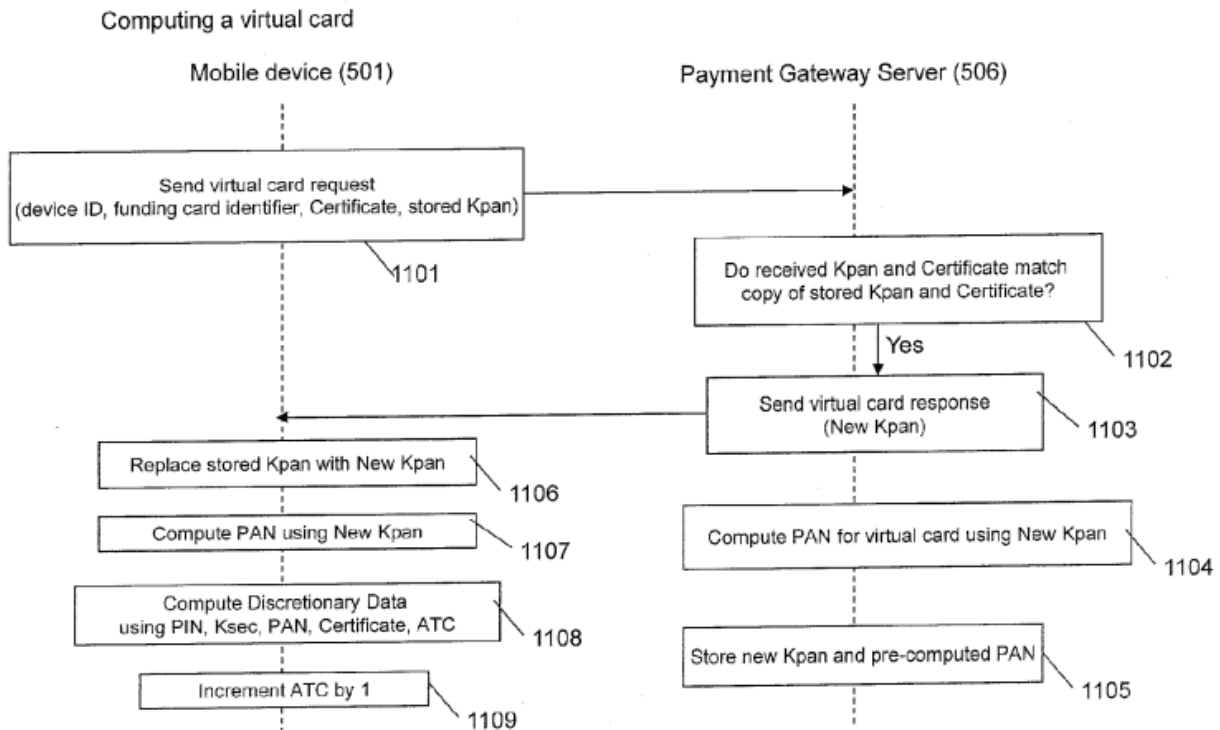


FIG. 11

EX1032, FIG. 11; EX1033, FIG. 11. Law explains that the mobile device 501 sends a virtual card request to the payment gateway server 506 (block 1101) which includes the device ID, the funding card identifier, the certificate and the stored Kpan. EX1032, [0144]; EX1033, [0111]. If the received Kpan and certificate match the Kpan and certificate stored on the payment gateway server, a virtual card response is sent back to the mobile device that includes a new Kpan (block 1103).

EX1032, [0145]; EX1033, [0112]. The newly received Kpan is used to compute a different PAN (i.e. limited-use payment information) from the previous transaction for the virtual card. The mobile device then computes discretionary data using the PIN, the Ksec, the PAN, the Certificate, and the ATC (block 1108). EX1032, [0147]; *see also id.*, [0149]-[0155] (describing details of algorithms creating dynamic payment information); EX1033, [0114], [0116]-[0122]. Law explains that discretionary data is dynamic data used in the transaction. EX1032, [0131]; EX1033, [0100]. “The ATC and the PAN keep changing with each transaction, which causes the discretionary data to be dynamic data.” EX1032, [0147]; EX1033, [0114]. A POSITA would recognize that Law’s funding card identifier (i.e., a static device account number payment information) is a limited-use number for limited use by the device in place of a issuer provided payment information.⁹ EX1003,

⁹ In its infringement contentions, Patent Owner identifies, among other things, a DPAN (or static number) as meeting [10.e]. *See* EX1037, 95. Applying that interpretation, the Law-Gomez combination discloses this limitation. EX1003, ¶¶144-145. Patent Owner also identifies “a issuer provided payment information” as a “PAN or associated expiration date or CVV.” *Id.* Applying that interpretation, the Law-Gomez combination discloses that limited-use numbers for limited-use by

¶¶144-145; *supra* [10.d]. A POSITA would also recognize that values such as Law’s ATC, Kpan, and one-time use discretionary data are limited-use numbers for limited-use by the device, and used in place of issuer provided payment information during the payment transaction process. EX1003, ¶¶144-145.

Additionally, Gomez discloses that the EPIC number (i.e., at least a portion of the payment information) is limited to use by a single device, and thus renders obvious a “limited-use number for limited use by the device.” EX1007, 2:25-27, 7:27-29; EX1003, ¶145. Gomez describes how the EPIC number is used in place of a live/actual card number of an issued payment card linked to the EPIC account (i.e., “a issuer provided payment information”). EX1007, 2:19-20; *see also id.*, 6:29-30, 18:57-59, 18:20-25, 2:25-39; EX1003, ¶145. Gomez teaches an “authentication cryptogram” generated uniquely for each transaction, which is paired with the EPIC number and communicated in place of conventional payment information including the live/actual issuer-provided account number, and the account name and/or security code. EX1007, 1:58-2:13, 5:25-60, 14:36-17:13. This also aligns with Patent Owner’s interpretation of the limitation which advances infringement contentions that identify a cryptogram, among other values, as [10.e]’s “limited-use

the device are used in place of at least a PAN (i.e., an actual credit card number). EX1032, [0082]; EX1033, [0052]; EX1003, ¶¶144-145.

number” (in addition to [10.f]’s “one-time limited use number”). EX1037, 95; *see also id.*, 99. Thus, Gomez’s disclosure of the EPIC number (i.e., “a static device account number payment information”) and an authentication cryptogram (i.e., “a dynamically-generated one-time limited-use number”) and the use of those values together align with Patent Owner’s interpretation of the limitation. *Id.* Applying that interpretation, the combination of Law-Gomez would also provide the recited limited-use number for limited use by the device in place of a issuer provided payment information. EX1003, ¶¶144-145; *supra* IX.A.3.

vii) [10.f]

Law and Gomez disclose a one-time limited-use number is dynamically generated based on at least one of a set of the claimed information. EX1003, ¶¶146-147; *supra* IX.A.3. Law explains that dynamic data can be generated based on the “PIN, the Ksec, the PAN, the Certificate, and the ATC.” EX1032, [0147]; EX1033, [0114]. Law describes the algorithm used to create the dynamic data (EX1032, [0149]-[0154]) and explains that the dynamic data is based on cryptographic number generation. EX1032, [0155]; EX1033, [0122]. Thus, Law discloses a PIN (e.g., user-identifying information/user secrets), a mobile device ID (e.g., device information), a Kpan and Ksec (e.g., device secrets), an ATC (e.g., sequence count), and a funding card identifier (e.g., account information), among other values recited in [10.f]. EX1003, ¶¶146-147.

Further, according to Gomez, the authentication cryptogram is generated from a “seed value” and a “temporal signal.” EX1007, 5:25-47, 7:17-48; EX1003, ¶147. The “seed value” is “unique for each payment card,” and provides combinations of bit values that render obvious “device secrets.” EX1007, 7:27-34; *see also id.*, 12:30-34, 16:31-34, 16:64-17:13. The “seed value” further includes user-identifying information and/or user secrets in the form of “non-random customer specific information, such as a unique customer key.” *Id.*, 7:34-41. Gomez also describes that “a temporal signal value may reflect the date/time of the attempted use [of the card],” and hence the authentication cryptogram can be generated based on time information as recited in [10.f]. *Id.*, 7:19-20. The temporal signal can also include a sequence count. *Id.*, 7:24-26, 8:36-38, 10:66-11:6. Thus, a POSITA would have recognized that the Law-Gomez combination discloses dynamic generation of a one-time limited-use number based on at least one of the set of values recited in [10.f]. EX1003, ¶¶146-147.

viii) [10.g]

The Law-Gomez combination renders obvious use of a static device account number and a dynamically generated one-time limited-use number together in place of issuer provided payment information for making a payment transaction. EX1003, ¶¶148-150; *supra* IX.A.3. As taught in Gomez, the payment device of the Law-Gomez combination renders obvious use of the EPIC number, or static payment card

identifying number (i.e., the static device account number) and authentication cryptogram (i.e., the dynamically generated one-time limited-use number) in making a payment transaction. *Id.* The card communicates the payment card identifying number, the authentication cryptogram, and other account information to the payment processing system in place of a live/actual issuer-provided account number for a payment card linked to the customer's EPIC account. EX1007, 2:25-35, 5:20-24, 2:29-39, 7:49-65, 8:16-24, FIGS. 3-4. Gomez shows in FIG. 2, for example, how the EPIC number or card ID and cryptogram are transmitted (444) by the device (442) in place of an account number and name (404) that would otherwise be used in a traditional transaction like that illustrated in FIG. 1. EX1007, FIGS. 1-2; EX1003, ¶148.

It would have been obvious and a POSITA would have been motivated to modify Law in view of Gomez such that complete payment information is formed with a static number and a dynamically-generated number used together when making a payment, as taught by Gomez. EX1003, ¶149; *supra* IX.A.3. The payment information in the resulting combination would be formed, for instance, by combining a static payment card identifying number stored on the mobile device (and received wirelessly on the device after wireless transmission of user provided payment information as taught in Law) with a cryptogram that hashes the combined data and encodes the output of the hash function in a manner suitable for

transmission in a contactless connection between the mobile device and payment processing authority (as taught in both Law and Gomez). *See supra* [10.c]-[10.d]; EX1007, 9:12-64. A POSITA would have sought to use a dynamically changing temporal signal in calculation of the cryptogram 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 a static device account number and dynamically-generated number from prior transactions to later consummate a fraudulent transaction. *See* EX1007, 1:58-63, 2:21-25, 5:43-47, 9:12-64, 13:63-14:2; EX1003, ¶149.

The application of Gomez's payment credential techniques to the combination as described above further would have been obvious as a predictable use of known techniques that would have achieved predictable results. *KSR*, 550 U.S. at 417; EX1003 ¶150. The function and use of Gomez's dynamic number/cryptograms are highly similar to what is disclosed in Law. EX1003, ¶150. Law and Gomez each describe contactless transactions from which the user's device submits dynamic limited-use information specifically generated to facilitate validation or authorization of a requested transaction. *See, e.g.*, EX1032, [0156]-[0166]; EX1033, [0123]-[0133]; EX1007, 17:23-18:42. The obviousness of the combination is also underscored by Law, 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. EX1032, [0156]-[0166]; EX1033, [0123]-[0133]; EX1003, ¶150. Accordingly, a POSITA would have expected a high likelihood of success implementing the combination with Gomez. EX1003 ¶150; *supra* IX.A.3.

5. Claim 11

The Law-Gomez combination discloses a touch sensor array that allows a user to input information. EX1032, [0092], [0100]; EX1033, [0062], [0070]. A POSITA would have understood that Law’s touch-screen display includes an array of touch sensors to provide location-dependent detection of user inputs contacting the touch screen. EX1003, ¶¶151-153; EX1041, 8-9. Law also discloses a near-field communication (NFC) unit within a mobile device. *See* EX1032 [0088]; EX1033 [0058]. Law further discloses that the payment device includes a display. EX1032 [0092], [0100]; EX1033 [0062], [0070]; EX1003 ¶¶151-152.

The Law-Gomez combination also renders obvious that the user input comprises at least an input sequence or a gesture by biometric input. EX1003, ¶153. For example, Gomez discloses that “[a] fingerprint reader 106 serves as a user credential input device[.]” EX1007, 11:30-31. Further, Gomez describes a “snap” action to “activate the card,” i.e., an unlock operation via snap membranes (i.e., touch sensor array). EX1007, 12:45-48; *see also id.*, 11:39-41 (describing “snap” action as activating the card by briskly snapping the card with a finger).

6. Claim 12

The Law-Gomez combination discloses that the device-specific information comprises at least device identifiers, device secrets/keys, sequence counters, and device account numbers. *See supra* [10.b]-[10.e]; EX1003, ¶¶154-155. For example, as part of funding card identifier provisioning, Law discloses a mobile device ID (“device identifier”). EX1032, [0082], [0158]; EX1033, [0052], [0124]. Law further discloses that the payment gateway server sends a registration response to the mobile device which includes “include a certificate, an Application Transaction Counter (ATC), a key value (called Kpan) for generating a PAN, a secure element key value (called Ksec), and a funding card identifier that identifies each registered funding card(s).” EX1032, [0142]; EX1033, [0109]. Law further discloses that the mobile device increments the ATC by 1 for each transaction. EX1032, [0148]; EX1033, [0115]. Incrementing by 1 generates a sequential parameter. The payment gateway server’s provisioning of data to the mobile device encompasses device-specific information. EX1003, ¶154. As explained above, the ATC (“device usage sequence counter”) is initialized to a random value during the device's registration process and is specific to the device, and then stored on both the mobile device and the payment gateway server and kept synchronized. EX1032, [0142], [0158], [0163]-[0164]; EX1033, [0109], [0125], [0130]-[0131]; EX1003, ¶154. This information is then used along with other device-specific information to

compute dynamic data for the transaction. *Id.* Further, Law discloses that the payment gateway server provisions a Kpan (“device key”) in response to receiving the mobile device ID. EX1032, [0142]; EX1033, [0109]; EX1003, ¶154.

Gomez also discloses, and the combination provides, a sequence counter (e.g., a sequential instance circuit) configured to generate a sequential parameter that, in turn, is combined with a seed value to generate a message and ultimately an authentication cryptogram when the processor initiates a transaction—each of which renders obvious a limited-duration credit card number. EX1003, ¶155. In particular, the temporal signal can indicate a “sequence value (or sequential number) of the attempted use.” EX1007, 7:17-20, 8:36-41. The seed value includes a secret such as a unique customer key or other non-random customer specific information, and is device-specific (i.e., specific to the EPIC card). EX1007, 7:27-28 (“This seed value is unique for each payment card[.]”), 10:64-11:6 (describing the “sequential instance circuit”), 7:17-20, FIG. 7 (348); *see also id.*, 7:26-47; EX1003, ¶155.

7. Claim 13

The Law-Gomez combination discloses that the user-specific information comprises at least password/PIN/passcode, user information, payment information, device account numbers, private/public keys, and user secrets. *See supra* [10.b]-[10.f]; EX1003, ¶156.

B. Ground 1B: Law, Gomez, and Spodak Render Claims 14-17 Obvious

1. Claim 14

As an initial matter, the additional features recited in claim 14 constitute printed matter and are entitled to no patentable weight. *In re DiStefano*, 808 F. 3d 845, 848-851 (Fed. Cir. 2015). Indeed, these features have no structural or functional relationship to the underlying display or other recited elements.

The Law-Gomez combination discloses rendering on the display of the electronic device the payment method types stored in the electronic device, wherein the rendering comprising rendering with at least images and alphanumeric characters. EX1003, ¶158. For example, Law discloses that multiple funding cards can be added to a payment application on a mobile device. EX1032, [0083]; EX1033, [0053]. Law further discloses that when a user wishes to make a payment, “the user selects the funding card” on the touch-screen display. EX1032, [0084]; *see also id.*, [0100]; EX1033, [0054], [0070]. “The mobile device 501 then displays the funding cards that have been pre-registered by the user (block 706). A user input is provided to select one of the funding cards (block 707).” EX1032, [0101]; EX1033, [0071]. Law discloses that an identifier for the payment network associated with the funding card is also stored in the payment application. *Id.*

Additionally, Gomez describes how a user can “scroll through available card accounts sequentially displayed on the card, and select[ing] one of the accounts.”

EX1007, 20:37-42; *see also id.*, 20:30- 37 (“manually select the actual credit card”). By displaying available card accounts linked to the EPIC account, along with information about the EPIC account itself, the payment device renders on the display the payment method types stored in the electronic device. EX1003, ¶159. The displayed accounts can represent cards for different payment methods (e.g., credit or debit cards) and cards from different payment networks (e.g., VISA, MasterCard, Discover, AMEX, etc.). EX1007, 2:19-39; *see also id.*, 11:19-27, 12:64-67; EX1003, ¶159. To the extent that Law and Gomez do not expressly disclose all of the recited features of claim 14, it would have been obvious in view of Spodak for the displayed card accounts in the combination to be rendered with images, alphanumeric characters, and iconography including at least one of the set recited in claim 14. EX1003, ¶159.

Spodak is directed to a “universal card which can be used at any type of terminal equipped with a magnetic stripe reader or a short range wireless communication capability.” EX1009, [0002]. The universal card can include a display which can show, among other things, an account number, an expiration date, a card issuer logo, or any combination of these types of information. *Id.*, [0068] (“The front of the universal card 800 can also have a display 803 which could be used at various times to display an account number, an expiration date, a card issuer logo, any other information, or any combination of these types of information.”),

FIG. 8A. Given that the Law-Gomez combination describes displaying payment cards on the screen of the device, it would have been obvious to display additional information about the virtual cards including the features recited in claim 14, as taught in Spodak, to provide an intuitive and convenient user interface by which the user could more readily select among the different payment cards based on visual depictions of those cards. EX1009, [0068]; EX1003, ¶160.

2. Claim 15

The Law-Gomez-Spodak combination renders obvious accepting a user selection of a payment method type for use in a transaction responsive to a user selection from a list of payment method images rendered on the display with use of a touch-screen interface. EX1003, ¶161. As discussed above, Law discloses use of a touch-screen interface (*supra* [10.a], [11], [14]) to select a payment card in a payment application for use in a payment transaction. *See supra* [10.a], [11], [14]. Spodak discloses that payment methods can be rendered with logos or images. *See supra* [14].

3. Claim 16

The Law-Gomez-Spodak combination renders obvious that a user selection can be a default payment method for use in transactions. EX1003, ¶162. Based on Gomez, a POSITA would have found it obvious for a user to select a default payment card to use in transactions with the electronic payment device: “After entering all

credit cards information, the customer may establish the default credit usage selection process.” EX1007, 20:12-13; *see also id.*, 20:63- 21:3; EX1003, ¶162.

4. Claim 17

The Law-Gomez-Spodak combination renders obvious that the issuer provided payment information is selected from at least one of the set recited in claim 17. EX1003, ¶163. For example, Law discloses that the issuer provided payment information sent to a payment gateway server during registration is the user’s actual credit card number. EX1032, [0082]; EX1033, [0052]; *supra* [10.a]-[10.e].

C. Ground 2A: Gill, Smith, Kay, and Gomez Render Claims 18-24 Obvious

This ground challenging claims 18-24 was previously instituted by the Board in IPR2023-00211. *See* IPR2023-00211, Paper 13.

1. Gill

Gill describes systems and methods for performing contactless transactions at an ATM. Upon tapping an 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.” EX1034, 5:13-18. Figure 7 of Gill illustrates example interactions:

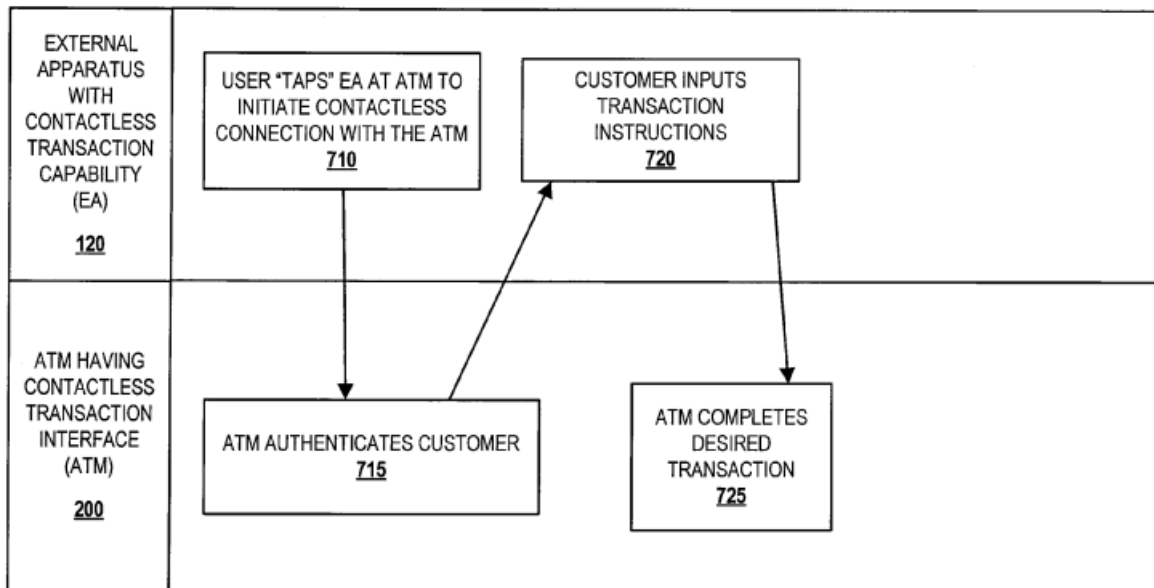


FIG. 7

Id., FIG. 7.

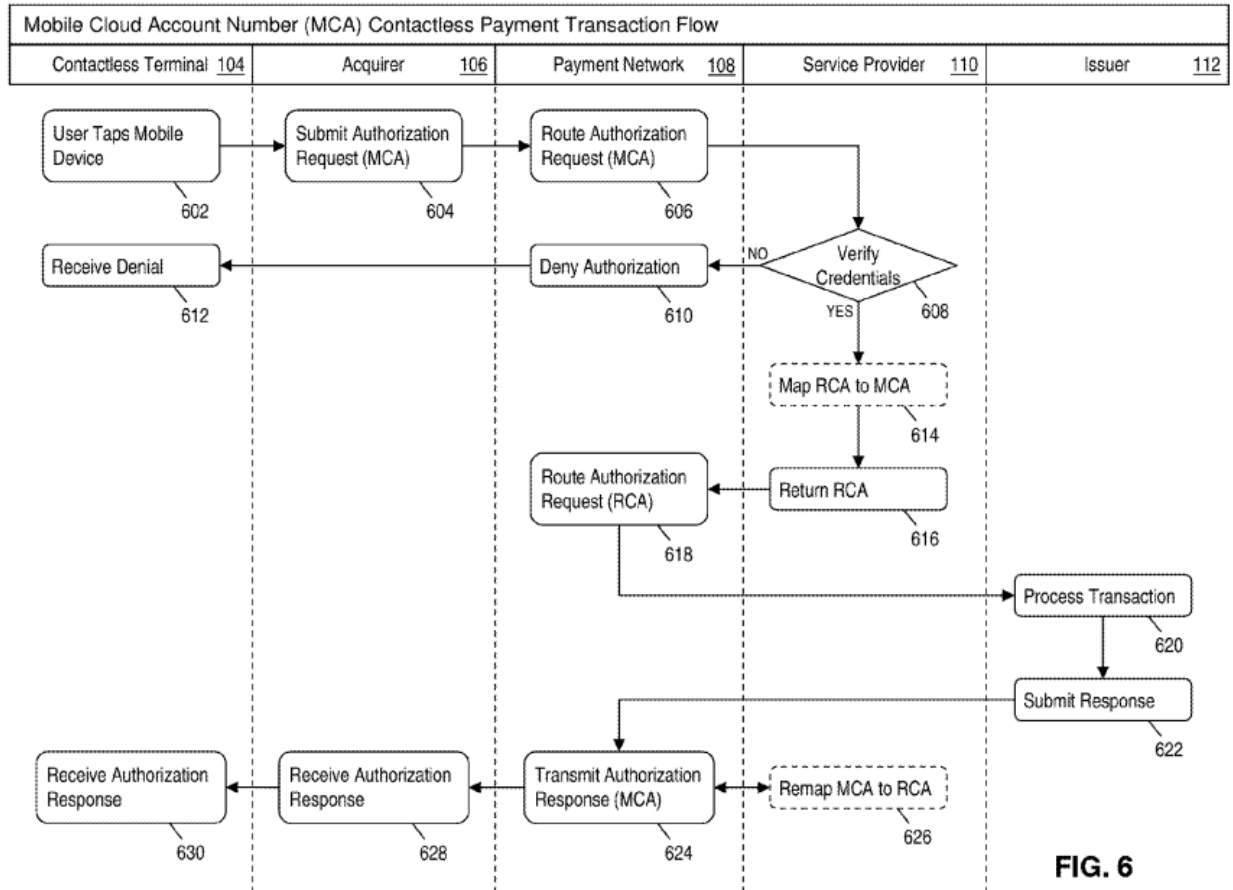
In some embodiments, “the customer may first authenticate himself prior to the contactless connection being established” by “input[ing] authentication information and such transfer such data to the ATM 200 upon establishing the contactless connection.” *Id.*, 14:13-20. The customer can further input 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.

2. Smith

Smith describes techniques for conducting contactless payment transactions with a mobile device. EX1035, [0002]. Smith discloses 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. *Id.*, [0032]-[0037]; *see also id.*, [0029]. “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.*

In Figure 6, Smith illustrates 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 and a “payment cryptogram” such as “an authorization request cryptogram or dynamic card validation code.” *Id.*, [0067]-[0068].



Id., FIG. 6. 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.*, [0070]. “If the credentials are successfully verified, then[] ... the service provider 110 may identify the RCA corresponding to the MCA” and returns the corresponding RCA to the payment network for further processing. *Id.*, [0071]. “[T]he payment network 108 may route the authorization request with the RCA in place of the MCA to the issuer

112,” and “the issuer 112 may approve and process the financial transaction.” *Id.*, [0072].

3. Kay

Kay generally describes techniques to “allow greater access to a banking platform via a mobile device” and a financial transaction terminal. EX1036, [0004], [0017]. “[T]he 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. *See id.*, [0038]-[0043].

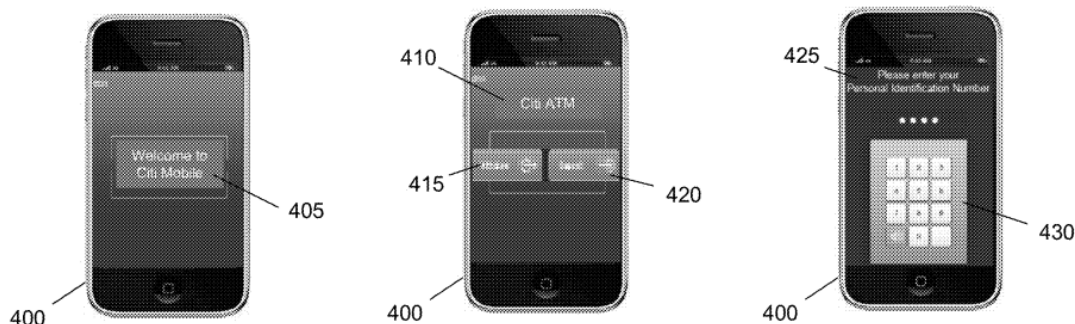


FIG. 4A

FIG. 4B

FIG. 4C

Id., FIGS. 4A-4C.

4. Gill-Smith-Kay-Gomez Combination

Gill describes techniques for using a mobile device in a contactless transaction at an ATM. *Supra* IX.C.1. 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. EX1034, 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.” *Id.*, 5:13-18, 13:41-46, FIG. 6. The ATM and a backend payment infrastructure then processes the information conveyed from the mobile device to complete the transaction. *Id.*; EX1003, ¶164. Notwithstanding these disclosures, Gill is not explicit in describing 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. EX1003, ¶164. Considering this, 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 as taught in Smith. *Id.* The payment credentials in the resulting Gill-Smith system would further include information such as “a mobile personal identification number (PIN)” as taught in Smith. EX1035, [0068]. Applying Smith’s proposed use of payment credentials—including an MCA and payment cryptogram—in a system of the resulting combination would have been obvious to a POSITA by the Critical Date of the ’520

patent. EX1003, ¶164. 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. EX1034, 10:34-53, FIG. 5; EX1035, [0041], [0075], FIG. 2. Gill 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. EX1034, 2:1-2, 4:62-63; EX1035 [0029], [0031]. A POSITA thus would have understood Smith’s payment credentials and expected them to be operable in ATM transactions like those discussed in Gill. EX1003, ¶164.

Moreover, a POSITA would have sought to use payment credentials like Smith’s in the combination with Gill (and Kay and Gomez, as described below) to realize predictable security improvements. EX1003, ¶165. 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* EX1035, [0034].

Conducting contactless transactions with the MCA rather than the RCA would also improve security by preventing unauthorized actors from exploiting the MCA

in fraudulent transactions. EX1003, ¶166. 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. EX1035, [0070], [0040]; EX1003, ¶166.

Additionally, cryptograms in payment devices were common long before the '520 patent. EX1003, ¶167. 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. *Id.*, ¶167. For example, Smith teaches that the cryptogram is generated based on device secrets securely 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. EX1035, [0007], [0067]. 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. EX1003, ¶167. 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* EX1034, 1:34-36, 4:35-55; EX1003, ¶167.

Integrating Smith's suggested use of payment credentials, including at least 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 achieved merely predictable results (e.g., more secure transactions). *KSR*, 550 U.S. at 417; EX1003, ¶168. 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. EX1003, ¶168; EX1035, [0029].

Next, it would have been obvious to a POSITA to apply in the combination Kay's suggestion for a graphical user interface (GUI) on a mobile device, which would allow a user to select a particular type of transaction from a list of available types. EX1003, ¶169. Gill discloses that a customer can "input[] instructions to [an] ATM 200 to execute [a] desired transaction." EX1034, 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. 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), 17:56-62. 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. EX1003, ¶170. Kay demonstrates, however, that such GUIs adapted to receive user instructions for ATM transactions on a mobile device were known well before the ’520 patent. *Id.* Kay, like Gill, discloses a method of conducting ATM transactions using a mobile device. EX1036, [0038]-[0052], FIGS. 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]. The application includes a user interface that allows a user to “choose a category of instructions or transactions.” *Id.* As shown in FIG. 4B, 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 FIG. 4D:

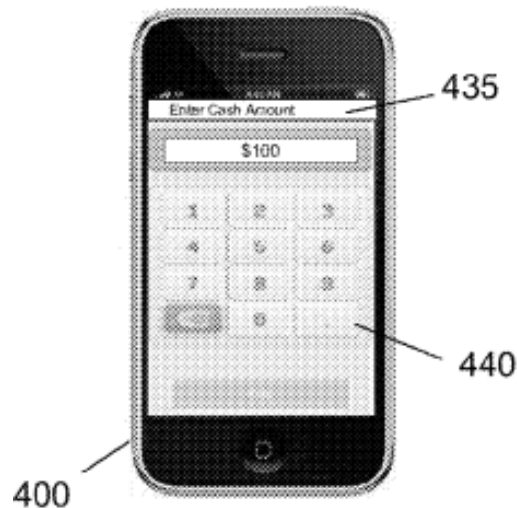


FIG. 4D

EX1036, FIG. 4D; *see also id.*, [0043].

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. EX1003, ¶171. 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. *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. EX1034, 10:42-46, 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. *Id.*; *see also* EX1034, 10:42-46, 13:9-17, 14:31-36, FIGS. 5, 7. 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. 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 in substantially the same way, and would have achieved merely predictable results (e.g., more secure transactions). *KSR*, 550 U.S. at 417; EX1003, ¶171. Kay's GUI is specifically designed for ATM transactions, and would naturally support ATM transactions in the combination as well. EX1003, ¶171. Hence, a POSITA would have expected a high likelihood of success combining the teachings of Kay with those of Gill and Smith in the manner described above. *Id.*

Although Smith discloses that the payment cryptogram can be a dynamic number, can take the form of an authorization request cryptogram or a dynamic card validation code, and can be generated based on at least a portion of the mobile cloud account data securely stored on the mobile device, Smith does not expressly disclose many details as to how the payment cryptogram would be made to change across transactions or how the cryptogram would be calculated. EX1003, ¶172. Nonetheless, the use of dynamic cryptograms in electronic transaction systems had been known for many years before the Critical Date. EX1003, ¶172. 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. *Id.*

Gomez provides one such solution that involves computing a cryptogram based on a "temporal signal" that changes from transaction to transaction. *See, e.g.*, EX1007, 1:64-2:1, 7:17-27. In Gomez, the temporal signal is combined with other data stored on the device (e.g., a seed value and static payment card identifying number) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. *Id.*, 8:11-51. The cryptogram is then formed by encoding the output of the hash function. *Id.*, 2:14-17, 8:52-9:11; EX1003, ¶173.

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.” *Id.*, 5:43-47; *see also id.*, 1:58-63, 2:21-25, 13:63-14:2; EX1003, ¶174.

It would have been obvious and a POSITA would have been motivated to further modify the Gill-Smith-Kay combination in view of Gomez such that the payment cryptogram would be generated using a temporal signal and cryptographic methods like those described in Gomez. EX1003, ¶175. 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* EX1007, 1:58- 63, 2:21-25, 5:43-47, 13:63-14:2; EX1003, ¶175.

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 that would have achieved no more than predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶176. Indeed, the function and use of Gomez's cryptograms are highly similar to Smith's. EX1003, ¶176. 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 (static payment card identifying number) in Gomez) paired with a cryptogram that is specifically generated to facilitate validation or authorization of a requested transaction. *See, e.g.*, EX1035, [0070]-[0071]; EX1007, 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. EX1035, [0070]. Accordingly, a POSITA would have expected a high likelihood of success implementing the combination with Gomez. EX1003, ¶176.

In the combination described above, the teachings of Gill in view of Smith, Kay, and Gomez would have rendered obvious claims 18-24, and the combination would have provided each element of these claims for the reasons described in detail below. EX1003, ¶177.

5. Claim 18

i) [18.pre]

To the extent the preamble is a limitation, the Gill-Smith-Kay-Gomez combination renders obvious the recited method. EX1003, ¶¶178-179. For example, Gill discloses “methods ... for receiving a contactless transmission from an external apparatus to an ATM.” EX1034, 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.*, 3:56-63, 5:13-18, 9:63-10:4, FIG. 5. Gill describes a range of possible transactions that can be performed with a mobile device and ATM. *Id.*, 14:32-36.

Gill 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. EX1034, 5:11-20, 7:29-46, 13:23-31, 13:47-51, 14:9-30, FIGS. 6 (614), 7 (715).

ii) [18.a]

Gill-Smith-Kay-Gomez renders obvious providing, by the mobile (electronic) device, account information, identification, and authorization for the ATM transaction.¹⁰ EX1003, ¶¶180-184.

As to “account information,” Gill’s mobile device provides such information to the ATM terminal via a contactless/wireless connection when a user “taps” the mobile device at the ATM. EX1034, 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.”), 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. Gill also discloses that the mobile device transmits account information as “payment vehicle data.” *Id.*, 12:29-32, 11:7-16; EX1003, ¶181.

In the combination, and based on Smith, the mobile device provides account information via a contactless/wireless connection including a mobile cloud account

¹⁰ Although Petitioner addresses all three recited items (i.e., account information, identification, and authorization), only one is required to satisfy this claim element.

number (MCA) and a payment cryptogram. EX1035, [0034], [0067], FIG. 6; EX1003, ¶182.

As to “identification” and “authorization,” the payment vehicle data provided by the mobile device includes a “security code associated with the payment vehicle.” EX1034, 11:9-14. A POSITA would have understood that the security code in a payment vehicle is used to verify the identity of a device or user and to authorize a transaction. EX1003, ¶183. Further, in the combination, the information transmitted from the mobile device identifies the requested financial account for a transaction. *Id.* For example, according to Smith, the mobile device conveys the MCA (and a corresponding cryptogram) to identify the account associated with a requested transaction. 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.” EX1035, [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. EX1035, [0070]-[0072], FIG. 6; *infra*, [18.g].

Gill-Smith-Kay-Gomez also renders obvious identification and authorization in a transaction in which a user authenticates himself/herself by presenting valid

credential(s). EX1034, 5:15-18, 7:29-46, FIGS. 6-7; EX1035, [0068], [0069]-[0071]; EX1003, ¶184.

iii) [18.b]

Gill-Smith-Kay-Gomez renders obvious a mobile device (electronic device) comprising a user interface that includes displays, touch sensors, and buttons. EX1003, ¶¶185-188.

For example, Gill teaches that “the mobile device 500 may have a user interface that includes user output devices 536 and/or user input devices 540.” EX1034, 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).” EX1034, 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. EX1003, ¶186. A keypad and keyboard would each include mechanical buttons, while a graphical user interface 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-Gomez combination). EX1036, FIGS. 4B, 4D. 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 as touch sensors and buttons. EX1003, ¶186.

Gill-Smith-Kay-Gomez 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* EX1001, FIGS. 2A-2B, 4A-4B. Even if [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-Gomez combination to expand options available for displaying information to a user. EX1003, ¶187. 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 (e.g., a first set of information could be displayed on a primary display located at a first part of the device and additional information could be displayed on a secondary display at a second part of the device). *Id.*

To the extent the term “displays” encompasses virtual display elements on a physical display, the combination also provides such features. *Id.*, ¶188. 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, displays of elements 430 for inputting a PIN, and displays of elements 440 for inputting a transaction amount. EX1036, FIGS. 4A-4C.

iv) [18.c]

Gill-Smith-Kay-Gomez 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. EX1003, ¶¶189-191. 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” for a transaction. EX1034, 13:9-17; *see also id.*, 4:1-6. The mobile device is operable to convey data corresponding to the selected payment vehicle (and thus the selected account) to an ATM. *Id.*, 5:13-16, 6:42-49, 13:44-46.

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). EX1035, [0067]-[0068], [0075], FIGS. 6-7. EX1003, ¶190.

A POSITA further would have understood and/or it would have been obvious for the mobile device to record the user’s selection. EX1003, ¶191. 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.*; EX1035, [0067]-[0068], [0075]; EX1034, 5:13-16, 13:9-17.

v) [18.d]

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.” EX1034, 18:19-22; EX1003, ¶¶192-194. For example, 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; *see also id.*, 19:12-19. Figure 7 shows the user inputting transaction instructions at the mobile device (external apparatus 120):

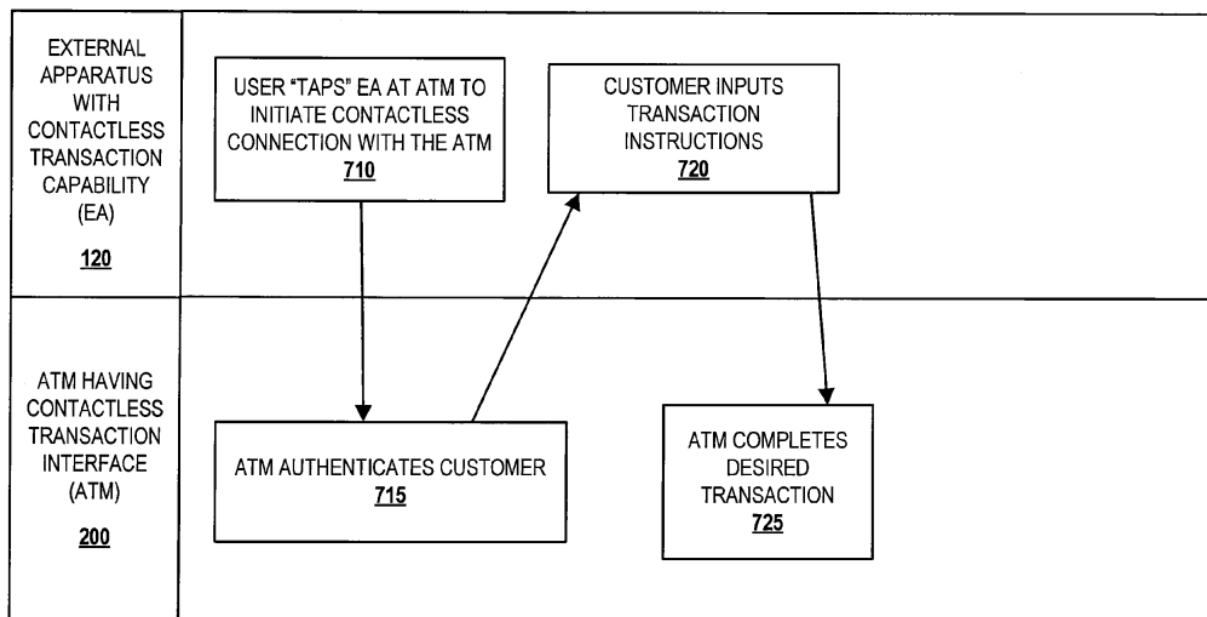
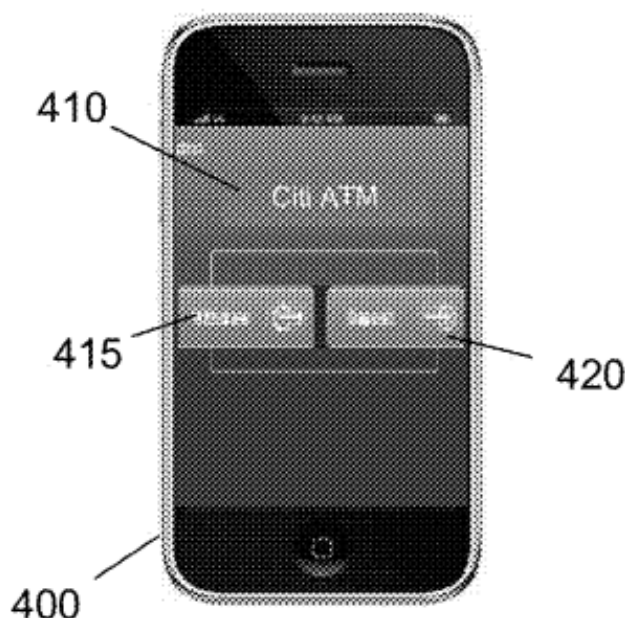


FIG. 7

EX1034, FIG. 7 (720); *see also id.*, 12:33-34, 13:9-17 (describing mobile device GUI); EX1003, ¶192.

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.



EX1036, FIG. 4B (illustrating withdraw 415 and deposit 420); *see also id.*, [0040]; *generally id.*, [0038]-[0044], FIGS. 3-4; EX1003, ¶193.

Kay's teachings in this regard would have been obvious to apply to the combination with Gill, Smith, and Gomez for the reasons described above. EX1003, ¶194. 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.” EX1034, 14:31-37. 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. EX1003, ¶194. 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.*; EX1034, FIG. 7; EX1036, [0040]-[0041]; EX1003, ¶194.

vi) [18.e]

Gill-Smith-Kay-Gomez renders obvious receiving user input information from the user interface that includes at least one from the set recited in [18.e]. EX1003, ¶¶195-199.

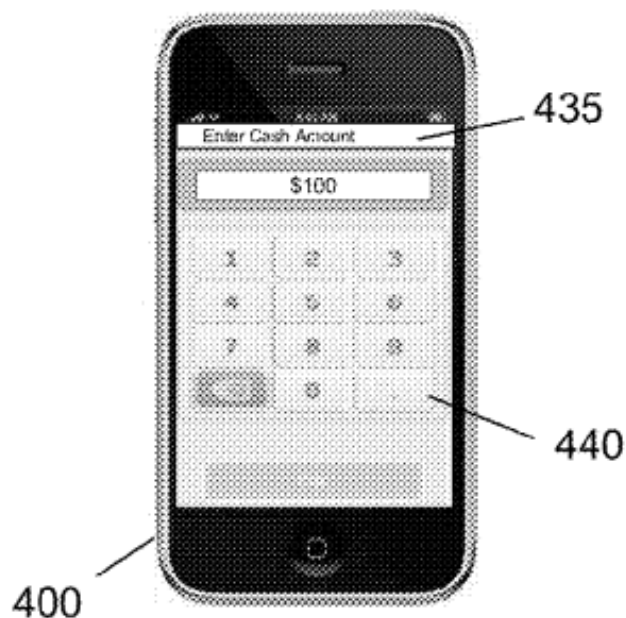
For example, Gill describes how the user can input identification and/or authorizing information to authenticate himself/herself for a transaction. EX1034, 14:15-21, 13:23-31; *see also id.*, EX1036, [0041] and FIG. 4C (user-entered pin).

Gill further describes user inputs from the user interface regarding account information. EX1034, 13:14-15 (“The GUI for the mobile wallet application 521 may allow the user 110 to enter input to select a payment vehicle”); *supra*, [18.a]; EX1003, ¶197.

Gill also describes user inputs received at the mobile device directed to operations of the device. EX1034, FIG. 7 (715-720) (depicting the user inputting

instructions to the external apparatus 120 to execute the desired transaction); *see also id.*, 14:31-37; EX1003, ¶198.

In the combination, Kay also discloses the mobile device receiving user input information from a user interface indicating an “amount of currency” for a transaction. EX1036, [0043]; EX1003, ¶199.



EX1036, FIG. 4D (illustrating amount of currency entered on device); *see also* EX1034, 12:33-34, 13:9-17 (describing mobile device GUI).

vii) [18.f]

Gill-Smith-Kay-Gomez renders obvious that the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC. Gill discloses that interactions between

the mobile device and the ATM occur wirelessly via near-field communications (NFC). EX1034, 3:56-67, 14:15-21, 13:41-46; EX1003, ¶¶200-201. 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 [18.a] and [18.c]-[18.e]. EX1034, 13:51-14:37; *see also id.*, 13:32-51, FIG. 6.

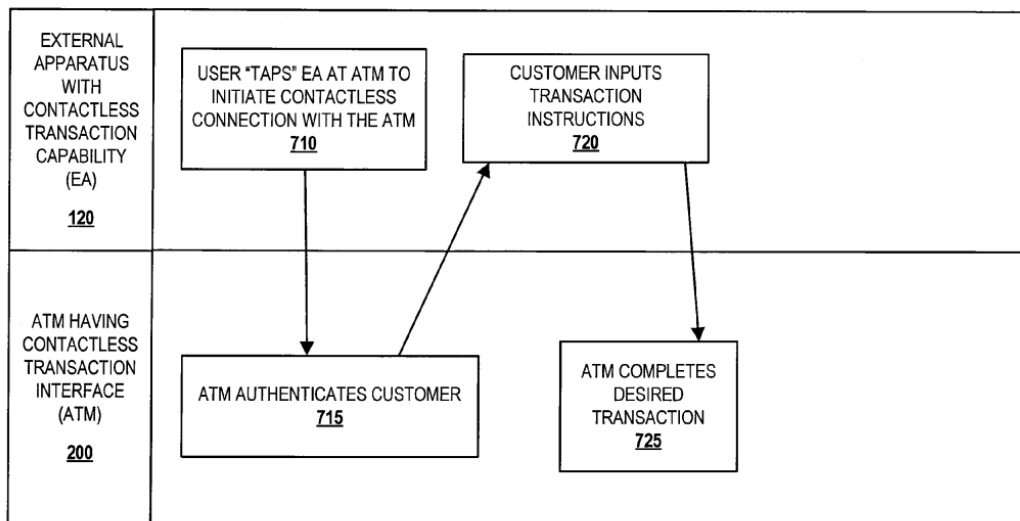


FIG. 7

EX1034, FIG. 7 (communication between external apparatus 120 and ATM 200).

Smith also discloses, and the combination provides, for the exchange of payment credentials (including an MCA and payment cryptogram) wirelessly between the mobile device and a terminal. *Supra*, [18.a]. 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. EX1035, [0067], [0034]; *see also id.*, [0045], [0058]-[0059] (describing user's selection of a payment account for a transaction), FIG. 6; *supra*, [18.a]; EX1003, ¶201.

viii) [18.g]

Gill-Smith-Kay-Gomez renders obvious configuring the ATM to perform the user-selected account operation using identification and authorization information received wirelessly from the mobile device. EX1003, ¶202; *supra*, [18.a], [18.c]-[18.f]. For example, Gill teaches that the ATM authenticates the customer based on credentials (e.g., a PIN) received wirelessly from the mobile device. EX1034, 14:17-20, 13:47-48 ("ATM 200 authenticates the user"), FIG. 6 (614), FIG. 7 (715). Once the ATM receives further transaction instructions including the user-selected account operation and identification and authorizing information, Gill discloses that the ATM is configured to "execute the desired transaction." *Id.*, 14:31-37, FIG. 7 (720); *see also id.*, 5:11-20, 7:29-46 ("ATM 200 will initiate, perform, complete, and/or facilitate a transaction").

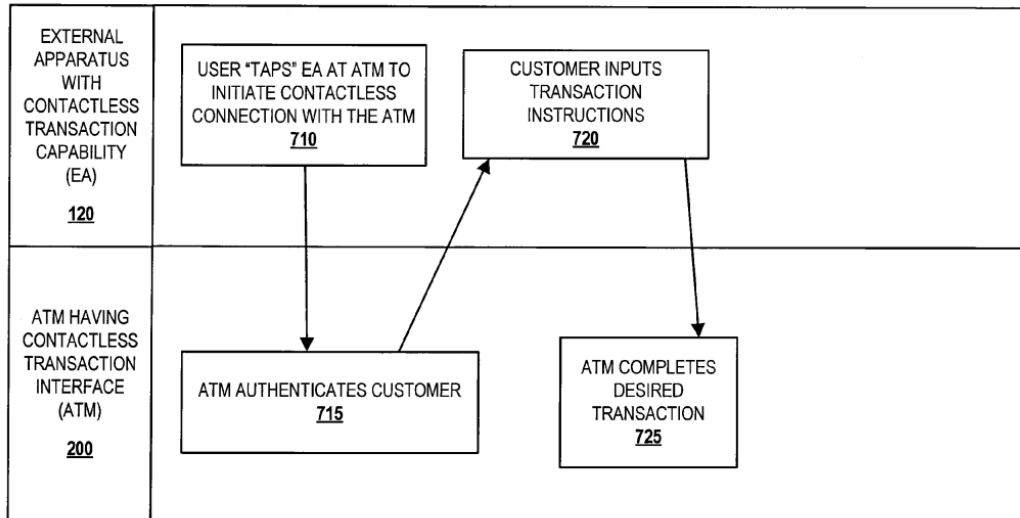


FIG. 7

EX1034, FIG. 7 (steps 720 and 725).

ix) [18.h]

Gill-Smith-Kay-Gomez renders obvious exchanging wirelessly with an ATM transaction data including account, identification, and authorizing information, as discussed above. *Supra* [18.a], [18.b]-[18.f]; EX1003, ¶¶203-207.

Based on Smith, it would have been obvious for the wireless exchange to further involve transmission of a mobile card account number (MCA) and a payment cryptogram from a mobile device to a terminal. EX1035, [0067], FIG. 6; *see also id.*, [0051] (“MCAs for use in conducting contactless payment transactions”); EX1003, ¶204.

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. EX1035, [0040], [0034]. 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”); EX1003, ¶205.

Further, according to Smith, the payment cryptogram 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 number portion of the payment credentials. EX1035, [0103], [0067], [0096]-[0097], [0063]; EX1003, ¶206. Smith specifically explains that the payment cryptogram is “generated” for each transaction—in contrast to the MCA which is read from memory of the device. EX1035, [0067]. 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 on a frequent basis (e.g., with each transaction) 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. EX1003, ¶206. Instead, Smith explains that the service provider can identify and authorize a transaction request by verifying the cryptogram using known techniques. EX1035, [0070], [0067]. 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 in the combination overview. *Supra* § IX.C.4; EX1003, ¶206.

Moreover, Gomez discloses that the payment cryptogram is dynamically generated based on a temporal signal and constitutes “dynamically generated limited-use number portions” that change from transaction to transaction. EX1007, 1:64-2:1, 7:17-27, 2:21-25. Gomez further discloses that the temporal signal value is combined with other data stored on the device (e.g., a seed value and static payment card identifying number) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. *Id.*, 8:11-51. The cryptogram is then formed by encoding the output of the hash function. *Id.*, 2:14-17, 8:52-9:11; EX1003, ¶207. 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.” EX1007, 5:43-47; *see also id.*, 2:21-25, 1:58-63, 13:63-14:2; EX1003, ¶207. It would have been obvious to apply Gomez’s suggested use of statically and dynamically generated number portions including a static payment card identifying number and authentication cryptogram in the resulting combination for the reasons discussed above in the combination overview. *Supra* IX.C.4; EX1003, ¶207. The cryptogram in the resulting combination with Gomez could be formed 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* EX1007, 1:58- 63, 2:21-25, 5:43-47, 13:63-14:2; EX1003, ¶207. 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 that would have achieved no more than predictable results.

KSR, 550 U.S. at 417; EX1003, ¶¶203-207. Accordingly, a POSITA would have expected a high likelihood of success implementing the combination with Gomez. EX1003, ¶¶203-207.

x) [18.i]

Smith discloses, and the combination renders obvious, that the MCA and payment cryptogram, i.e., said static and dynamic information, is combined into “payment credentials” to form an authorization request for performance of a user-selected operation. EX1035, [0067], FIG. 6 (602); *see also id.*, [0059].¹¹ In the combination as described above (*supra* IX.C.4), the MCA and cryptogram are combined into payment credentials to perform a user-selected ATM operation such as a deposit, withdrawal, or funds transfer operation like those described in Gill, Smith, Kay, and Gomez. EX1034, 14:34-37; EX1035, [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”); *supra*, [18.g]; EX1003, ¶208.

¹¹ Smith alternately refers to the MCA and payment cryptogram being combined to form “transaction data.” EX1035, [0011] (“the transaction data includes at least an MCA and a payment cryptogram”), [0096] (“the transaction data may include at least an MCA and a payment cryptogram”).

6. Claim 19

Gill describes how identification and authorization information is generated from “account information” and/or “payment vehicle data” that includes an account name (e.g., user identification or username), an account number (e.g., payment numbers, ATM accounts, bank account), and an expiration date (e.g., transaction information). EX1034, 5:11-20, 12:29-32, 11:7-16. Gill further describes identification and authorization information is generated from credentials (e.g., secrets, passwords, or passcodes) such as a user’s PIN. *Id.*, 5:18-20, 7:34-40, 14:13-20; EX1003, ¶¶209-211.

Smith further discloses, and the combination provides, that the mobile device generates transaction data or payment credentials for identification and authorization from an MCA and a payment cryptogram. *Supra* [18.h]-[18.i]; EX1035, [0067]. The MCA points to a real card account and constitutes a device account number, payment number, and/or device identifier. *Id.* The cryptogram is generated based on secret mobile cloud account data stored on the mobile device, including secrets and a key. EX1035, [0067], [0086]; EX1003, ¶210.

Gomez further discloses, and the combination provides, that the mobile device generates transaction data or payment credentials for identification and authorization from a static payment card identifying number and authentication cryptogram. Gomez discloses a temporal signal value is combined with other data stored on the

device (e.g., a seed value and static payment card identifying number) to form a message that is cryptographically hashed to produce a fixed-length, seemingly random number. EX1007, 8:11-51; EX1003, ¶211.

7. Claim 20

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.” EX1034, 7:32-38; *see also id.*, 5:18-20 (“require at least the input of the proper PIN associated with the account”), 13:47-51, 14:9-30. Gill further discloses “[t]he user input devices 540” of the mobile device can include a “touchscreen” and “keypad.” *Id.*, 12:33-44. A POSITA would have understood and/or it would have been obvious that the user’s entry of a PIN, passcode, or like credentials 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.” EX1003, ¶212; *see also* EX1036, FIG. 4C and [0042].

8. Claim 21

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, a password, a

biometric identification, and user known secrets. EX1034, 7:32-38, 14:9-13; EX1003, ¶213.

9. Claim 22

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. EX1035, [0067]. The mobile cloud account data comprises device-internal secrets such as the ICC public key certificate and ICC public key certificate. *Id.*, [0086]. In the combination, Gomez further teaches that the cryptogram can be generated based on a temporal signal including a date and a time of day, or a sequence count or count of past transactions. EX1007, 7:17-27, 8:36-41, 10:58-11:6. As discussed in the overview of the Gill-Smith-Kay-Gomez combination (§ IX.C.4), it would have been obvious to combine the temporal signal with additional information such as the mobile cloud account data or other information like Gomez's seed value, which includes device internal secrets, device unique identifiers, and/or a user secret. EX1007, 7:27-39; EX1003, ¶214.

10. Claim 23

The mobile device of the Gill-Smith-Kay-Gomez combination generates and transmits payment information that includes a mobile card account number (MCA)

and a payment cryptogram as taught in Smith. *Supra* [18.h]-[18.i]. Further, and as described above, and the combination renders obvious, the Gill-Smith-Kay-Gomez combination discloses 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* IX.C.4; EX1003, ¶¶215-217.

In this context, the Gill-Smith-Kay-Gomez combination provides the additional features recited in [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. EX1035, [0095], [0091]. Both portions of the MCA are static, 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], [0040]; EX1003, ¶216.

Moreover, Gomez teaches and the combination renders obvious that the cryptogram can be generated by combining a “date” and a “time” (i.e., a plurality of dynamically-generated limited use portions) to form a temporal signal used in calculating the cryptogram. EX1007, 7:17-24, 7:41-48. 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 (i.e., a plurality of dynamically generated limited-use portions) are combined to form the complete cryptogram. *Id.*, 15:43-51, 15:61-65. 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. EX1007, 14:37-63, 15:17-60; EX1003, ¶217. 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”); EX1003, ¶217.

11. Claim 24¹²

As discussed with respect to [18.e], Kay discloses and the combination renders obvious a mobile device that receives user input information from a user

¹² 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.

interface indicating an “amount of currency” for a transaction. EX1036, [0043]; EX1003, ¶218.

X. DISCRETIONARY DENIAL IS NOT APPROPRIATE

In view of the Patent Office’s interim process regarding discretionary denial, Petitioner will substantively address this issue during discretionary denial briefing.

XI. CONCLUSION

Petitioner requests institution of IPR for claims 10-24 of the ’520 patent based on the grounds specified in this petition.

Respectfully submitted,

Dated: September 4, 2025

By: /Naveen Modi/
Naveen Modi (Reg. No. 46,224)
Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), the undersigned certifies that the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 10,339,520 contains, as measured by the word-processing system used to prepare this paper, 13,996 words. This word count does not include the items excluded by 37 C.F.R. § 42.24 as not counting towards the word limit.

Respectfully submitted,

Dated: September 4, 2025

By: / Naveen Modi /
Naveen Modi (Reg. No. 46,224)
Counsel for Petitioner

CERTIFICATE OF SERVICE

I hereby certify that on September 4, 2025, I caused a true and correct copy of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 10,339,520 and supporting exhibits to be served via express mail on the Patent Owner at the following correspondence address of record as listed on PAIR:

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

By: /Naveen Modi/
Naveen Modi (Reg. No. 46,224)

APPENDIX A (CLAIM LISTING)

[10.pre]	A method of storing and generating payment information in an electronic device, the method comprising:
[10.a]	accepting a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information;
[10.b]	wherein the electronic device comprises device-specific and user-specific information; and,
[10.c]	wherein the issuer provided payment information is communicated wirelessly; and,
[10.d]	receiving wirelessly a static device account number payment information for storage on the electronic device; and wherein
[10.e]	at least a portion of the payment information is a limited-use number for limited use by the device, in place of a issuer provided payment information; and,
[10.f]	dynamically generating a one-time limited-use number based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information; and
[10.g]	using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.
[11]	The method of claim 10, wherein the electronic device is configured to accept the user input by at least one of a means comprising: a touch sensor array; a touch screen; a keypad; buttons; device motion; an accelerometer; a biometric input; a proximity contact sensor; optical sensors; an NFC unit; a wireless interface; a wired connection; a USB connection; an RF antenna; an inductor assembly.
[12]	The method of claim 10, wherein the device-specific information comprises at least one of a set including: device identifiers; device secrets; devices keys; device usage sequence counters; and device account numbers.

[13]	The method of claim 10, wherein the user-specific information comprises at least one of a set comprising: an email address; a username; a password; a PIN; a passcode; gestures; user information; bank accounts; payment information; device account numbers; merchant accounts; online accounts; currency amount; currency type; cryptocurrency address; cryptocurrency keys; private/public keys; signature information; and user secrets.
[14]	The method of claim 10, further comprising rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name.
[15]	The method of claim 14, further comprising accepting a user selection of a payment method type for use in a transaction responsive to a user selection from a list of payment method images rendered the display and using a touch screen interface for the user selection.
[16]	The method of claim 15, wherein the user selection is a default payment method to be used in transactions.
[17]	The method of claim 15, wherein the issuer provided payment information is selected from at least one of a set comprising: account number; card number; device account number; expiration date; card security codes; card validation values; card identification numbers; cardholder name; payment method type; merchant account; online account; an account type; a direction of transaction; the payment issuing authority; the amount of currency; the unit of currency; a funds type; cryptocurrency address; cryptocurrency key; cryptocurrency network; and card-type information.
[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:
[18.a]	providing, by the electronic device, at least one of account information; identification; and authorization, for the ATM transaction; and,
[18.b]	wherein the electronic device comprises a user interface comprising: displays; touch sensors; and buttons; and,

[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,
[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,
[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,
[18.f]	wherein the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC; and,
[18.g]	wherein the ATM is configured for performing the user selected account operation using the identification and authorizing information; and,
[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,
[18.i]	wherein said static and dynamic information is combined to perform the user selected ATM operation.
[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.

[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.
[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.
[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.
[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.

[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.
------	---