

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner

v.

CARDWARE INC.,
Patent Owner

Patent No. 10,810,579

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,810,579**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES	1
III.	PAYMENT OF FEES UNDER 37 C.F.R. §§ 42.15 AND 42.103	4
IV.	GROUND FOR STANDING.....	4
V.	PRECISE RELIEF REQUESTED AND GROUNDS RAISED.....	4
VI.	LEVEL OF ORDINARY SKILL	7
VII.	OVERVIEW OF THE '579 PATENT	8
VIII.	CLAIM CONSTRUCTION	9
IX.	DETAILED EXPLANATION OF GROUNDS.....	9
A.	Ground 1A: Royyuru in View of Phillips and Casey Render Claims 1, 2, 4, 6-9, 11-12, and 15-23 Obvious	9
1.	Royyuru.....	9
2.	Phillips	10
3.	Casey	11
4.	Royyuru-Phillips-Casey Combination.....	13
5.	Claim 1	18
6.	Claim 2	26
7.	Claim 4.....	27
8.	Claim 6.....	29
9.	Claim 7.....	31
10.	Claim 8.....	31
11.	Claim 9.....	32
12.	Claim 11	34
13.	Claim 12.....	34
14.	Claim 15.....	35
15.	Claim 16.....	36
16.	Claim 17.....	36

17.	Claim 18	37
18.	Claim 19	37
19.	Claim 20	41
20.	Claim 21	41
21.	Claim 22	43
22.	Claim 23	44
B.	Ground 1B: Royyuru in view of Phillips, Casey, and Spodak renders Claim 3 Obvious.....	44
1.	Claim 3	44
C.	Ground 1C: Royyuru in View of Phillips, Casey, Spodak, and Giordano Render Claim 5 Obvious.....	48
1.	Claim 5	48
D.	Ground 1D: Royyuru in View of Phillips, Casey, and Deibert Render Claims 10 and 14 Obvious.....	50
1.	Claim 10	51
2.	Claim 14	52
E.	Ground 1E: Royyuru in View of Phillips, Casey, Deibert, and Power Render Claim 13 Obvious.....	54
1.	Claim 13	54
F.	Ground 1F: Royyuru in View of Phillips, Casey, and Carlson Render Claims 4, 21, and 22 Obvious.....	55
G.	Ground 2A: Gomez in View of Amacker and Spodak Render Claims 1-9, 11-12, 15-20, and 22-23 Obvious.....	58
1.	Gomez	58
2.	Amacker	58
3.	Spodak.....	59
4.	Gomez-Amacker-Spodak Combination.....	59
5.	Claim 1	64
6.	Claim 2	70
7.	Claim 3	71

Petition for *Inter Partes* Review
Patent No. 10,810,579

8.	Claim 4.....	74
9.	Claim 5.....	75
10.	Claim 6.....	76
11.	Claim 7.....	77
12.	Claim 8.....	77
13.	Claim 9.....	77
14.	Claim 11.....	78
15.	Claim 12.....	79
16.	Claim 15.....	80
17.	Claim 16.....	81
18.	Claim 17.....	81
19.	Claim 18.....	81
20.	Claim 19.....	82
21.	Claim 20.....	84
22.	Claim 22.....	84
23.	Claim 23.....	85
H.	Ground 2B: Gomez in View of Amacker, Spodak, and Deibert Render Claims 10 and 14 Obvious.....	85
1.	Claim 10.....	86
2.	Claim 14.....	86
I.	Ground 2C: Gomez in View of Amacker, Spodak, Deibert, and Power Render Claim 13 Obvious.....	86
1.	Claim 13.....	86
J.	Ground 2D: Gomez in View of Amacker, Spodak, and Carlson Render Claims 4 and 22 Obvious.....	87
K.	Ground 2E: Gomez in View of Amacker, Spodak, Carlson, and Royyuru Render Claim 21 Obvious.....	88
X.	DISCRETIONARY DENIAL IS NOT APPROPRIATE	89
XI.	CONCLUSION.....	89

LIST OF EXHIBITS

EX1001	U.S. Patent No. 10,810,579 to Wyatt (“the ’579 patent”)
EX1002	Prosecution History of U.S. Patent App. No. 16/459,150
EX1003	Declaration of Dr. Michael Ian Shamos, Ph.D.
EX1004	U.S. Patent Publication No. 2010/0185545 to Royyuru
EX1005	U.S. Patent Publication No. 2012/0310760 to Phillips
EX1006	U.S. Patent No. 8,255,323 to Casey
EX1007	U.S. Patent No. 9,600,808 to Gomez
EX1008	U.S. Patent No. 8,423,462 to Amacker
EX1009	U.S. Patent Publication No. 2012/0123937 to Spodak
EX1010	U.S. Patent Publication No. 2013/0036050 to Giordano
EX1011	U.S. Patent Publication No. 2008/0017704 A1 to VanDeburg
EX1012	U.S. Patent Publication No. 2008/0172317 to Deibert
EX1013	U.S. Patent Publication No. 2008/0319905 to Carlson
EX1014	Curriculum Vitae of Dr. Michael Ian Shamos, PhD
EX1015	Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0
EX1016	U.S. Patent No. 8,052,052 to Power
EX1017	RESERVED
EX1018	RESERVED
EX1019	RESERVED
EX1020	RESERVED

EX1021	RESERVED
EX1022	CI Data Security Standard (PCI DSS), Information Supplement: PCI DSS E-commerce Guidelines (January 2013)
EX1023	RESERVED
EX1024	RESERVED
EX1025	Kadambi et al., Near-Field Communication-Based Secure Mobile Payment Service, ACM 11th International Conference on Electronic Commerce 2009
EX1026	CI Data Security Standard, Navigating PCI DSS: Understanding the Intent of the Requirements, Version 2.0 (October 2010)
EX1027	RESERVED
EX1028	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

I. INTRODUCTION

Google LLC (“Petitioner”) respectfully requests *inter partes* review of claims 1-23 (“the challenged claims”) of U.S. Patent No. 10,810,579 (“the ’579 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 LLC as the real party-in-interest.¹

Related Matters: The ’579 patent is asserted against Petitioner in *Cardware Inc., v. Google, LLC*, Case No. 7:24-cv-00278 (W.D. Tex.), which was filed on November 4, 2024.

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 11, 2017, now Pat. No. 10,339,520 (“the ’520 patent”), 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 Pat. No. 9,224,083, which is a division of application No. 14/217,261,

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.

filed on March 17, 2014, now Pat. No. 9,022,286, which claims priority to provisional application No. 61/794,891, filed on March 15, 2013, now expired. (EX1001, Cover.)

Additionally, the '579 patent is related to U.S. Patent Nos. 11,176,538 (“the '538 patent”) and 11,620,634 (“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.

The '634, '520, and '538 patents are also at issue in *Cardware Inc., v. Google, LLC*, Case No. 7:24-cv-00278 (W.D. Tex.).

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. 1-25-cv-00446 (W.D. Tex.), which was filed on November 4, 2024 and is still pending. The '520 patent is at issue in *Apple Inc. v. CardWare Inc.*, IPR2025-01145 (PTAB) and *Apple Inc. v. CardWare Inc.*, IPR2025-01146 (PTAB); the '579 patent is at issue in *Apple Inc. v. CardWare Inc.*, IPR2025-01148 (PTAB); the '538 patent is at issue in *Apple Inc. v. CardWare Inc.*, IPR2025-01149 (PTAB) and *Apple Inc. v. CardWare Inc.*, IPR2025-01150 (PTAB); and the '634 patent is at issue in *Apple Inc. v. CardWare Inc.*, IPR2025-01152 (PTAB). Petitioner has had no involvement with the earlier IPRs filed by Apple or Samsung.

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 '579 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 1-23 of the '579 patent. The challenged claims should be found unpatentable on the following grounds:

Ground 1A: Claims 1, 2, 4, 6-9, 11-12, and 15-23 are unpatentable under 35 U.S.C. §103 as being obvious in view of Royyuru (EX1004), Phillips (EX1005), and Casey (EX1006).

Ground 1B: Claim 3 is unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, and Spodak (EX1009).

Ground 1C: Claim 5 is unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, Spodak, and Giordano (EX1010).

Ground 1D: Claims 10 and 14 are unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, and Deibert (EX1012).

Ground 1E: Claim 13 is unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, Deibert, and Power (EX1016).

Ground 1F: Claims 4, 21, and 22 are unpatentable under §103 as being obvious in view of Royyuru, Phillips, Casey, and Carlson (EX1013).

Ground 2A: Claims 1-9, 11-12, 15-20, and 22-23 are unpatentable under §103 as being obvious in view of Gomez (EX1007), Amacker (EX1008), and Spodak.

Ground 2B: Claims 10 and 14 are unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, and Deibert.

Ground 2C: Claim 13 is unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, and Power.

Ground 2D: Claims 4 and 22 are unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, and Carlson.

Ground 2E: Claim 21 is unpatentable under §103 as being obvious in view of Gomez, Amacker, Spodak, Carlson, and Royyuru.

The earliest possible priority date of the '579 patent is March 15, 2013.² Royyuru published July 22, 2010 from an application filed January 22, 2009 (EX1004, Cover); Deibert published July 17, 2008 from an application filed January 9, 2008 (EX1012, Cover); Power published November 8, 2011 from an application filed December 4, 2008 (EX1016, Cover); Carlson published December 25, 2008 from an application filed June 24, 2008 (EX1013, Cover); and thus each qualifies as prior art under pre-AIA §§102(a), (b), and (e). Phillips published December 6, 2012 from an application filed September 1, 2011 (EX1005, Cover); Casey published August 28, 2012 from an application filed January 9, 2009 (EX1006, Cover); Spodak published May 17, 2012 from an application filed January 26, 2012 (EX1009, Cover); Giordano published February 7, 2013 from an application filed January 1, 2012 (EX1010, Cover); and thus, each qualifies as prior art under pre-AIA § 102(a) and (e). Gomez stems from an application filed June 22, 2012 (EX1007, Cover); Amacker stems from an application filed May 1, 2009 (EX1008, Cover); and thus, each qualifies as prior art under pre-AIA § 102(e).

² Petitioner does not concede that the '579 patent is entitled to a March 15, 2013 priority date.

VI. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) at the time of the alleged invention of the ’579 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, ¶¶49-54.³ More education can supplement practical experience and vice versa. *Id.*

³ Petitioner submits the declaration of Dr. Michael Shamos (EX1003), an expert in the field of the ’579 patent. EX1003, ¶¶1-13.

VII. OVERVIEW OF THE '579 PATENT

The '579 patent describes an electronic payment card capable of generating a “limited-duration number” for use in a payment transaction. EX1001, 2:23-61, 10:4-11:55, FIG. 7. Figure 7 illustrates a process for generating and using a limited-duration number:

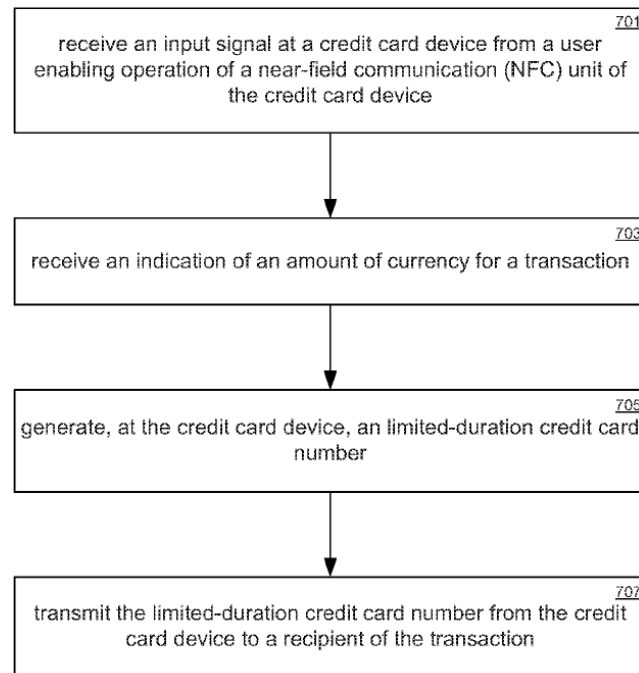


FIG. 7

EX1001, FIG. 7.

“The limited duration credit card number is able to be produced at the time the credit card device is performing a transaction, and is able to be generated according to the user’s private information, a bank information, information regarding the facility performing the transaction, and the time of day.” *Id.*, 10:13-18. Further, the “limited-duration credit card number is able to be limited to only one transaction.” *Id.*, 10:18-23.

VIII. CLAIM CONSTRUCTION

For IPR proceedings, the Board applies the claim construction standard set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). See 83 Fed. Reg. 51,340-59 (Oct. 11, 2018). The Board, however, only construes the claims when necessary to resolve the underlying controversy. *Toyota Motor Corp. v. Cellport Sys., Inc.*, IPR2015-00633, Paper No. 11 at 16 (P.T.A.B. Aug. 14, 2015)). Here, given the correlation between the prior art references and the challenged claims of the '579 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. (EX1003, ¶¶79-82.)⁴

IX. DETAILED EXPLANATION OF GROUNDS

As detailed below, each of the challenged claims are unpatentable. (EX1003, ¶¶83-480.)

A. Ground 1A: Royyuru in View of Phillips and Casey Render Claims 1, 2, 4, 6-9, 11-12, and 15-23 Obvious

1. Royyuru

Royyuru describes a system for conducting contactless financial transactions between a device and a Point-of-Sale (POS) device. EX1004, [0034]-[0035],

⁴ Petitioner reserves all rights to raise claim construction and other arguments in other venues.

[0044], [0045], [0047], [0046]. The user device generates “a set of dynamic cryptograms that are valid for a single transaction” including a “Dynamic Transaction Cryptogram (DTC)” and a “dynamic PAN” using various information stored on or received by the device. *Id.*, [0005]-[0010], [0032]-[0034], [0047]-[0048], [0051], [0057]. FIG. 3 shows the communication flow of the system:

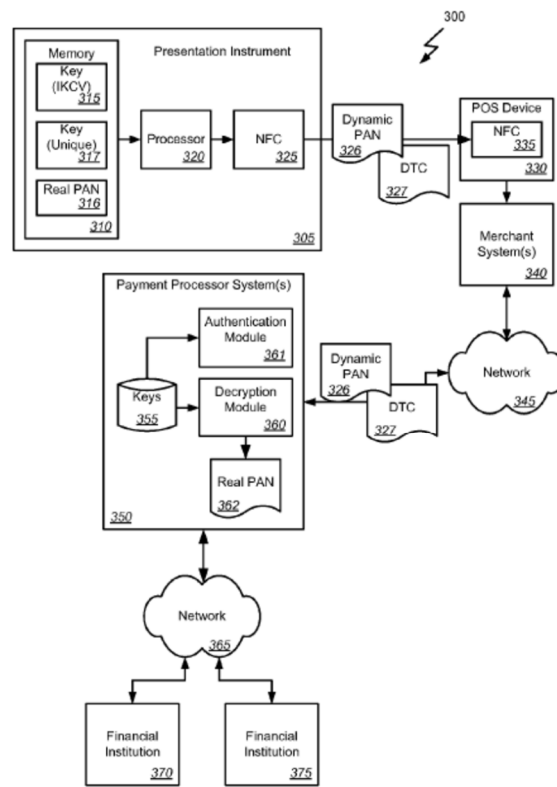


FIG. 3

EX1004, FIG. 3.

2. Phillips

Phillips describes interfaces that allow a user to select from among multiple payment options or use “an automatic card selection option.” EX1005, [0017], [0029], [0033]-[0035], [0059].

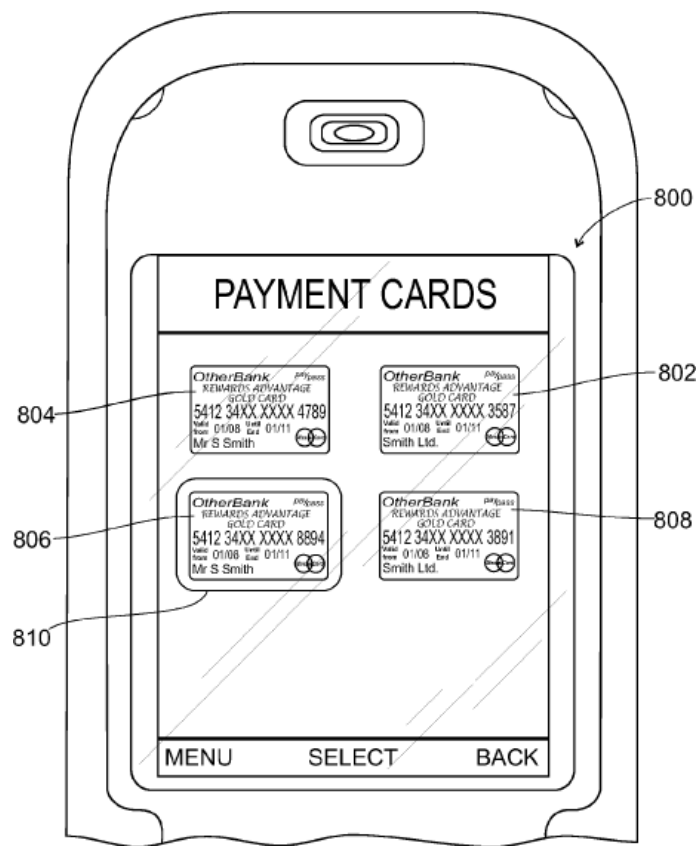


FIG. 8

Id., FIG. 8.

Phillips describes receiving “a payment request that includes a merchant identifier (merchant ID)” to initiate the card selection and payment transaction functions. *Id.*, [0072]. The request can take the form of “interrogation signals” received from a POS terminal via NFC. *Id.*, [0023], [0027], [0057].

3. Casey

Casey describes a mobile payment system that allows a user “to confirm or decline a payment transaction using a selected payment instrument” before transmitting “payment information for the payment transaction...to a merchant or

payment recipient.” EX1006, Abstract. FIG. 5 shows an example user interface flow for confirming a transaction:

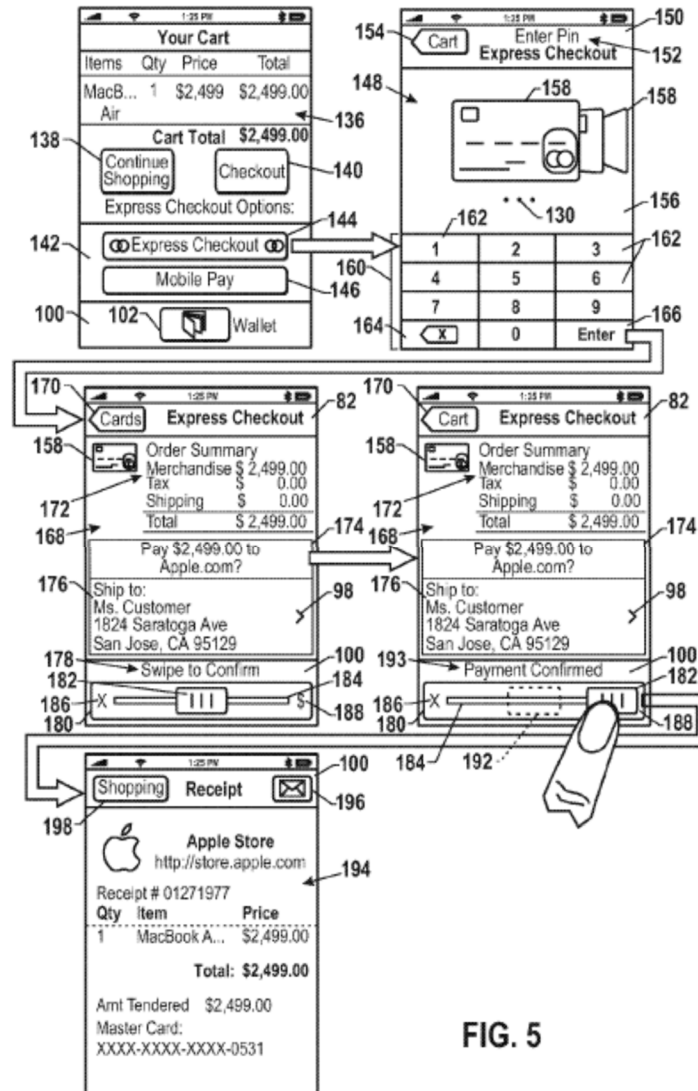


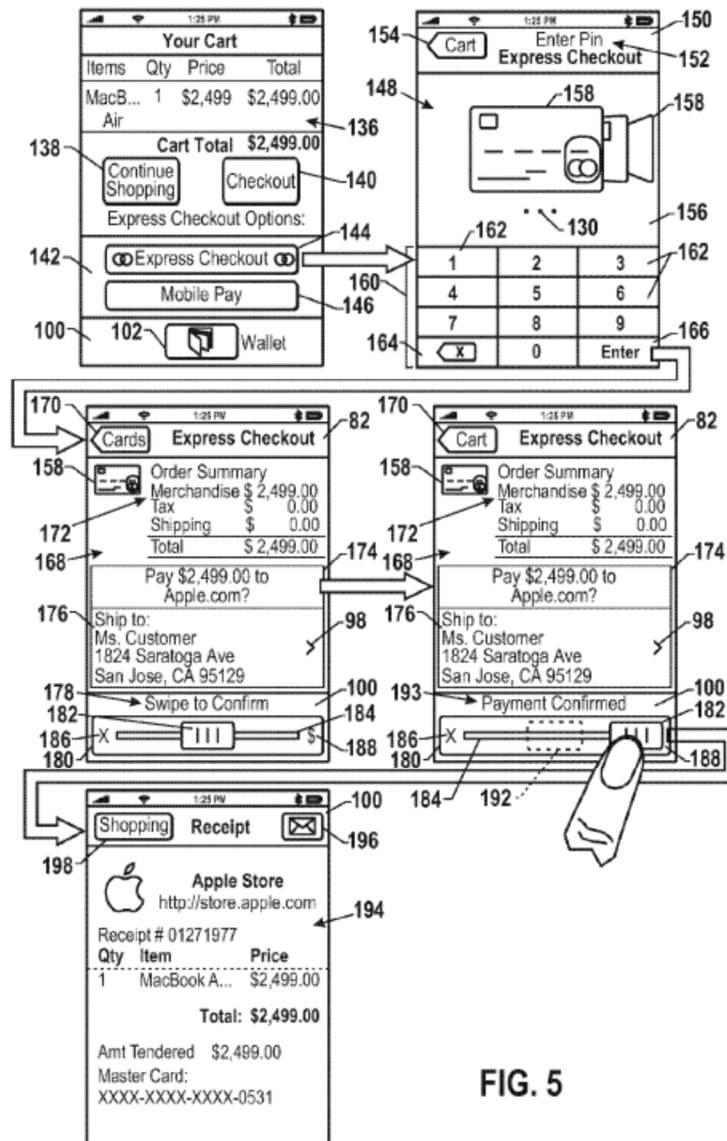
FIG. 5

Id., FIG. 5. After confirmation of the payment information by the payment processor, “device 10 may receive and display (block 78) a receipt for the payment transaction. *Id.*, 10:47-53, 10:20-29, 16:3-20.

4. Royyuru-Phillips-Casey Combination

A POSITA would have beneficially applied the teachings of Phillips and Casey to Royyuru to modify Royyuru's mobile payment system to include multiple improvements, including additional user interface and authentication features that complement Royyuru's focus on secure cryptogram generation. EX1003, ¶¶131-138.

First, a POSITA would have modified Royyuru based on Phillips and Casey such that the device receives a payment request from a POS terminal or other merchant device that includes information regarding the merchant and transaction. EX1005, [0072]; EX1006 8:52-9:8, FIGs. 5-8; EX1003, ¶¶132-133. Royyuru already discloses NFC communication between the user device and merchant device and Phillips beneficially discloses that such NFC communications can include a payment request for initiating a payment transaction from a POS terminal including transaction information such as a merchant identifier. EX1004, [0022], [0044], [0047]; EX1005, [0072], [0023], [0027], [0057]. Casey discloses the additional benefit of displaying such request information including the merchant, products being purchased, price, tax, etc. on the user device as shown in FIG. 5:



EX1006, FIG. 5, 8:52-9:8.

Modifying Royyuru's system such that the user device receives a payment request from a merchant device would have improved the system by providing information to the device that could be used to complete the payment transaction. EX1005, [0057]; EX1003, ¶¶133; *see also* EX1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49; EX1004, [0051].

Second, a POSITA would have modified Royyuru based on well-known authentication and confirmation techniques as taught by Phillips and Casey such that the user authorizes the payment transaction prior to payment information being provided to the merchant terminal such as by entering a PIN (Phillips and Casey) or moving a graphical element to confirm or deny the transaction (Casey). EX1003, ¶134; EX1005, [0035], [0038]-[0039], [0047], [0059], [0066], [0061]-[0062], [0068]; EX1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49. Requiring the user to enter a PIN “adds a layer of security to the process” by verifying that the current user is “the owner of a selected payment card account.” EX1005, [0035], [0038], [0062]; EX1003, ¶134. Requiring user authorization/confirmation would have provided multiple distinct improvements:

- allowing the user to review transaction information (e.g., price, purchased items) prior to completing the transaction;
- allowing the user extra opportunity to reconsider a transaction and definitively confirm or deny the transaction;
- ensuring that an authorized user of the payment method is conducting the transaction (in the case of entering a PIN); and
- avoiding unintended activation of a payment application and/or transmission of payment information.

EX1003, ¶134; EX1005, [0035], [0047]; EX1006, 3:20-35, 9:9-36.

Third, a POSITA would have modified Royyuru such that the device stores information for multiple payment options and provides a graphic interface, including payment method indicia, to allow user selection of a payment method as shown in FIG. 8 of Phillips.

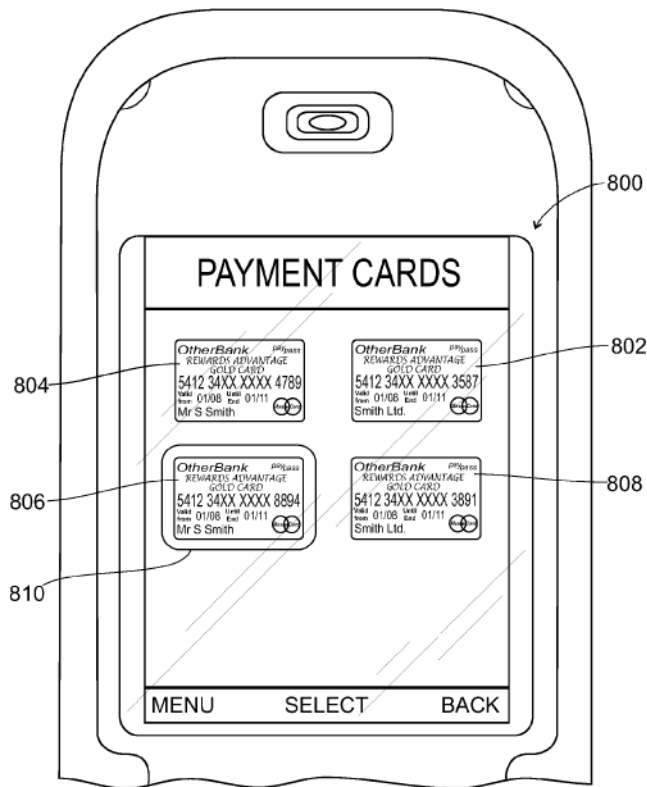


FIG. 8

EX1003, ¶135; EX1005, [0036]-[0041]; EX1006, 9:4-28, 9:58-10:2, 12:46-65; FIGs. 5-8. Allowing a user to select among multiple payment options would have provided more choices and options with respect to how the user spent their money, would have allowed the user to select payment options that are the most appropriate for a given scenario, and reduced or eliminated the need for the user to carry additional physical payment options. EX1003, ¶135.

Fourth, a POSITA would have modified Royyuru based on Phillips to allow the user to preselect one or more default payment options for different transaction scenarios to “enhance[] the speed and convenience of transactions” in those specific scenarios by allowing the user to make some payments using a default payment option (thus eliminating the need to select a payment option) while providing full flexibility to select a payment option in other scenarios when the user so desires. EX1003, ¶136; EX1005, [0005], [0017], [0059], [0066], [0017], [0029].

Fifth, a POSITA would have modified Royyuru based on Casey such that the device displays transaction status information, including received payment receipt information. EX1006, 10:47-53, 14:25-36, 16:3-20; EX1003, ¶137. Such a modification would have allowed the user to “confirm” that the correct transaction occurred, or more quickly take steps to correct an incorrect transaction, thus increasing user satisfaction and eventually increasing the customer base. *Id.*; EX1003, ¶137. The receipt could include such useful information as notification “when an order is ready to be picked up” and maps of the pickup location. EX1006, 16:3-20. Such a modification would have also allowed the user to more easily keep digital records of financial transactions. *Id.*; EX1003, ¶137.

Finally, a POSITA would have modified Royyuru based on Phillips and Casey because doing so would have been merely the application of known techniques to a

known system ready for improvement to yield predictable results. EX1003, ¶138; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

Here, all three references describe aspects of conducting wireless payment transactions using payment information stored on or generated by a device and Phillips and Casey describe improvements that would have been beneficially applied to Royyuru's system. EX1003, ¶138, 131. A POSITA would have furthermore had a reasonable expectation of success in modifying the mobile payment system of Royyuru based on Phillips and Casey as they all are directed toward similar mobile payment systems with Phillips and Casey simply providing additional details on known user interfaces and security measures. *Id.*

5. Claim 1

i) [1.pre]⁵

To the extent the preamble is treated as limiting, Royyuru describes “method[s] of processing a financial transaction.” EX1004, [0005]-[0010], [0002], [0035]. EX1003, ¶139.

⁵ Claim language corresponding to the limitations at issue may be found in the claim listing provided as Appendix A.

ii) [1.a]

Royyuru describes that “[w]hen the cardholder wishes to execute a transaction, such as a financial transaction...[he] passes or taps the presentation instrument 305 on or near the point-of-sale device 330.” EX1004, [0047], *see also* [0005], [0044], [0050], [0053]; EX1003, ¶140. Phillips teaches that in the combination, the user is required to “enter a PIN” before initiating a financial transaction and “add[] a layer of security to the process.” EX1005, [0035], [0038]-[0039], [0066]. A POSITA would have recognized that entry of a correct “personal identification number” is the input that corresponds to a priming operation that identifies the user as valid to initiate the card for executing a transaction. EX1003, ¶140; EX1005, [0035], [0038]; *see also* EX1001, 11:34-42, 13:25-32 (the ’579 patent’s examples of priming).

iii) [1.b]

The “device for initiating a financial transaction related to a financial account can comprise a processor.” EX1004, [0007]; EX1003, ¶141.

iv) [1.c]

Royyuru describes “a mobile device” and that “a presentation instrument 305 can comprise a smart card, mobile device, or any other device.” EX1004, [0021], [0040], [0046]. Royyuru incorporates by reference a patent publication that describes that the device “include[s] a touch screen” display. EX1004, [0021];

EX1011, [0006]; EX1006, 3:10-19. Phillips describes that a “display” is “in communication with and/or controlled by the control circuitry,” which “may be, for example, a main processor or microprocessor.” EX1005, [0018], [0020]; EX1003, ¶¶142, 60-63.

v) [1.d]

Royyuru’s device includes “an NFC module 325 communicatively coupled with the processor 320.” EX1004, [0051], [0046], [0002], [0022]; EX1003, ¶¶143, 55-59.

vi) [1.e]

Royyuru’s device can “detect initiation of the transaction.” EX1004, [0009]. The device uses NFC for “close proximity...short range communications between [the] mobile device and [the] POS device.” *Id.*, [0022], [0044], [0047], [0057] (describing transmission of UN to device via NFC); EX1005, [0023]. Phillips discloses that in the combination “the mobile device...receives 1302 a payment request that includes a merchant identifier (merchant ID)” from a POS terminal via NFC. EX1005, [0072], [0023], [0027], [0057]; *see also* EX1006, 8:52-9:8; FIGs. 5-8; EX1003, ¶144.

vii) [1.f]

FIG. 8 of Phillips shows “a ‘Payment Cards’ sub-menu” showing faces of “payment card account[s] issued to” the user to allow “selection of the payment card

account that corresponds to the payment card represented by the card-face image.”

EX1005, [0039]-[0041]; EX1003, ¶¶145-148.

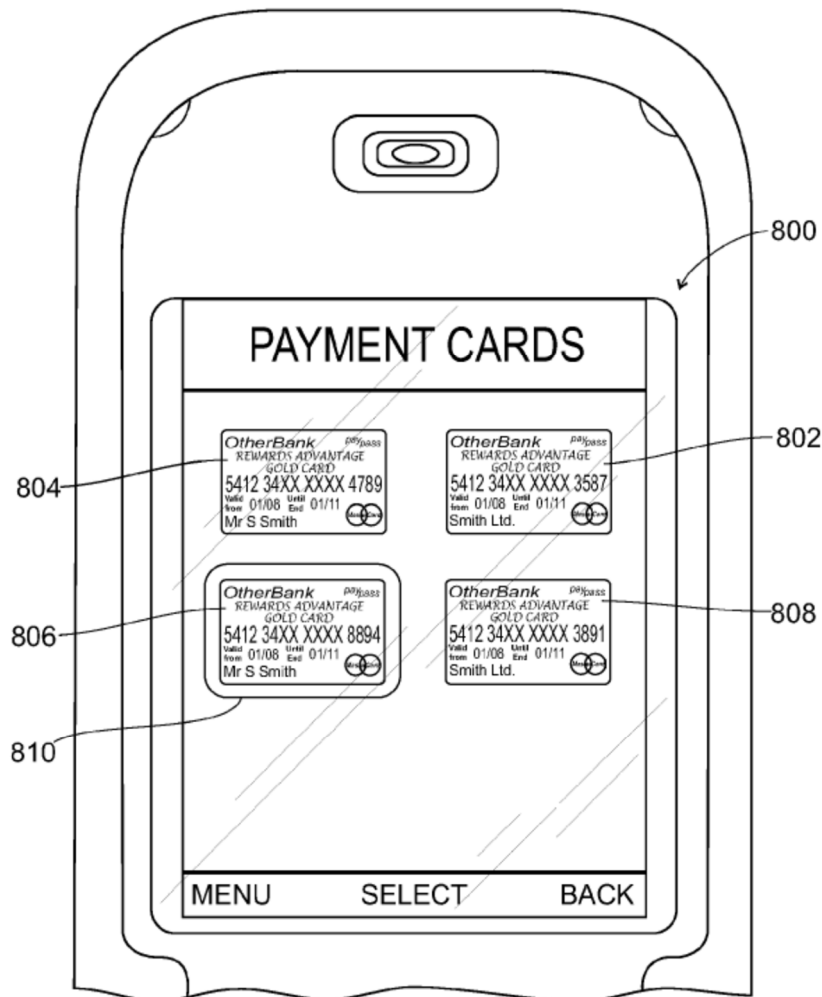


FIG. 8

EX1005, FIG. 8. The menu allows a user to “select one of the payment cards...to use in a current transaction.” *Id.*, [0037], [0039]; *see also* EX1006, 9:4-28, 9:58-10:2, 12:46-65. The displayed payment cards “include information such as the payment card account number [and] issuer bank name.” EX1005, [0039], [0036].

As shown in FIG. 8, the displayed issuer card account numbers are partial numbers with the last four digits displayed. *Id.*, FIGs. 8, 11; EX1003, ¶146. To the extent this element is interpreted narrowly, it would have been obvious to a POSITA to display **only** the last four digits of the issuer card account numbers to further enhance security by obscuring a larger portion of the credit card number while providing enough of the number to facilitate easy card recognition/selection by a user. EX1003, ¶¶147-148; EX1004, [0032] (describing displaying only the last four digits of “the real PAN” on a payment receipt for security purposes).

viii) [1.g]

As shown in FIGs. 8 and 11 of Phillips, the Royyuru-Phillips-Casey combination provides that an “issuer logo” is displayed on the touchscreen. EX1005, [0039], [0036], [0041], [0058], [0065]; EX1003, ¶¶149-151.

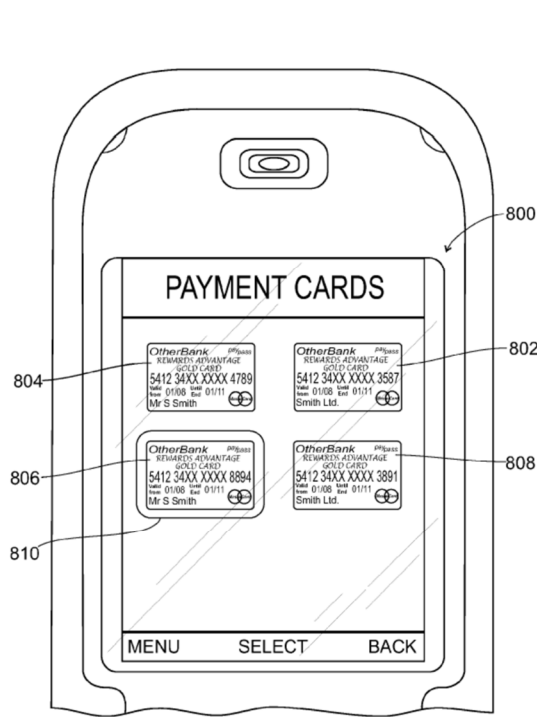


FIG. 8

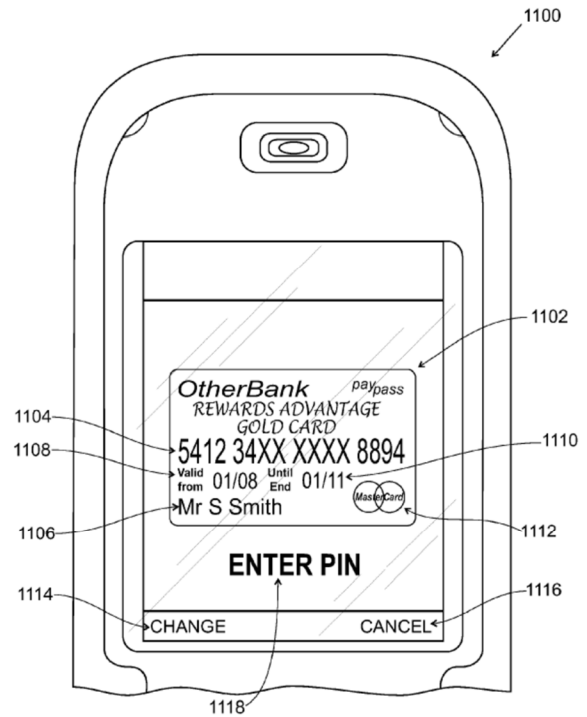


FIG. 11

EX1005, FIGs. 8, 11.

ix) [1.h]

As shown in FIGs. 8 and 11 of Phillips, *supra*, the displayed card-face “include[s] information such as the payment card account number, issuer bank name, issuer logo, card account holder name, the expiration date, a unique color or color combination, and/or other pertinent data.” EX1005, [0039], [0041], [0036]; EX1003, ¶¶152-154.

x) [1.i]

Royyuru provides at least two examples of the claimed “limited-use payment information”: the “Dynamic Transaction Cryptogram (DTC)” and the “dynamic PAN.” EX1004, [0005]-[0010], [0032]-[0033], [0047]; EX1003, ¶¶155-156. “A

Dynamic Transaction Cryptogram (DTC) can be ***generated at the device***, using a unique card level key stored on the device.” EX1004, [0005]. In another example, “[t]he DTC can be computed by the device by combining several fields including the PAN, service code, expiration date, unpredictable number, and ATC and encrypting them using the CK.” *Id.*, [0057]. The CK “is unique per card” and therefore the DTC is limited in use to the specific user device. *Id.*, [0057], [0032] (explaining that the term “card” refers to “a smart card” or “other device adapted for use as a payment instrument”), [0021]; EX1003, ¶155.

Similarly, the dynamic PAN is generated by the user device “based on the real PAN and an Institution Key Card Variant (IKCV) stored on the device.” EX1004, [0005]. In another example, the dynamic PAN is “computed by the device for each transaction by combining the digits from the card number with the ATC and with the unpredictable number sent by the RFID or NFC reader and then encrypting these digits with the IKCV.” *Id.*, [0057]. Both the DTC and dynamic PAN are “valid for a single transaction” and are therefore limited-use. *Id.*, [0033]. The dynamic PAN or “Pseudo-PAN can be sent in place of the real PAN.” *Id.*, [0057], [0007], [0032]. In other examples, Royyuru describes “providing the DTC and dynamic PAN to a Point-of-Sale (POS) device” and “from the POS device to a payment processor system” rather than the real PAN. *Id.*, [0006]-[0010]; EX1003, ¶156.

xi) [1.j]

Royyuru describes “[t]he device can then provide the DTC 327 and the dynamic PAN 326 to the NFC module 325” and then “providing the dynamic PAN to a Point-of-Sale (POS) device” via the NFC interface. EX1004, [0051]-[0052], [0034], [0047], [0054], [0057]; EX1003, ¶157.

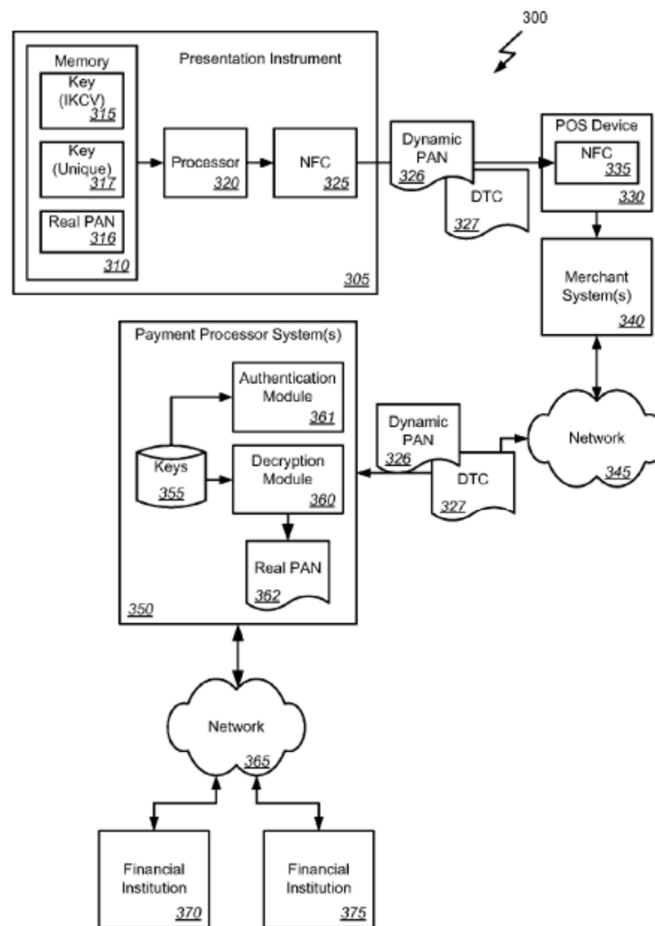
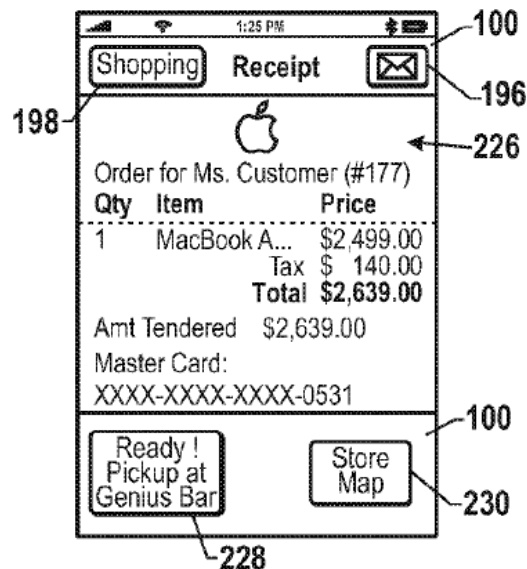


FIG. 3

EX1005, FIG. 3.

xii) [1.k]

As described by Casey, in the Royyuru-Phillips-Casey combination, “the device 10 may receive and display (block 78) a receipt for the payment transaction.



EX1006, FIG. 8. For example, the receipt may identify the amount tendered, the payment recipient, and the payment instrument used.” *Id.*, 10:47-53, *see also* 10:20-29, 16:3-20; EX1003, ¶¶158-159.

6. Claim 2

Royyuru describes that “[t]he DTC can be computed by the device by combining several fields including the PAN, service code, expiration date, unpredictable number, and ATC and encrypting them using the CK.” EX1004, [0057]. Similarly, in one example, the dynamic PAN is computed using “the digits from the card number with the ATC and with the unpredictable number sent by the RFID or NFC reader and then encrypting these digits with the IKCV.” *Id.* The PAN/card number are payment information; the unpredictable number is transaction,

device, merchant, NFC recipient, and payment reader information; the IKCV and CK are card issuer keys; the IKCV is a device account number; and the ATC is a device transaction sequence counter or device secret keys. *Id.*, [0004], [0006], [0057], [0047] (“time of day”), [0051]; EX1003, ¶¶160-163.

7. Claim 4

Royyuru’s IKCV is a device account number. EX1003, ¶¶164-168. The IKCV is “generated when each card (device) is being customized” and is generated by the payment processor or issuer based on the PAN and “institution key of the issuer of the account.” EX1004, [0057], [0046], [0033], [0055] (“IKCV of the device”); EX1003, ¶165. Because the IKCV can be generated by the issuer, a POSITA would have recognized that it is provided, either directly or indirectly, to the device for use by the device in payment transactions. EX1003, ¶165; EX1004, [0046], [0033], [0055], [0057]. A POSITA would have therefore recognized the IKCV as a device account number because it is specific to the device and based on payment account information. EX1003, ¶165. Royyuru describes that the IKCV is a card-level key (CK). EX1004, [0006], [0057]. The DTC is generated using one of the card-level keys (such as the IKCV) and the dynamic PAN is generated using the IKCV and therefore each comprises the device account number. *Id.*, [0057], [0005]-[0009].

The “expiration date” of the payment account is also used in generating the IKCV. EX1004, [0091]-[0096]. As would have been recognized by a POSITA, the IKCV has a limited time-duration of valid use because after the expiration date has expired, a new IKCV would need to be generated based on the new expiration date to match the valid account information having the new expiration date. EX1003, ¶166. Alternatively, it would have been obvious to a POSITA to make the IKCV of a limited time-duration of valid use tied to the payment account expiration date so that an IKCV generated using an expired PAN could not be used for transactions. EX1003, ¶166. This would help ensure that the user’s account is still valid. *Id.*

Because the IKCV is the device account number, the IKCV makes up part of the DTC and is therefore combined with the limited-use number (the dynamic PAN) as part of the device generated payment information. EX1003, ¶167; EX1004, [0057], [0005]-[0009]. As described with respect to claim 1, *supra*, the DTC and dynamic PAN are transmitted together to the POS terminal, and then the payment processor, in place of card issuer information (e.g., the real PAN and validation code) to perform payment transactions. EX1004, [0032]-[0034], [0047], [0051]-[0052]; EX1003, ¶167. The dynamic PAN can be sent in place of the real PAN. EX1004, [0057], [0032].

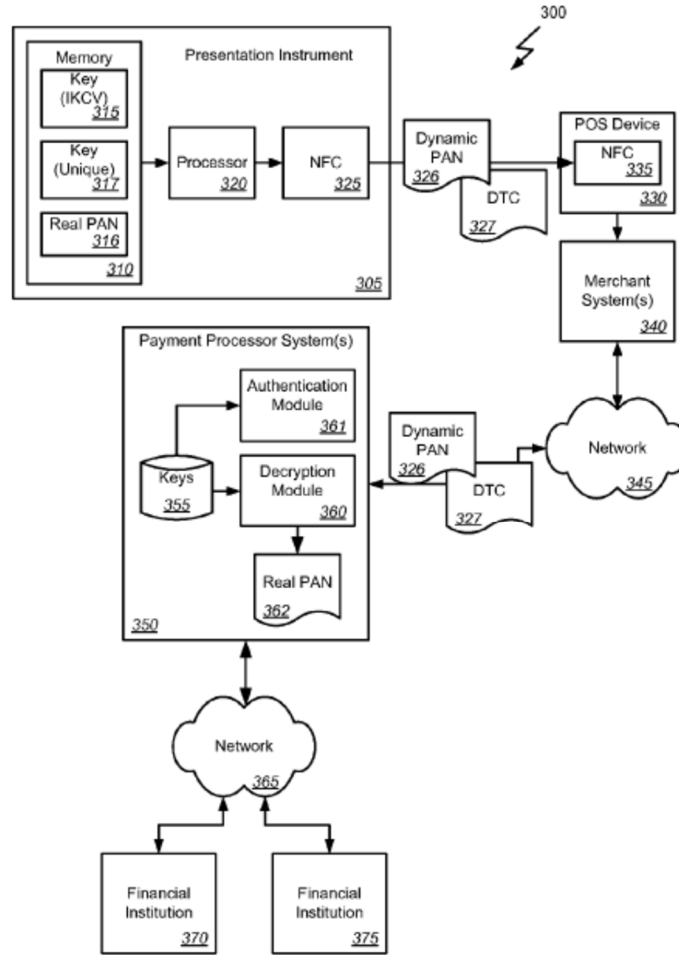


FIG. 3

EX1004, FIG. 3.

8. Claim 6

Royyuru discloses this limitation. EX1003, ¶¶169-173. Royyuru discloses that “[t]he transaction can be authenticated at the payment processor system or at the financial institution based on the DTC. For example, determining the real PAN can comprise decrypting the dynamic PAN using a key maintained by the payment

processor system and corresponding to one of the card-level keys of the device (e.g., the IKCV).” EX1004, [0006], [0034], [0039], [0048]. Furthermore, “[a]uthenticating the transaction at the payment processor can comprise validating the DTC using a key maintained at the DTC validation system (e.g., the payment processor system or the financial institution), corresponding to the unique card level key on the payment device.” *Id.* “The real PAN can then be sent from the payment processor system to a financial institution to affect processing of the transaction.” *Id.*

Therefore, the keys are used to verify the limited-use number for use in processing the transaction. EX1003, ¶¶171. After the DTC is validated, “using the unique card level key,” the real PAN is sent to the financial institution to process the transaction. EX1004, [0055], [0050]. The financial institution provides a response “to indicate approval and/or completion of the transaction.” *Id.*

A POSITA would have found obvious from the above disclosures that verification of the DTC and/or dynamic PAN by the payment processor are used in processing the transaction and therefore the limited-use number (DTC or dynamic PAN) is rejected if invalid number generation (e.g., invalid DTC or dynamic PAN) is detected. EX1003, ¶172. Furthermore, the DTC and dynamic PAN are valid for a single transaction, therefore they will be rejected by the payment processor if used

after the single transaction (invalid use of an expired limited-duration number).
EX1004, [0033], [0053], [0057]; EX1003, ¶172.

9. Claim 7

Phillips further discloses that the device of the Royyuru-Phillips-Casey combination can be primed by entering a pin to initiate a financial transaction to increase security. EX1005, [0035], [0038]-[0039], [0066]. The combination has “a touch screen capable of accepting user input” and therefore the user would enter the PIN using the device touch-screen interface. EX1005, [0020]; EX1003, ¶¶174-177.

10. Claim 8

Royyuru teaches that the priming operation can be an electronic device tap. EX1004, [0047], [0044]. The priming operation can also be entering a PIN on a touchscreen (a touch-input sequence) or selecting a payment method as taught by Phillips. EX1005, [0036]-[0041], [0020]; EX1003, ¶¶178-180; *see also* EX1006, 9:4-28, 9:58-10:2, 12:46-65. Phillips and Casey disclose that in the combination, the electronic device is enabled for payment through user entry of a valid PIN or correct user swiping. EX1005, [0059], [0062], [0066], [0070]; EX1006, 9:9-36, 12:64-13:51, FIGs. 5-8.

11. Claim 9

i) [9.a]

The device has a touchscreen for receiving input. *Supra*, Element [1.c]. Casey teaches that a user can swipe, or select a control, on the touchscreen to approve the payment:



EX1006, FIG. 5, *see also* FIGs. 6-8, 9:9-36, 13:24-51 (“...prompt the user to move a graphical element 180 to confirm the payment transaction”); EX1003, ¶¶181-183.

ii) [9.b]

Phillips discloses that the device of the Royyuru-Phillips-Casey combination displays a plurality of selectable payment accounts, expiration dates, payment bank logos, card images, etc.:

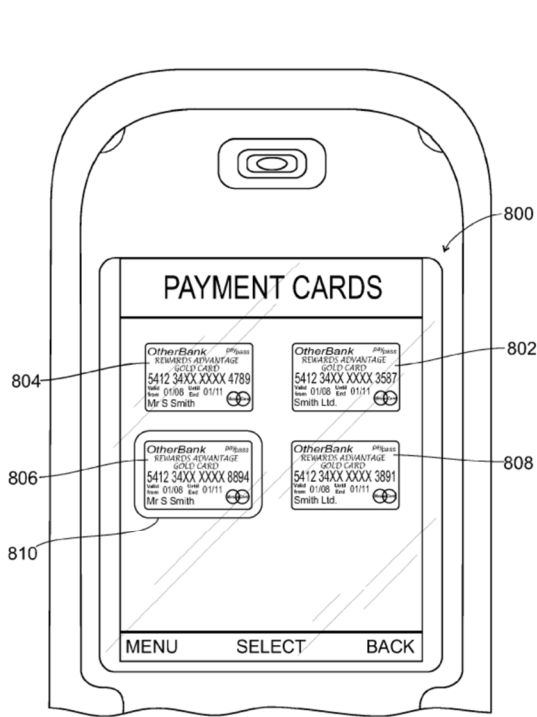


FIG. 8

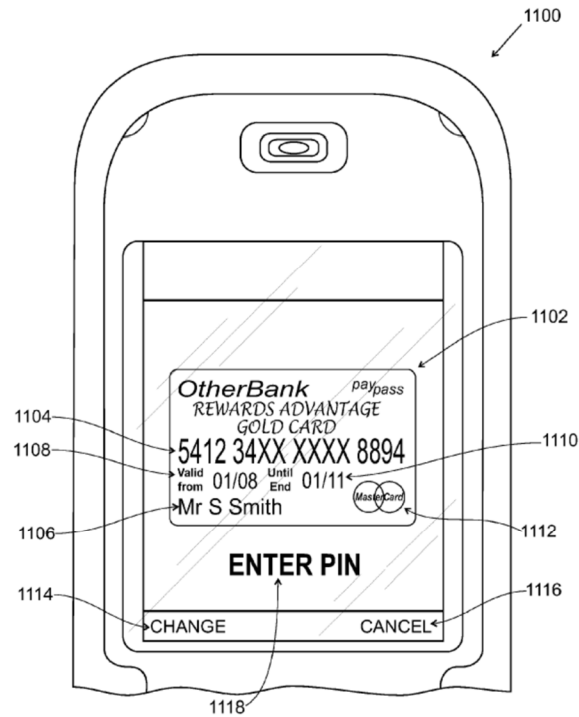


FIG. 11

EX1005, FIGs. 8, 11; [0036]-[0041]; *see also* EX1006, 8:52-9:28, 9:58-10:2, 12:46-65, 13:24-51, FIGs. 5-8; EX1003, ¶¶184.

iii) [9.c]

Phillips discloses receiving payment method selection user input. EX1005, [0036]-[0041]. The user can provide approval of an automatically selected card by entering a PIN. *Id.*, [0059], [0066]. The user can also cancel (deny) the transaction or adjust the transaction payment (change payment type). *Id.*, [0068].

Casey similarly discloses approving and denying the transaction such as by entering “a PIN to verify the payment instrument” or swiping in different directions to confirm or deny the transaction. EX1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49; EX1003, ¶¶185-188.

12. Claim 11

Phillips discloses exceptional conditions such as “a transaction in an amount above a certain limit” (“the transaction exceeding a pre-set amount limit”) (EX1005, [0059], [0066]). Phillips discloses that in response to the exceptional conditions, the device receives an authorization input from the user approving an “automatically selected card” by entering a PIN and the device presents a selectable option for the user to select “a different choice of card account.” *Id.*, [0059], [0066], [0061], [0068]; EX1003, ¶¶189-194; *see also* EX1006, FIGs. 5-8, 9:9-36, 9:66-10:2, 13:24-51, 14:12-49 (Casey providing similar disclosures).

13. Claim 12

As discussed with respect to Element [1.f], *supra*, the combination’s “‘Payment Cards’ sub-menu” allows “selection of the payment card account that corresponds to the payment card represented by the card-face image.” EX1005, [0036]-[0041], FIG. 8; 9:58-10:2, 12:46-65; EX1003, ¶¶196.

The displayed cards include expiration dates, card issuer icons, bank logos, card images, etc. EX1005, [0036]-[0041], FIG. 8. “[T]he user may be required to enter a PIN or code before selecting a payment card” and therefore the card selection menu is presented subsequent to the priming operation because priming is required to activate the payment function. EX1005, [0039]; EX1003, ¶196.

Phillips discloses that the device will proceed with a default payment option (“automatically selected card”) if the user does not select an alternative payment method, and the default card is identified based on previously entered user criteria. EX1005, [0005], [0017], [0029], [0059], [0066]; EX1003, ¶197.

14. Claim 15

i) [15.pre]

Supra, Preamble [1.pre]; EX1003, ¶200.

i) [15.a]

Supra, Elements [1.a], [1.d]-[1.e]; EX1003, ¶¶201-202.

ii) [15.b]

Supra, Elements [1.c], [1.f], [9.b]; EX1003, ¶203.

i) [15.c]

Supra, Elements [1.f], [9a], [9c], [11]-[12]; EX1003, ¶¶204-205.

i) [15.d]

Supra, Element [1.i]; EX1003, ¶¶206-207.

i) [15.e]

Supra, Element [1.j]; EX1003, ¶¶208-209.

i) [15.f]

Supra, Element [9.a]; EX1003, ¶¶210-211.

i) [15.g]

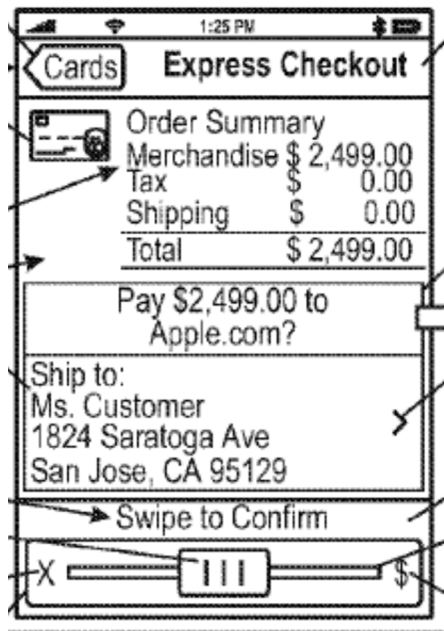
Supra, Elements [1.g]-[1.h], [9.b]; EX1003, ¶¶212-213.

i) [15.h]

Supra, Elements [9.a], [9.c], [11]; EX1003, ¶¶214-215.

15. Claim 16

The device of the Royyuru-Phillips-Casey combination has a touchscreen display. *Supra*, [1.c]; EX1004, [0021]; EX1011, [0006]; EX1005, [0018]; EX1006, 3:10-19. As described by Casey, the device presents a confirmation screen displaying “details about the sales order, such as the item price” and “a prompt asking a user to confirm the payment transaction.” EX1006, 13:24-51. The device “prompt[s] the user to move a graphical element 180 to confirm the payment transaction.” *Id.*



EX1006, FIG. 5; *see also* FIGs. 6-8; EX1003, ¶¶217-219.

16. Claim 17

Supra, Elements [1.f]-[1.h], [9.b]-[9.c], [11]-[12]; EX1003, ¶¶220-223.

17. Claim 18

Supra, Elements [1.a], [8]; EX1003, ¶¶224-227.

18. Claim 19

i) [19.pre]-[19.b]

In the combination, Royyuru discloses “a mobile device” having “a processor... and a memory communicatively coupled with and readable by the processor.” EX1004, [0021], [0007], [0046], [0051]; EX1003, ¶¶228-231; *supra* [1.a]-[1.b].

ii) [19.c]

Supra, Element [1.c]; EX1003, ¶232.

iii) [19.d]

The device of the Royyuru-Phillips-Casey combination includes “one or more input devices 210 (e.g., a scan device, a mouse, a keyboard, etc.)” including a touchscreen. EX1004, [0040], [0021]; EX1011, [0006]; EX1005, [0018]; EX1003, ¶¶233-234, *supra* [1.c].

iv) [19.e]

Supra, Elements [1.e]-[1.f]; EX1003, ¶¶235.

v) [19.f]

“The memory can also have stored therein a series of instructions which, when executed by the processor, cause the processor to” perform the described actions. EX1004, [0007], [0051]; EX1003, ¶236.

vi) [19.g]

Supra, Elements [1.a], [7]-[8]; EX1003, ¶¶237.

vii) [19.h]

In the combination, Royyuru describes “a consumer can use the presentation instrument 305 to initiate a transaction at the POS device 330, for example by scanning or tapping the presentation instrument 305 on or near the POS device 330 at the time of payment for a purchase.” EX1004, [0044]; *supra*, Elements [1.a], [8]. In another example, “[p]assing or tapping the presentation instrument near the POS device 330 can trigger” the device to generate the dynamic PAN and DTC and provide them “to the merchant system 340, e.g., via the NFC module 325 of the presentation instrument and corresponding NFC module 335 of the POS device 330” to enable the device for imminent performance of the transaction. *Id.*, [0047]; EX1003, ¶¶238.

In the combination, Phillips and Casey disclose that the electronic device is enabled for payment by priming actions such as user entry of a valid PIN or correct user swiping. EX1005, [0035], [0059] (“a payment transaction...is not enabled unless the PIN had been recently entered”), [0062], [0066], [0070]; EX1006, 9:9-36, 12:64-13:51, FIGs. 5-8; EX1003, ¶¶239.

viii) [19.i]

Supra, Elements [1.f]-[1.h]; EX1003, ¶240.

ix) [19.j]

Supra, Elements [1.f], [9a], [9c], [11]-[12]; EX1003, ¶241.

x) [19.k]

As discussed with respect to Elements [1.e] and [1.i], *supra*, Royyuru discloses generating a limited-use payment information for use in place of a card issuer supplied payment information in the form of both the DTC and dynamic PAN. *Supra*, [1.i]; EX1003, ¶¶242.

Phillips discloses that in the predictable Royyuru-Phillips-Casey combination, the verification cryptograms (DTC and dynamic PAN) are generated in response to receiving an NFC transaction payment request. EX1003, ¶243. Similar to Royyuru, Phillips discloses that the device interacts with the POS terminal via NFC. EX1005, [0023]. In the combination, Phillips discloses that the transaction is initiated when “the mobile device...receives 1302 a payment request.” EX1005, [0072]. The request can come in the form of “interrogation signals” received from a POS terminal via NFC. *Id.*, [0023], [0027], [0057]; *see also* EX1006 8:52-9:8 (“receiving information through...the NFC device...may include a request for payment”); FIGs. 5-8; EX1003, ¶243.

Phillips discloses that, after receiving these interrogation signals and receiving a merchant identifier, the user device automatically selects a user payment card or allows the user to select a different payment method. EX1005, [0057]-[0058].

Phillips further discloses that the device “cryptographically generate[s] a dynamic security code (CVC3) for the transaction and transmit[s] the dynamic security code to the reader.” *Id.*, [0059]. Because the transaction is initiated in response to a request from the POS device, a POSITA would have recognized that this cryptographic dynamic security code is generated in response to receiving the NFC transaction payment request. EX1003, ¶244.

Therefore, because Royyuru discloses that the DTC and dynamic PAN are dynamically generated responsive to the device “detect[ing] initiation of the transaction” (EX1004, [0047], [0009]), a POSITA would have recognized that in the combination of Royyuru with Phillips and Casey, based on Phillips’ disclosure that the transaction is initiated responsive to receiving the payment request at the device (EX1005, [0072], [0023], [0027], [0057]-[0059]), the device generates the DTC and dynamic PAN responsive to receiving the NFC transaction payment request. EX1003, ¶245.

xi) [19.l]

Supra, Element [1.j]; EX1003, ¶246.

xii) [19.m]

Supra, Element [1.k]; EX1003, ¶247.

19. Claim 20

Supra, Elements [1.a], [1.c], [7]-[8], [11]. A POSITA would have recognized that a touchscreen provides or at least renders obvious a touch sensor array and a touch key-pad and that a valid PIN entry, as described above with respect to Elements [1.a] and [9.c] and claims [7]-[8] and [11]-[12] provides a correct passcode entry sequence and a correct user response input from a security challenge (“an ‘Enter PIN’ prompt”) to verify that the user is a valid user. EX1003, ¶¶249-251; EX1005, [0035], [0038], [0058]-[0059] (describing PIN entry using a “numeric keypad” of the touchscreen).

20. Claim 21

Royyuru discloses that the “memory [is] communicatively coupled with and readable by the processor.” EX1004, [0007]. As discussed with respect to claims [3]-[4], *supra*, Royyuru discloses a static device-specific device account number of limited-use in the form of the IKCV stored on the device. EX1003, ¶¶253. The IKCV is “generated when each card (device) is being customized” and is generated by the payment processor or issuer based on the PAN and “institution key of the issuer of the account.” EX1004, [0057], [0046], [0032]-[0033], [0054]-[0055]. The IKCV is a device account number because it is specific to the device and is based on payment account information. EX1003, ¶253. Because it can be generated by the issuer and provided to the device, it is static and originates from a card issuing

authority. *Id.* The IKCV is of limited-use because it can only be used for transactions by the specific device. EX1003, ¶253; EX1004, [0057].

The IKCV has a limited time-duration based on the expiration date of the payment account or alternatively it would have been obvious to a POSITA to make the IKCV of a limited time-duration based on the expiration date of the payment account. *See, supra*, Claim [4]; EX1004, [0091]-[0096]; EX1003, ¶254.

The DTC is generated using one of the card-level keys (such as the IKCV) and the dynamic PAN is generated using the IKCV. EX1004, [0057], [0005]-[0009]. Both the DTC and the dynamic PAN are limited-use payment information. *Supra*, Element [1.i]. Furthermore, Royyuru discloses that the “dynamic PAN can also be based on an undeterminable number.” *Id.*, [0033]. Royyuru also discloses “generat[ing] a dynamic PAN 326 based on the real PAN 316, the card-level key 315, and one or more factors from the payment device or the POS reader such as unpredictable numbers or counters.” *Id.*, [0051]. The undeterminable number can be any “received by the presentation instrument 305” which includes the expiration date, which, as described above, is the expiration date for both the real PAN and the IKCV generated using the expiration date. *Id.*, [0051], [0057], [0091]-[0096]; EX1003, ¶255. Therefore, the dynamic PAN is limited-use payment information generated in part based on combining the IKCV (static device-specific device account number) and the device account expiration date. EX1003, ¶255.

Similarly, the DTC is generated using values including “expiration date” and a card-level key (which can be the IKCV). EX1004, [0057], [0005]-[0006]; EX1003, ¶256. Therefore, the DTC is another example of limited-use payment information generated in part based on combining the IKCV (static device-specific device account number) and the device account expiration date. EX1003, ¶256. Phillips discloses that the cryptogram is generated after selection of the payment method. EX1005, [0059], [0066]. Indeed, the DTC and dynamic PAN are generated based on information specific to the selected account. EX1004, [0051], [0057], [0005]-[0006].

21. Claim 22

As discussed with respect to claims [21] and [3]-[4], *supra*, the IKCV is a limited-use device account number stored in the memory accessible to the processor that is valid for a limited duration (expiration date) or alternatively it would have been obvious to a POSITA to make the IKCV of a limited time-duration of valid use. EX1004, [0007], [0057], [0046], [0032]-[0033], [0054]-[0057], [0091]-[0096]; EX1003, ¶¶259.

The IKCV is a key and Royyuru discloses that the device stores numerous other “unique card level key[s] stored on the device.” EX1004, [0005]-[0007], [0032] (describing “a unique encryption key per card or other device” and “a unique, card-level key” each stored on the device), [0051], [0057], FIG. 3; EX1003, ¶¶260.

The DTC is generated using one of the card-level keys (such as the IKCV) and the dynamic PAN is generated using the IKCV. EX1004, [0057], [0005]-[0009]. Both the DTC and the dynamic PAN are one-time limited-use cryptogram numbers. *Supra*, Claim [3]. The IKCV makes up part of the dynamic PAN and is therefore combined with the limited-use cryptogram number (the DTC) (as part of the device generated payment information. EX1003, ¶261; EX1004, [0057], [0005]-[0009]. Alternatively, the IKCV makes up part of the DTC and is therefore combined with the limited-use cryptographic number (the dynamic PAN) as part of the device generated payment information. EX1003, ¶261; EX1004, [0057], [0005]-[0009].

22. Claim 23

Supra, Elements [1.j], [2]-[3]; EX1003, ¶263-264.

B. Ground 1B: Royyuru in view of Phillips, Casey, and Spodak renders Claim 3 Obvious

1. Claim 3

Royyuru discloses generating a “Dynamic Transaction Cryptogram (DTC)” that is “valid for a single transaction.” EX1004, [0005], [0033], [0053], Abstract. This cryptogram is generated based on an Application Transaction Counter (ATC) and an “unpredictable number,” and then “encrypting them.” *Id.*, [0057], [0084]. The “unpredictable number” can be “a time of day.” *Id.*, [0047]. Royyuru discloses dynamically generating the cryptogram by “cryptographically combining a device transaction sequence counter count and at least one [of] ... a time.” EX1003, ¶266.

Royyuru discloses that the ATC “increments for each transaction,” EX1004, [0057], which discloses that generating the cryptograms “results in a one-time limited-use number via the device incrementing said device transaction sequence counter count on a transaction,” as claimed. EX1003, ¶267.

Having looked to Royyuru’s disclosure about scanning the presentation instrument at a POS device that is capable of reading a magnetic stripe (EX1004, [0024], [0044]), a POSITA would have looked to Spodak for how to communicate with such POS devices. EX1003, ¶¶268-269. Similar to Royyuru-Phillips-Casey, Spodak discloses 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], [0027], [0033]-[0035]. To emulate the magnetic stripe and “authenticate the transaction with the card issuer,” the universal card generates a “dynamic authentication value,” which discloses the claimed “cryptogram number.” *Id.*, [0094]. Spodak discloses that “the universal card may generate a dynamic authentication value and write the dynamic authentication value in the field typically used for the static CVV value,” *id.*, which discloses that this value is generated “for use by the electronic device in place of a card validation value originated from the card issuer” as claimed. EX1003, ¶269. The dynamic authentication value is generated based on “a random number” and “a transaction counter.” EX1009, [0094]. Because the “dynamic authentication value is unique

for every transaction,” *id.*, generating the dynamic authentication value “results in a one-time limited-use number” as claimed. EX1003, ¶270.

For the Royyuru-Phillips-Casey combination to communicate with a magnetic stripe reader, a POSITA would have been motivated to incorporate the dynamic magnetic stripe from the universal card of Spodak into the Royyuru-Phillips-Casey combination. EX1009, [0035], [0088]-[0089]; EX1003, ¶271. The improved device would be compatible with a greater number of POS devices: those that communicate via a magnetic stripe reader and those that communicate via short range wireless communications such as NFC. EX1003, ¶271.

To the extent that the Royyuru-Phillips-Casey combination does not disclose generating a cryptogram separately from the limited-use payment information in claim 1, a POSITA would have applied Spodak to improve the device by generating the dynamic authentication value to enable the device to conduct transactions with both a magnetic stripe reader and a contactless payment terminal. EX1009, [0088]-[0089], [0094]; EX1003, ¶272. The improved device would be compatible with a magnetic stripe reader by generating the dynamic authentication value for use in place of a card validation value (CVV) originating from the card issuer. EX1009, [0094]; EX1003, ¶¶272.

To the extent that Spodak does not disclose generating the dynamic authentication value cryptographically, a POSITA would have further been

motivated to apply Royyuru's disclosure about encrypting its dynamic transaction cryptogram to Spodak to encrypt its dynamic authentication value. EX1004, [0058]-[0060], [0084]; EX1003, ¶¶273. A POSITA would have been motivated to encrypt Spodak's dynamic authentication value because like Royyuru's dynamic transaction cryptogram, Spodak's dynamic authentication value is used to securely conduct a transaction. EX1004, [0047], [0057], [0084]; EX1009, [0094]; EX1003, ¶273. To the extent that Spodak does not disclose incrementing its transaction counter, a POSITA would have further been motivated to apply Royyuru's disclosure about incrementing its Application Transaction Counter (ATC) to Spodak to increment its transaction counter. A POSITA would have been motivated to increment Spodak's transaction counter by virtue of it being a counter, and because both Royyuru's dynamic transaction cryptogram and Spodak's dynamic authentication value are generated based on a transaction counter and a random/unpredictable number. EX1004, [0047], [0057], [0084]; EX1009, [0094]; EX1003, ¶273.

Furthermore, a POSITA would have recognized that application of Spodak's teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. EX1003, ¶¶274. A skilled person would have appreciated that the above-described combination would have merely involved a combination of known prior art

technologies (e.g., known devices for conducting transactions via both a magnetic stripe reader and a contactless payment terminal) according to known methods (e.g., known process for securing payment information during the transactions) to yield the predictable result of a device that could securely conduct transactions with both a magnetic stripe reader and a contactless terminal. EX1003, ¶274.

C. Ground 1C: Royyuru in View of Phillips, Casey, Spodak, and Giordano Render Claim 5 Obvious

1. Claim 5

Spodak’s generation of the dynamic authentication value in the Royyuru-Phillips-Casey-Spodak combination renders obvious “generating a limited-use security number” and the remaining features of this “generating” step for the reasons discussed in Ground 1B, *supra*, Element [3]; EX1003, ¶¶265-275. As for the “displaying” step, Spodak discloses that its universal card includes a display for displaying “an account number” or “any other information.” EX1009, [0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A. A POSITA would have understood that “information” can be the “authentication value” that satisfies the claimed “limited-use security number.” EX1003, ¶¶277. Having appreciated Spodak’s display, a POSITA would have further been motivated by Giordano to display the claimed number. EX1003, ¶¶277.

Similar to Royyuru and Spodak, Giordano describes a mobile payment system for a person-to-merchant (P2M) payment service “to make payments...without

having to share any confidential account information.” EX1010, [0028]. Giordano describes a mobile payment device that generates an “alias” for each transaction based on information unique to the device and other information related to the transaction. *Id.*, [0028], [0029], [0033], [0080]. Giordano further discloses “prompt[ing] the user to approve a random or default static alias.” *Id.*, [0032]. The user can select, generate, or modify an alias “using the P2M application,” a “web-based module,” or a “banking application.” *Id.*, [0032], [0038], [0066]. The “alias is only available for a limited time or limited number of transactions before it expires and must be changed.” *Id.*, [0032]. To manage the alias, the user can use a web browser or the P2M application on a device that displays graphical user interfaces on its display. *Id.*, [0033], [0059], [0066]; EX1003, ¶¶278-279.

A POSITA would have been prompted to apply the teachings of Giordano to the Royyuru-Phillips-Casey-Spodak combination to provide a mobile payment system in which the generated limited-use security number (e.g., the combined dynamic authentication value and alias) is displayed on the device for the user to approve or modify the security number. *Id.*, [0032], [0038]; EX1003, ¶¶280. Because the security number is only available for a unique transaction (EX1009, [0094]) or a limited time or limited number of transactions (EX1010, [0032]), a POSITA would have further been motivated to display the number to increase the utility of the device by allowing the user to know when the security number is

expected to expire and require modification. EX1003, ¶280. Furthermore, a POSITA would have recognized that the application of Giordano’s teachings to the Royyuru-Phillips-Casey-Spodak device is merely the application of known techniques to known devices ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. *Id.*

D. Ground 1D: Royyuru in View of Phillips, Casey, and Deibert Render Claims 10 and 14 Obvious

Deibert describes a mobile payment system with a disabling feature. EX1012, Abstract. The user can set “a predetermined timeout time such that the mobile payment application is disabled after the predetermined timeout time has elapsed” to “help prevent the accidental transmittal of [payment] information.” *Id.*, [0009], [0023]. Deibert discusses manual activation of a mobile payment application and multiple techniques for disabling the mobile application to prevent unintentional transmittal of payment information, including completion of a transaction, manual disabling based on user input, and expiration of a predetermined timeout time. *Id.*, [0023]-[0025], [0058]-[0059]; EX1003, ¶283.

A POSITA would have been prompted to apply the teachings of Deibert to the Royyuru-Phillips-Casey combination to include multiple mechanisms by which a payment priming operation is disabled (including through completion of a transaction, manual user input, and expiration of a timeout period) to “help prevent

the accidental transmittal of information,” provide increased functionality of allowing the user to intentionally return the device to an idle state, and to “allow[] the phone to have full contactless card functionality, while removing limitations.” EX1012, [0023]-[0025], [0061]. EX1003, ¶284. This modification also “minimize[s]” user concern and hesitancy regarding mobile payment transactions, thus increasing user satisfaction. EX1012, [0061]; EX1003, ¶284. Such a modification would also save power by decreasing the amount of time that the NFC circuit is actively transmitting payment information and increase ease of use by providing mechanisms for disabling payment priming that don’t require user interaction. EX1003, ¶284. Furthermore, a POSITA would have recognized that application of Deibert’s teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. EX1003, ¶284.

1. Claim 10

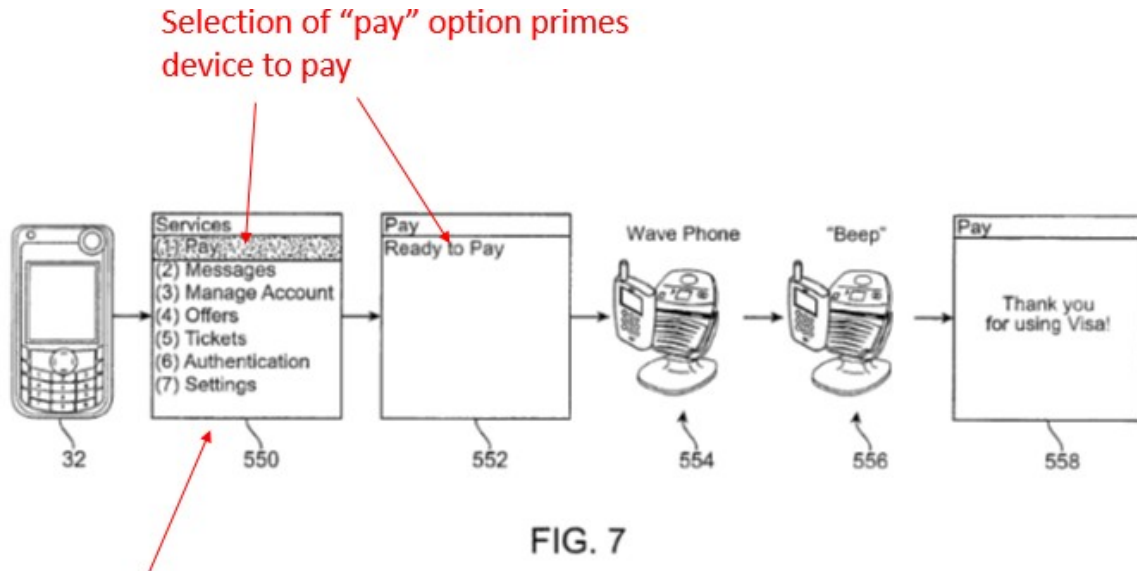
Like Royyuru, Deibert similarly discloses using NFC to facilitate communications between the user device and merchant terminal during mobile payment transactions. EX1012, [0019], [0040]; EX1004, [0022], [0044], [0047]. Deibert describes manually activating an application (e.g., priming) and in response “the mobile phone will transmit payment information.” EX1012, [0023]. This

communication can be disabled after “a predetermined timeout time.” *Id.*, [0025]-[0026], [0058]. The manual activation can include “entering a password.” *Id.*, [0057]. A POSITA would have understood that terminating the mobile payment application provides, or at least renders obvious, terminating the NFC communication and aborting the transaction. EX1003, ¶286.

2. Claim 14

Both Phillips and Casey disclose requiring a PIN (a passcode) to access the payment application/functionality prior to selecting a specific payment method. EX1005, [0035], [0038]-[0039], [0066]; EX1006, 9:9-36. A POSITA would have recognized that user selection of a payment method provides a priming operation after entry of the PIN/passcode. EX1003, ¶289. Deibert similarly describes requiring “entering a password into the mobile phone application, in order to authenticate the consumer 30 and prevent fraud.” EX1012, [0057], [0049] (“user is prompted to enter a password”). Deibert describes further priming operations after entry of the password, including manual activation of the payment application after expiration of a timeout period without requiring additional password entry. EX1012, [0058], [0023] (describing that the user “manually select[s] the mobile phone application each time before making a purchase). In another example, Deibert describes that after the payment application is opened (which can require entry of a password), the device requires a further priming operation of selecting the “pay

functionality of the mobile payment application” to prime the device “to engage in a payment transaction.” EX1012, [0060], [0057]; EX1003, ¶289.



EX1012, FIG. 7, [0057], [0060].

Furthermore, a POSITA would have recognized that payment priming is a type of device priming. EX1003, ¶290. Deibert discloses disabling a device priming on further button pressing. EX1012, [0024]. Deibert further teaches that “[i]f no payment transaction occurs within the predetermined timeout time, then after the predetermined timeout time, the mobile payment application on the phone will automatically disable so that contactless payments cannot be made.” *Id.*, [0025]-[0026], [0058]-[0060]; EX1003, ¶290.

E. Ground 1E: Royyuru in View of Phillips, Casey, Deibert, and Power Render Claim 13 Obvious

1. Claim 13

Phillips discloses priming (preparing the device to transmit payment information) through selection of a “card accounts” option from menu 700 followed by selection of a displayed payment option. EX1005, [0036]-[0037], FIGs. 7-8. These menu button selections would have been conducted via the “select button” disclosed by Phillips in at least some embodiments. EX1005, [0033]; EX1003, ¶297. This sequence of menu selections using a button falls within the disclosure of a button double press in the ’579 patent. EX1001, 9:64-10:3, 17:19-23.

Furthermore, a POSITA would have applied the teachings of Power to Royyuru-Phillips-Casey-Deibert to require biometric sensing of the device continuously remaining in contact of the valid user and disabling the priming operation when the device is not continuously in contact with the user. EX1003, ¶¶294-295, 298. Powers teaches that the device “detects a presence or an absence of a gating signal.” EX1016, 2:1-3. In some embodiments, presence of the gating signal (to allow use of a smart payment device) requires continued contact with “the customer’s body.” *Id.*, 4:37-43. The device includes a transducer to “monitor[] the one or more physical phenomena” and enables/disables the wireless-communication circuit in response to detection or absence of the physical phenomena. *Id.*, 2:52-60, 3:51-67. The transducer(s) can detect a temperature, resistance, capacitance, or

pressure change “when the user is holding the payment card” such that the device “is only active (and able to communicate the financial information) when it is being used by customer.” *Id.*, 1:55-62, 3:65-4:19.

A POSITA would have applied these teachings of Power to Royyuru-Phillips-Casey-Deibert to “protect” transaction information from being inadvertently transmitted when the user does not intend to conduct a financial transaction, thereby preventing unintended or fraudulent charges to the user’s payment cards and “increas[e/ing] security.” EX1016, 2:47-3:5; EX1003, ¶295. Furthermore, such protections are not overly burdensome and provide “ease of use” because the user only needs to make physical contact with the card to maintain the priming state. *Id.*

Both Phillips and Casey require PIN (passcode) entry to re-validate a user, which a POSITA would have recognized as adding an extra layer of security when combined with Power’s physical contact detection requirement. EX1005, [0035], [0038]-[0039], [0066]; EX1006, 9:9-36; EX1003, ¶299.

Deibert discloses that the Royyuru-Phillips-Casey-Deibert-Power combination provides the last three “disabling” steps of claim 13 for the reasons discussed in Ground 1C, *supra*. EX1003, ¶300.

F. Ground 1F: Royyuru in View of Phillips, Casey, and Carlson Render Claims 4, 21, and 22 Obvious

Claims [4], [21], and [22] are rendered obvious by the Royyuru-Phillips-Casey combination for the reasons discussed in Ground 1A, *supra*, Elements [4],

[21], [22]; EX1003, ¶¶164-168, 252-262. To the extent Royyuru-Phillips-Casey does not disclose that the device account number is of “limited time-duration” (claim 4), has an “expiration date” (claim 21), or of “limited-use” (claim 22), Carlson discloses these features.

Similar to Royyuru, Carlson describes a device for “conducting transactions using pseudo primary account identifiers.” EX1013, [0012], [0029]. The pseudo account identifier can be “similar in format to a consumer’s real account identifier” without revealing the true sequence of numbers or characters in the real account identifier. *Id.*, [0030]. The pseudo account identifier is generated by the payment processor and provided to the device for use in place of the primary account identifier. *Id.*, [0035], [0017]-[0018]. “[T]he pseudo primary account number may be set to expire after a certain number of transactions or after a certain time period” to avoid “illicit use.” EX1013, [0036], [0044], [0086]; EX1003, ¶303.

A POSITA would have been prompted to apply the teachings of Carlson to the Royyuru-Phillips-Casey combination such that the IKCV is “set to expire...after a certain time period.” EX1013, [0036]; EX1003, ¶304. Implementing the IKCV to “have a limited lifetime... provides a level of protection to the consumer's account” because it would likely “expire[] before any illicit use could be made.” EX1013, [0044]; EX1003, ¶304. Therefore, setting an expiration for the IKCV can prevent fraudulent use of the IKCV to generate DTCs and dynamic PANs by

unauthorized devices. EX1003, ¶304. A POSITA would have found it beneficial to apply such an expiration date/time limitation to other account and device related information in the combination to achieve similar benefits. *Id.*

Furthermore, a POSITA would have recognized that application of Carlson’s teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. EX1003, ¶305.

With respect to claims [4], [21], and [22], as discussed above, in the Royyuru-Phillips-Casey-Carlson system, the IKCV is “set to expire...after a certain time period” by the payment processor or issuer. EX1013, [0036], [0044], [0086]; EX1003, ¶307. The IKCV therefore has an expiration date of limited duration of validity and is therefore of limited time-duration of valid use. EX1003, ¶307. Furthermore, the DTC and dynamic PAN can be generated using both the IKCV and any “unpredictable number” including any “number...received by the presentation instrument .” EX1004, [0051], [0057], [0006]; EX1003, ¶307. Therefore, the DTC and dynamic PAN are generated by combining the IKCV of limited duration (based on Carlson) and the expiration date for the IKCV, as disclosed by Royyuru (claim [21]). EX1003, ¶307; EX1004, [0006]-[0007], [0057].

G. Ground 2A: Gomez in View of Amacker and Spodak Render Claims 1-9, 11-12, 15-20, and 22-23 Obvious

1. 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, 5:7-11, FIG. 7.

Gomez describes an EPIC card having a static payment card identifying number corresponding to the customer’s EPIC account, which is linked to multiple actual credit/debit cards. *Id.*, 2:19-39, 20:1-37.

The payment card transmits the static EPIC 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.

2. Amacker

Amacker discloses a “mobile wallet server” stored on a user’s personal device that allows a user to “control the distribution of personal/payment information...by selectively approving or rejecting requests.” EX1008, 2:13-57. “The person may respond to the request by interacting with the mobile wallet server...Upon a selection of ‘accept’ (or similar approval), the mobile wallet server may transmit the

requested information (e.g., personal/payment information, etc.) to the retailer to complete a pending process.” *Id.*

3. Spodak

Spodak discloses 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], [0027], [0034]. The universal card can use a dynamic magnetic stripe to communicate with a traditional credit card magnetic stripe reader, and a short range transceiver to communicate with a contactless payment terminal such as via NFC. *Id.*, [0033], [0035], [0088]-[0089].

4. Gomez-Amacker-Spodak Combination

A POSITA would have beneficially applied the teachings of Amacker and Spodak to modify Gomez’s mobile payment system to include multiple improvements. EX1003, ¶¶311-323.

First, a POSITA would have modified Gomez such that the EPIC payment card of Gomez is modified to include a larger touchscreen display and/or is integrated into a device having a touchscreen display, as taught by Amacker. EX1007, 5:48-57, 10:34-42; EX1008, 4:51-60, 2:13-25, 6:21-30; EX1003, ¶312. A POSITA would have recognized that including a larger touchscreen display would have allowed the device to display additional information regarding payment cards, details of the transaction, and transaction status on the device while allowing for

easier, intuitive user manipulation via the touchscreen, such as when selecting a payment card, thereby improving the user experience. EX1003, ¶312; EX1008, 5:1-17, FIG. 2.

Second, a POSITA would have modified Gomez based on Amacker to receive a payment request for a transaction and display payment options for conducting the transaction at the device. EX1008, 2:37-3:3, 3:42-57, 4:37-5:17; EX1003, ¶313. Gomez describes NFC communication with the merchant and Amacker beneficially discloses that such NFC communications can include a payment request. EX1007, 8:53-57, 7:49-54; EX1008, 3:27-57, 2:37-3:3, 4:37-5:17. As shown by Amacker, the request can include useful information about the transaction displayed on the device:

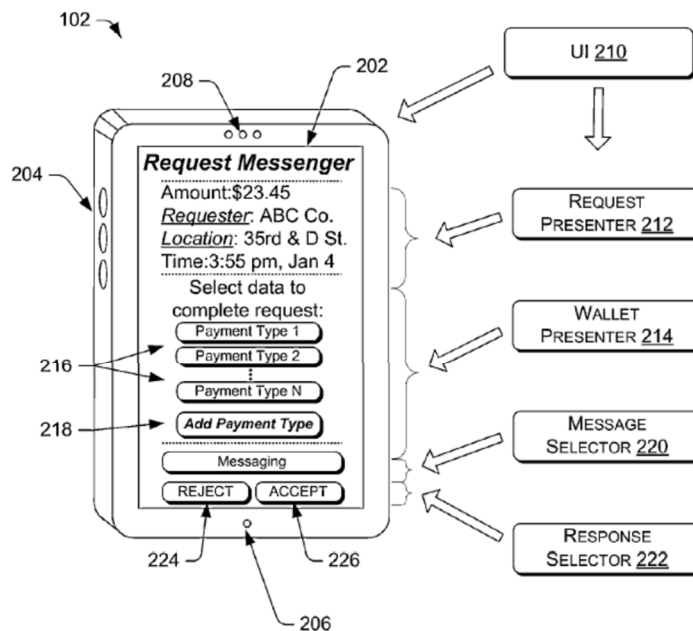


Fig. 2

EX1008, FIG. 2. This modification would have improved the system by allowing the user to better ensure that they are approving a payment transaction and transmitting payment information to a correct merchant terminal, which can prevent fraudulent transmittal of payment information to an incorrect terminal. EX1003, ¶314. Such a modification would also allow the user to visually review transaction data before approving (or denying) the transaction. *Id.*; EX1008, 3:27-57, 2:37-3:3, 4:37-5:41, 6:2-15. Requiring the user to authorize the transaction (as taught by Amacker) would have allowed the user to review transaction information (e.g., price, purchase items) prior to completing the transaction, allowed the user extra opportunity to change their mind regarding a transaction, and provide extra assurance that the user intends to initiate a payment transaction rather than having inadvertently opened a payment application. EX1003, ¶314.

Third, a POSITA would have modified Gomez based on Amacker and Spodak to display additional information when allowing a user to select a payment method. Gomez discloses that the user can “manually select the actual credit card that he/she wishes to use during a purchase transaction.” EX1007, 20:30-42, 21:5-20; EX1003, ¶315. Amacker provides additional details on how a user can use a touchscreen display to view additional information about payment methods before selecting. EX1003, ¶315; EX1008, 5:18-41, Cl. 1, FIG. 2. Spodak further discloses that its universal card includes a display for displaying payment information. EX1009,

[0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A. A POSITA would have recognized that including additional information (issuer name, processor and issuer logos, account number, etc.) in the card selection process would have allowed the user to more easily identify a desired card for a particular transaction. EX1003, ¶316.

Fourth, a POSITA would have modified Gomez based on Spodak to only display the last four digits of the account number. EX1009, [0068] (displaying account number), [0089] (displaying last four digits of an account number); EX1003, ¶317. A POSITA would have recognized that only displaying the last four digits of the payment number for each card would have allowed the user to more readily recognize and identify a desired payment method from among the multiple payment methods stored on the device while obscuring the full payment number to prevent fraud due to nearby third-parties observing the displayed payment numbers, thereby increasing user utility while increasing security. EX1003, ¶317.

Fifth, a POSITA would have modified Gomez based on the teachings of Amacker to generate the authentication cryptogram in response to receiving the request to ensure that the limited-duration cryptogram is valid for the intended transaction. EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; EX1003, ¶318. Such a modification would have saved processing resources by only utilizing the processor

to generate the authentication cryptogram when a valid payment request has been received. EX1003, ¶318.

Sixth, when Amacker's screen displays the payment request, a POSITA would have understood that it visually conveys that the status of the transaction is incomplete. EX1003, ¶319; EX1008, FIG. 2; *see also generally* EX1001 (specification does not define "status").

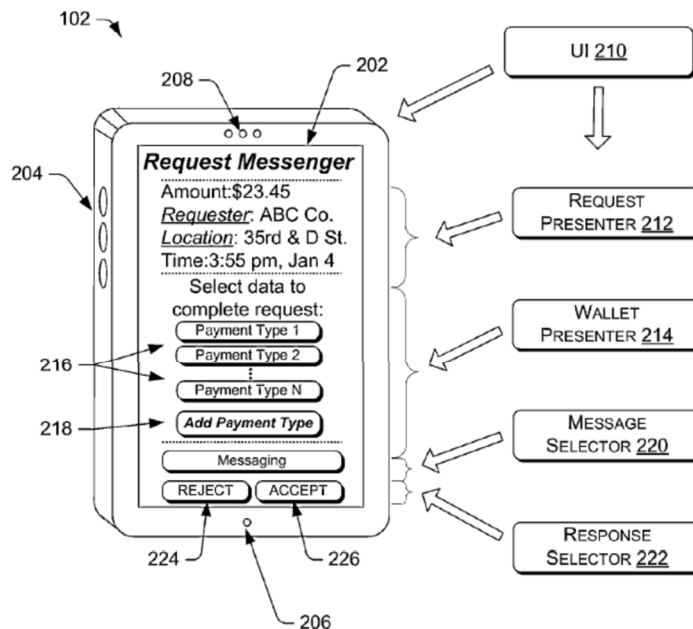


Fig. 2

EX1008, FIG. 2. As shown in FIG. 2, the user interface visually conveys to the user that the transaction is incomplete by displaying "request" in the heading, the name of the requester, payment types to "**complete**" the request, and the option to reject or accept the payment request. *Id.*; EX1003, ¶320. To the extent that this user interface does not explicitly display that the transaction is incomplete, Amacker's disclosure

would have motivated a POSITA to explicitly display that the status of the transaction is incomplete until the user selects a “payment type” and “accept.” EX1008, 6:3-15, 11:25-35, FIG. 2; EX1003, ¶320.

Finally, a POSITA would have recognized that applying the teachings of Amacker and Spodak to Gomez is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. EX1003, ¶¶321-322.

5. Claim 1

i) [1.pre]

To the extent the preamble is treated as a limitation, Gomez describes “purchase transaction approval at a retail merchant.” EX1007, 3:65-67, 5:65-6:4, 2:45-54. EX1003, ¶¶323-324.

ii) [1.a]

Gomez describes an input such as entry of “a fingerprint or PIN number, into the payment card” that corresponds to a priming operation of authorizing the payment card to perform the transaction. EX1007, 2:59-64, 5:13-18, 7:9-16, 9:12-33, 13:40-44; EX1003, ¶324. Gomez discloses performing the described functions using an “EPIC payment card.” EX1007, 11:19-38, 2:55-3:3, FIG. 9. In the combination, a POSITA would have also looked to Spodak for disclosure of an input

that a user pushes a button or taps or bends the universal card itself, which corresponds to a priming action of activating the universal card. EX1009, [0045], [0084]; *see also* EX1001, 11:34-42, 13:25-32 (the '579 patent's examples of priming); EX1003, ¶325.

iii) [1.b]

The device of the Gomez-Amacker-Spodak combination “includes a processor.” EX1007, 10:34-38, 2:59-64; EX1003, ¶326.

iv) [1.c]

Gomez discloses “a display” and “an activation input device” that are “coupled to” the processor. EX1007, 12:49-61; 10:34-38, FIG. 7. The display “may be a touch screen display.” EX1008, 4:51-60; EX1003, ¶327.

v) [1.d]

The Gomez-Amacker-Spodak device’s “processor ... may include more than one IC operating together,” such as “NFC circuits for implementing a near-field communications transceiver.” EX1007, 10:53-57, 7:49-54, 2:40-3:3; EX1003, ¶328.

vi) [1.e]

In the combination, Amacker discloses that the retailer can “transmit a request to the person’s mobile device” including requests for “payment information” for completing “in person” transactions. EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61;

EX1003, ¶329. The communication occurs via the NFC interface. EX1007, 10:53-57, 7:49-54; EX1008, 3:27-34.

vii) [1.f]

The Gomez-Amacker-Spodak device includes “a display and a selection capability” to allow the user “to manually select the actual credit card that he/she wishes to use during a purchase transaction.” EX1007, 20:30-59, 21:5-20, FIG. 9. In the combination, Amacker confirms that “when the MWS 102 receives a payment request, the wallet presenter 214 may present relevant payment options that may be used to respond to the payment request (e.g., payment card selections, etc.).” EX1008, 5:18-41, Cl. 1; EX1003, ¶¶330-331.

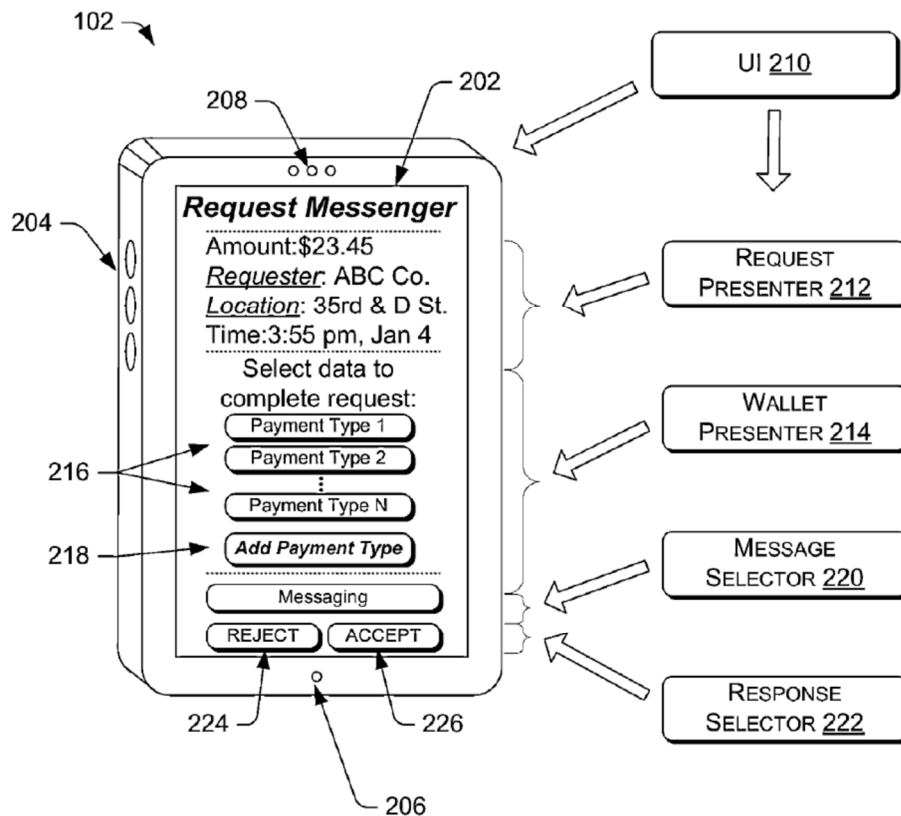


Fig. 2

EX1008, FIG. 2.

Spodak further discloses that its universal card includes a display for displaying payment information. EX1009, [0034], [0068] (displaying account number), [0069], [0074], [0076], [0079], [0089] (displaying last four digits of an account number), FIGs. 8A, 8B, 8D, 10A, 11A, 12A; EX1003, ¶332.

viii) [1.g]

Gomez discloses displaying a “card logo” for each card. EX1007, 20:43-59; *see also* EX1008, 5:18-41; *see also* EX1009, [0068] (displaying card issuer logo); EX1003, ¶¶332-333.

ix) [1.h]

Gomez discloses displaying additional iconography of the payment card such as “name (or nickname)” and “graphical information, such as logos and barcodes.” EX1007, 20:43-59; *see also* EX1009, [0068] (displaying card issuer logo); EX1003, ¶¶334-335.

x) [1.i]

Gomez describes “a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card” based on a seed value and temporal value “which expires within a short period of time thereafter.” EX1007, 1:58-2:4. The device generates an “authentication cryptogram for each attempted transaction only after the cardholder successfully presents a credential.” *Id.*, 5:13-18; *see also* 7:26-8:9; EX1003, ¶336.

As would have been recognized by a POSITA, the authentication cryptogram (the limited-use payment information) is used in place of the card issuer supplied payment information (the “actual credit card account number” disclosed by Gomez) in that the authentication cryptogram is combined with the static EPIC account

number to form limited-use payment information and provided to the merchant rather than the issuer supplied payment information. EX1007, 1:55-2:39, 5:19-24, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3; EX1003, ¶337.

xi) [1.j]

Gomez discloses “communicating a payment card identifying number to a payment processing system, and communicating the authentication cryptogram in a payment card account name field to the payment processing system” “using near field communication (NFC).” EX1007, 2:50-54, 7:49-54, 8:16-23. As discussed above, in some embodiments, the “payment card identifying number” is “an EPIC account which is not itself a live payment card account, but to which are linked one or more live payment card accounts” and therefore is not an issuer supplied payment information. *Id.*, 5:19-24, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3; 1:55-2:39; EX1003, ¶338.

xii) [1.k]

Gomez describes that “a great variety of useful information may be displayed, including...secure messages, alarms, and other notifications.” EX1007, 12:58-67, 10:18-26, 11:53-62. Having looked to Gomez, a POSITA would have applied the teachings of Amacker, which, as discussed above, visually conveys that the status of the transaction is incomplete. EX1003, ¶¶340-341; EX1008, FIG. 2.

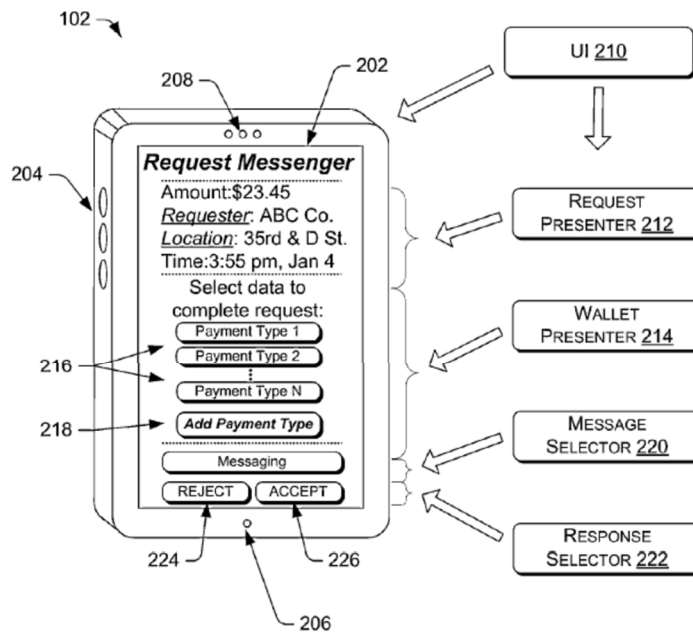


Fig. 2

EX1008, FIG. 2. To the extent that the user interface does not explicitly display that the transaction is incomplete, a POSITA would have modified Gomez based on Amacker to explicitly display that the status of the transaction is incomplete until the user selects a “payment type” and “accept.” EX1008, 6:3-15, 11:25-35, FIG. 2; EX1003, ¶342.

6. Claim 2

Gomez’s “authentication cryptogram” is generated using a seed value and a temporal signal value such as “the date/time of the transaction” or “the sequence value (or sequential number) of the attempted use.” EX1007, 1:58-2:4, 5:25-32, 6:27-33, 7:17-48, 10:66-11:6. The “seed value is unique for each payment card, []

corresponds to the payment card identifying number,” and “may include certain non-random customer specific information, such as a unique customer key.” *Id.*, 7:17-48; EX1003, ¶345.

7. Claim 3

Gomez’s “authentication cryptogram” is dynamically generated on the device by combining “a seed value” and “a temporal signal” such as “the sequence value (or sequential number) of the attempted use.” EX1007, 1:58-2:4, 7:41-43, 21:37-48, 7:17-26, 8:36-41, 10:58-11:6, FIG. 7; EX1003, ¶348. The “seed value is unique for each payment card” and can include “unique customer key” and therefore provides the claimed device account number, device identifier, device secrets, device key, and payment issuer key. *Id.*, 7:17-48, 12:30-34, 16:31-34, 16:64-17:13; EX1003, ¶348. Alternatively, Gomez discloses that the temporal value can be a sequence counter or time and it would have been obvious to a POSITA to use both a sequence counter and time when generating the cryptogram to increase the security of the cryptogram by incorporating multiple temporal values. EX1007, 5:25-32, 6:27-33, 7:17-48, 10:66-11:6; EX1003, ¶348.

The authentication cryptogram is provided in place of “the 3-digit security code” provided by the issuer to validate the transaction. EX1007, 9:65-10:17, 2:4-12, 14:37-63, 6:23-38; EX1003, ¶349. The cryptogram “is generated uniquely for each attempted use of the payment card” and good for a single transaction. EX1007,

1:58-2:1, 21:37-48; 5:15-16, 8:36-39, 14:3-4; EX1008, 4:26-30, 8:28-33, 11:38-51; EX1003, ¶350. The sequential counter used to generate the cryptogram is “increment[ed] for each attempted use” such that each cryptogram is unique for each attempted use. EX1007, 8:36-39.

To the extent Gomez does not render obvious generating a cryptogram number separately from generating payment information in claim 1, this would have been obvious in view of Spodak. Similar to Gomez, Spodak discloses 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], [0027], [0033]-[0035], [0088]-[0089]; EX1003, ¶352. To emulate the magnetic stripe and “authenticate the transaction with the card issuer,” the universal card generates a “dynamic authentication value,” which discloses the claimed “cryptogram number.” *Id.*, [0094]. Spodak discloses that “the universal card may generate a dynamic authentication value and write the dynamic authentication value in the field typically used for the static CVV value,” *id.*, which discloses that this value is generated “for use by the electronic device in place of a card validation value originated from the card issuer” as claimed. EX1003, ¶353. The dynamic authentication value is generated based on “a random number” and “a transaction counter.” EX1009, [0094]. Because the “dynamic authentication value is unique

for every transaction,” *id.*, generating the dynamic authentication value “results in a one-time limited-use number” as claimed. EX1003, ¶353.

To the extent that Gomez does not disclose generating a cryptogram separately from the limited-use payment information generated in claim 1, a POSITA would have been motivated to combine Spodak’s dynamic authentication value and Gomez’s encryption techniques in the Gomez-Amacker-Spodak combination to generate the claimed cryptogram number to improve the security and compatibility of the device with existing POS equipment that use magnetic stripes. EX1009, [0088]-[0089], [0094]; EX1008, 4:26-30, 8:28-33, 11:38-51; EX1007, 1:58-2:4, 2:42-44, 5:15-16, 5:50-51, 7:17-26, 7:41-43, 8:36-41, 10:58-11:6, 21:37-48; EX1003, ¶354-356. A POSITA would have further been motivated to increment Spodak’s transaction counter by virtue of it being a counter, and because both Gomez’s authentication cryptogram and Spodak’s dynamic authentication value are generated based on counters and numbers. EX1007, 7:17-48, 12:30-34, 16:31-34, 16:64-17:13; EX1009, [0094]; EX1003, ¶357.

A skilled person would have reasonable expectation of success in making the above-described combination of known prior art technologies (e.g., known devices for conducting transactions via both a magnetic stripe reader and a contactless payment terminal) according to known methods (e.g., known process for securing payment information during the transactions) to yield the predictable result of a

device that could securely conduct transactions with both a magnetic stripe reader and a contactless terminal. EX1003, ¶358; *see KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007).

8. Claim 4

The device account number is disclosed by Gomez’s seed value, which “is unique for each payment card, and corresponds to the payment card identifying number” that can be the 16-digit card number that a POSITA would understand is provided by a card issuing authority. EX1007, 1:44-47, 7:17-48, 12:30-34, 13:45-14:2, 16:31-34, 16:64-17:13; EX1003, ¶361. The “authentication cryptogram” is generated based on the “seed value” and the “cryptographic hash” (one-time limited-use cryptogram number). EX1007, 8:3-9:11. The seed value “corresponds to the payment card identifying number,” and therefore the expiration date for the payment card number is the expiration date for the seed value, giving the seed value a limited time-duration of valid use. EX1007, 3:67-4:4, 5:50-57, 11:23-27, 7:17-48; EX1003, ¶361. Alternatively, it would have been obvious to a POSITA to make the seed value of a limited time-duration of valid use tied to the payment account expiration date so that a seed value generated using an expired account number could not be used for transactions. EX1003, ¶361.

Gomez’s device combines the “payment card identifying number” and the “authentication cryptogram” to form complete payment information that is

transmitted to the payment processing system to perform a payment transaction. EX1007, 2:50-3:3, 5:48-60, 6:23-38, 7:57-65, 8:16-23. The payment card identifying number can be “an EPIC account number” “which is not itself a live payment card account, but to which are linked one or more live payment card accounts.” EX1007, 6:7-22, 5:19-24. Therefore, the combined payment information is conveyed in place of card issuer information during a payment transaction. EX1003, ¶362.

9. Claim 5

The Gomez-Amacker-Spodak combination renders obvious “generating a limited-use security number” and the remaining features of the generating step of Claim [5] for the reasons discussed, *supra*, Element [3]; EX1003, ¶365. Gomez expressly discloses that “the generated authentication cryptogram may be displayed.” EX1007, 12:64-13:4, 13:22-33, 21:5-20. Spodak further discloses that its universal card includes a display for displaying payment information. EX1009, [0034], [0068], [0069], [0074], [0076], [0079], [0089], FIGs. 8A, 8B, 8D, 10A, 11A, 12A. Having appreciated that Gomez displays the cryptogram and Spodak displays the payment information, a POSITA would have looked to the Gomez-Amacker-Spodak combination for the displaying step of Claim 5. EX1003, ¶366.

10. Claim 6

An account authentication request including “the EPIC account number, the date and time of the transaction, and the authentication cryptogram” is sent to an authentication server. EX1007, 6:12-38, 14:21-27, 17:40-62. The authentication server “independently generat[es] a ‘reference’ authentication cryptogram based upon the seed value corresponding to the EPIC account number, and based upon the *date/time of the transaction* (or other temporal signal value, as described below).” *Id.* As discussed above (*supra*, Claims [2]-[4]), the “other temporal signal values” include a transaction sequence counter and the seed value provides at least a device account number, user account information, issuer secrets, issuer keys, and issuer-provided device keys. EX1007, 7:17-48, 8:36-41, 10:58-11:6, 12:30-34, 16:31-34, 16:64-17:13; EX1003, ¶368. The authentication cryptogram is provided in place of the card issuer card security code. *See supra*, Claims [3]-[4]; EX1007, 9:65-10:17, 2:4-12, 14:37-63; EX1003, ¶368.

The payment processor/authentication server authorizes the transaction “[i]f the server-calculated reference authentication cryptogram matches the received authentication cryptogram.” EX1007, 6:23-64, 17:23-28, 18:20-25. The transaction is rejected if a previously used authentication cryptogram is reused or has expired. EX1007, 5:34-47, 21:37-48; EX1003, ¶369.

11. Claim 7

Supra, Elements [1.a], [1.c].

12. Claim 8

Gomez describes priming: “the cardholder successfully presents a credential, such as a fingerprint or PIN number, into the payment card.” EX1007, 5:13-18, 13:40-44; EX1003, ¶375.

13. Claim 9

In the combination, Amacker provides a touchscreen display of “a requester's identity/location, a time of the request, an amount (if applicable) and/or other relevant information” (Element [9.b]). EX1008, 5:1-17; EX1003, ¶¶378-379.

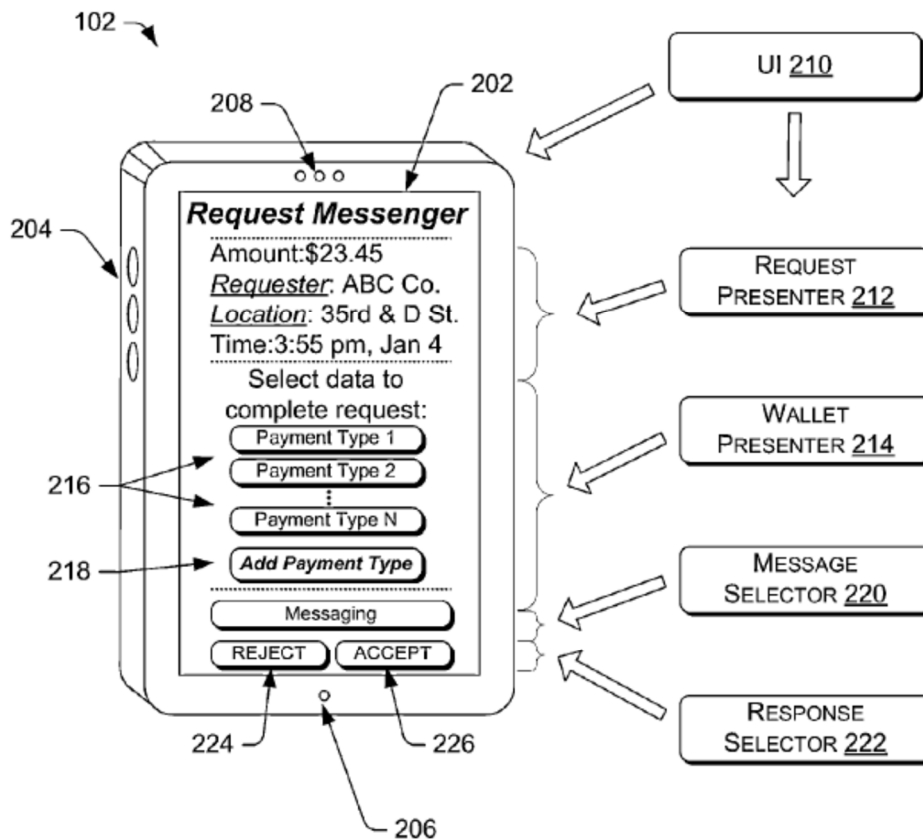


Fig. 2

EX1008, FIG. 2. As shown in FIG. 2, the display includes “a reject option 224 and an accept option 226” and a plurality of selectable payment options (Elements [9.a] and [9.c]). *Id.*, 6:2-15, 5:18-41; 4:40-46; EX1007, 20:30-21:20; EX1003, ¶¶378-380; *supra*, Element [1.f].

14. Claim 11

The combined device allows for “selectively approving or rejecting requests for personal information using the mobile wallet server” after a transaction timeout period or an exceeded transaction amount. EX1008, 2:32-49, 6:2-15, 12:34-46,

12:47-57 (time range for handling transactions), 12:58-67 (transaction restrictions based on fund availability and request limit), 13:1-6, FIG. 2; EX1003, ¶383.

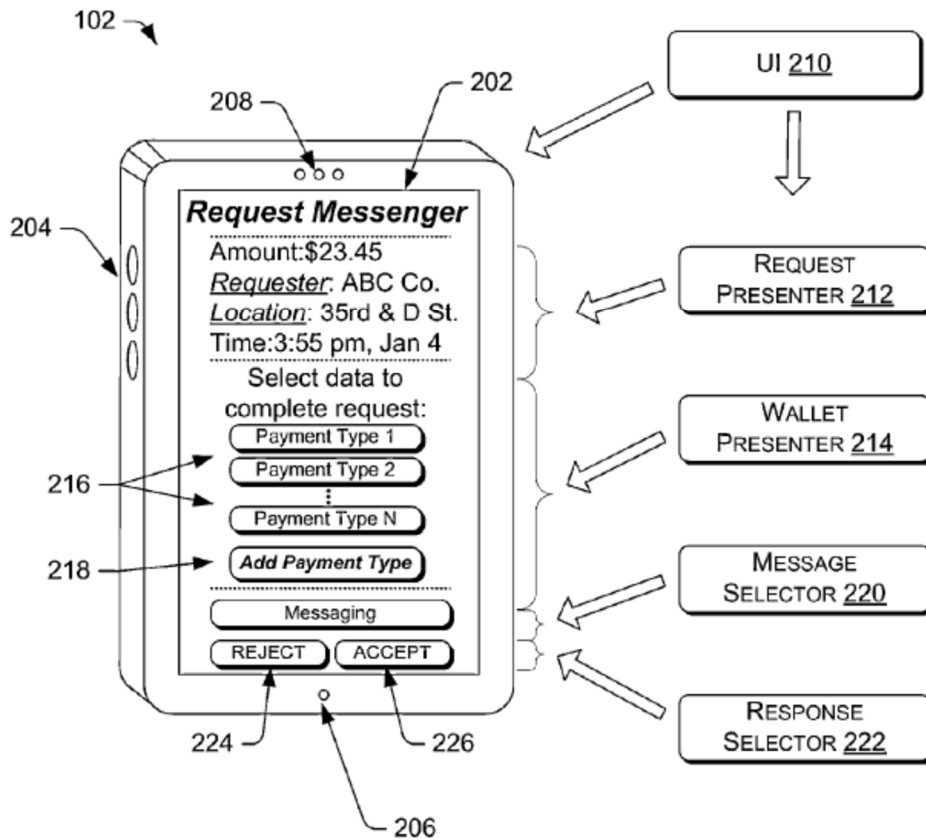


Fig. 2

EX1008, FIG. 2

15. Claim 12

Gomez discloses the claimed “priming operation” because “after entering a customer-established PIN authorization code, a customer may then view all credit cards in their EPIC account by their description name (or nickname) and card logo, and select the card they wish to use.” EX1007, 20:43-21:20, 20:12-23. If the user

does not select a payment option, “the EPIC card defaults to the pre-established credit card account selection order.” *Id.*; EX1003, ¶386.

16. Claim 15

i) [15.pre]

Supra, Preamble [1.pre]; EX1003, ¶389.

ii) [15.a]

Supra, Elements [1a], [1d], [1.e]; EX1003, ¶¶390-391.

iii) [15.b]

Supra, Elements [1.c], [1.f], [9.b]; EX1003, ¶¶392-393.

iv) [15.c]

Supra, Elements [1.f], [9], [11]-[12]; EX1003, ¶¶394-395.

v) [15.d]

Supra, Element [1.i]; EX1003, ¶¶396-397.

vi) [15.e]

Supra, Element [1.j]; EX1003, ¶¶398-399.

vii) [15.f]

Supra, Element [9]; EX1003, ¶¶400-401.

viii) [15.g]

Supra, Elements [1.g]-[1.h], [9.b]; EX1003, ¶¶402-403.

ix) [15.h]

Supra, Elements [9a], [9c], [11]; EX1003, ¶¶404-406.

17. Claim 16

The device has a touchscreen. *Supra*, Ground 2A, [1.c]; EX1008, 4:51-60. The confirmation screen includes a requester identity, amount, and accept/reject options. EX1008, 5:1-17, 6:2-15; EX1003, ¶408.

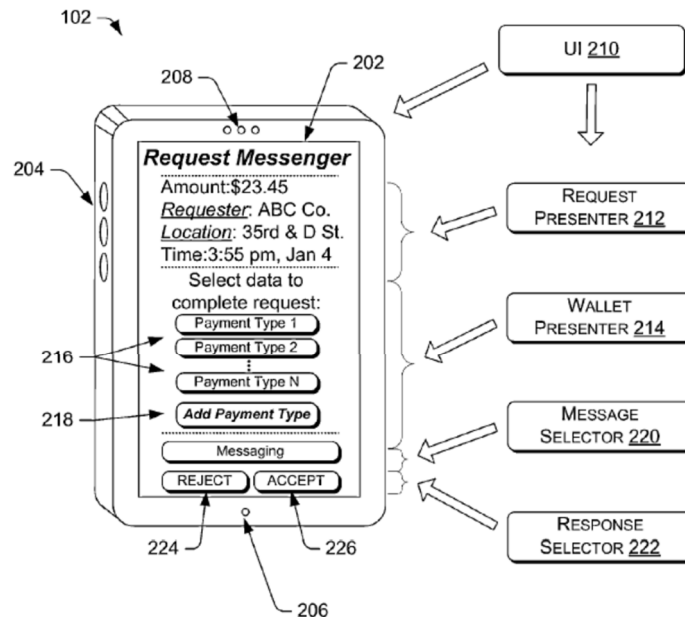


Fig. 2

18. Claim 17

Supra, Elements [1.f]-[1.h], [9.c], [11]-[12]; EX1003, ¶410.

19. Claim 18

Supra, Elements [1.a], [8]; EX1003, ¶412 .

20. Claim 19

i) [19.pre]-[19.b]

The device includes a processor coupled to memory and can be implemented as a mobile device. EX1007, 10:34-38, 11:19-38, 2:55-3:3, FIG. 9; EX1008, 2:13-25; EX1009, [0027], [0028], [0059], [0086], [0111]; EX1003, ¶¶415-416.

ii) [19.c]

Supra, Element [1.c]; EX1003, ¶416.

iii) [19.d]

Gomez discloses “an activation input device” including “a fingerprint reader.” EX1007, 10:34-38, 11:14-31, 2:55-59; EX1008, 4:51-60, 5:42-49, 8:49-53; EX1007, 13:22-33; EX1003, ¶¶418-419.

iv) [19.e]

Supra, Elements [1.d]-[1.e]; EX1003, ¶420.

v) [19.f]

The device includes a processor that executes instructions to perform the described functions. EX1007, 2:59-64; EX1008, 6:21-30; EX1003, ¶421.

vi) [19.g]

Supra, Elements [1.a], [7]-[8]; EX1003, ¶422.

vii) [19.h]

The device generates the cryptogram “upon verification of a valid credential,” which is a priming action that authorizes the payment card to perform a transaction.

EX1007, 2:59-64, 5:13-18, 7:17-20;*see also* EX1001, 11:34-42, 13:25-32. At this point, “the card is considered ready to communicate with the payment processing system.” EX1007, 8:11-15, 9:30-41, 11:53-62; EX1008, 2:32-57, 6:2-15; EX1003, ¶423.

viii) [19.i]

Supra, Elements [1.f]-[1.h]; EX1003, ¶424.

ix) [19.j]

Supra, Elements [1.f], [9.a], [9.c], [11]-[12]; EX1003, ¶425.

x) [19.k]

In the combination, Gomez discloses generating a limited-use payment information for use in place of card issuer payment information in the form of the authentication cryptogram. *Supra*, Element [1.e] and [1.i]; EX1007, 1:58-2:4, 5:13-24, 7:26-8:9, 1:55-2:39, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3; EX1003, ¶426. Amacker discloses that the authentication cryptogram is generated in response to receiving the NFC transaction payment request. EX1003, ¶427; EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; *supra*, [1.e]. The device “generate[s] the limited use number following the ‘yes’ route” of the user accepting the request. *Id.*, 12:9-17, 10:66-11:64; EX1003, ¶427. In another example, the limited use number is generated and provided to the merchant “[u]pon a selection of ‘accept’” in response to the payment request. EX1008, 2:46-49.

xi) [19.l]

Supra, Element [1.j]; EX1003, ¶428.

xii) [19.m]

Supra, Element [1.k]; EX1003, ¶429.

21. Claim 20

Supra, Elements [1.a], [1.c], [7], [8], [12]. A valid PIN entry provides a correct passcode entry sequence and a correct user response input from a security challenge. EX1003, ¶432; EX1007, 2:59-64, 5:13-18, 7:9-16, 20:43-21:20, 20:12-23, 11: 15-38 (“fingerprint reader”).

22. Claim 22

Supra Claim [4]. Gomez discloses a memory coupled to the processor. EX1007, 10:34-38. Gomez’s seed value (stored on the device), used to generate the authentication cryptogram, “is unique for each payment card, and corresponds to the payment card identifying number,” which can be the 16-digit number that a POSITA would understand is a device account number of limited-use (i.e., limited in use to the specific card). EX1007, 1:44-47, 7:17-48, *see also id.*, 12:30-34, 13:45-14:2, 16:31-34, 16:64-17:13, 5:25-28; EX1003, ¶435. The seed value includes “a unique customer key.” EX1007, 7:31-41, 14:30-36, 9:23-29. In the combination, the limited use number is provided by the issuer because Gomez discloses a number issued by a card issuer and Amacker discloses a data provider that may be a financial

institution that generates the limited use number. EX1007, 1:44-47; EX1008, 4:21-23, 11:58-12:8; EX1003, ¶435. Having the issuer provide the seed value would beneficially improve the system by ensuring that the seed value is known to the issuer (and payment processor) for purposes of verifying the authentication cryptogram. EX1003, ¶435.

A POSITA would have recognized that, because the seed value “corresponds to the payment card identifying number,” the expiration date for the payment card number is also the expiration date for the seed value. EX1007, 3:67-4:4, 5:50-57, 11:23-27, 7:17-48; EX1003, ¶436. Alternatively, it would have been obvious to a POSITA to make the seed value of a limited time-duration of valid use tied to the payment account expiration date so that a seed value generated using an expired account number could not be used for transactions. EX1003, ¶436.

23. Claim 23

Supra, Elements [1.j], [2]-[3]; EX1003, ¶439.

H. Ground 2B: Gomez in View of Amacker, Spodak, and Deibert Render Claims 10 and 14 Obvious

A POSITA would have applied the teachings of Deibert to the Gomez-Amacker-Spodak combination in the same manner, for the same reasons, and to achieve the same benefits discussed in Ground 1D, *supra*, and would have had a reasonable expectation of success. EX1003, ¶¶442-444.

1. Claim 10

The Gomez-Amacker-Spodak-Deibert combination renders obvious Claim [10] based on Deibert's disclosure for the same reasons discussed in Ground 1D, *supra*. EX1003, ¶¶446-447; *see also supra* Ground 2A, Elements [1.d]-[1.e] (transactions conducted using NFC).

2. Claim 14

Gomez discloses requiring a PIN (a passcode) to access the payment application/functionality prior to selecting a specific payment method. *Supra* Ground 2A, Claim [12]; EX1007, 20:43-21:20, 20:12-23. A POSITA would have recognized that user selection of a payment method provides a priming operation after entry of the PIN/passcode. EX1003, ¶450. Deibert's disclosure renders obvious the additional recitations of Claim [14] for the same reasons discussed in Ground 1C, *supra*. EX1003, ¶¶451-452.

I. Ground 2C: Gomez in View of Amacker, Spodak, Deibert, and Power Render Claim 13 Obvious

1. Claim 13

A POSITA would have applied the teachings of Power to Gomez-Amacker-Spodak-Deibert in the same manner and for the same reasons as discussed with respect to the Royyuru-Phillips-Casey-Deibert-Power combination. *Supra*, Ground 1E; EX1003, ¶¶455-458. Spodak further discloses that, to activate the universal card, a user pushes a button or taps or bends the universal card itself. EX1009,

[0045], [0084]; EX1003, ¶459; EX1001, 9:64-10:3, 17:19-23. Furthermore, Gomez discloses requiring PIN (passcode) entry to re-validate a user. EX1007, 20:43-21:20, 20:12-23; EX1003, ¶459.

Disclosure from Deibert and Power renders obvious all remaining elements of claim 13 for the reasons discussed in Grounds 1D-1E, 2B, *supra*. EX1003, ¶¶460-462.

J. Ground 2D: Gomez in View of Amacker, Spodak, and Carlson Render Claims 4 and 22 Obvious

Claims [4] and [22] are rendered obvious by the Gomez-Amacker-Spodak combination for the reasons discussed in Ground 2A, *supra*, Elements [4] and [22]. To the extent Royyuru-Phillips-Casey do not disclose that the device account number is of “limited time-duration” (claim 4) or of “limited-use” (claim 22), Carlson discloses these features.

A POSITA would have been prompted to apply the teachings of Carlson to the Gomez-Amacker-Spodak combination such that Gomez’s seed value is “set to expire...after a certain time period” by the payment processor or issuer to provide “protection to the consumer’s account” by limiting the amount of possible damage should the seed value be stolen. EX1013, [0036], [0044]; EX1003, ¶¶465-466, 469, 472. The seed value therefore has an expiration date of limited duration of validity and is therefore of limited time-duration of valid use. EX1003, ¶¶469, 472.

Furthermore, a POSITA would have recognized that application of Carlson's teachings to the Gomez-Amacker-Spodak system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. EX1003, ¶467.

K. Ground 2E: Gomez in View of Amacker, Spodak, Carlson, and Royyuru Render Claim 21 Obvious

Claim [21] is rendered obvious by the Gomez-Amacker-Spodak combination for the reasons discussed in Ground 2A, *supra*, Elements [4] and [22]. To the extent Royyuru-Phillips-Casey do not disclose that the device account number has an "expiration date," (claim 21), Carlson and Royyuru disclose this feature.

A POSITA would have been prompted to apply the teachings of Royyuru and Carlson to Gomez-Amacker-Spodak to use additional values when generating the authentication cryptogram including one or more unpredictable/undeterminable and one or more expiration dates. EX1004, [0057], [0051]; EX1003, ¶475. A POSITA would have recognized that using these additional values when generating Gomez's authentication cryptogram would have increased security because the cryptogram would be based on additional values that would be difficult for third parties to determine or intercept. EX1003, ¶475; EX1004, [0004].

It would have been beneficial to combine the seed value with the expiration date for the seed value when generating the authentication cryptogram to increase

the difficulty for third parties to replicate it. EX1003, ¶476, 478. Carlson teaches that in the combination the seed value is “set to expire...after a certain time period.” EX1013, [0036], [0044], [0086]; EX1003, ¶476, 478; *supra* Ground 2D. Royyuru discloses that values similar to the seed value (Royyuru’s IKCV) can be combined with their respective expiration dates or other unpredictable/undeterminable numbers known to the device (which would include the expiration for the seed value) to increase security. EX1004, [0057], [0051]. For example, Royyuru’s DTC, which is highly similar to Gomez’s authentication cryptogram, is generated using values including “expiration date” and the IKCV. EX1004, [0057], [0005]-[0006]; EX1003, ¶476, 478. A POSITA therefore would have similarly combined the seed value and its respective expiration date when generating the authentication cryptogram.

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 1-23 of the ’579 patent based on the grounds specified in this petition.

Petition for *Inter Partes* Review
Patent No. 10,810,579

Respectfully submitted,

Dated: July 24, 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. 10,810,579 contains, as measured by the word-processing system used to prepare this paper, 13,989 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: July 24, 2025

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

CERTIFICATE OF SERVICE

I hereby certify that on July 24, 2025, I caused a true and correct copy of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 10,810,579 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)

[1.pre]	A method of performing a transaction, the method comprising:
[1.a]	receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user and wherein the electronic device comprises:
[1.b]	a processor;
[1.c]	a touch screen display coupled to the processor; and
[1.d]	a near field communications (NFC) interface coupled to the processor;
[1.e]	receiving a request for a transaction payment at said electronic device via the NFC interface;
[1.f]	displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card;
[1.g]	a card logo; and
[1.h]	other iconography of the payment card;
[1.i]	generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information;
[1.j]	transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and
[1.k]	visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.
[2]	The method of claim 1, wherein the generating the limited-use payment information utilizes at least one information from a set of information comprising: a device transaction sequence counter; a device account number; device secret keys; card issuer keys; merchant information; NFC recipient information; payment reader information; a time; a timestamp; an amount; a location; an online location; transaction information; payment information; device information; user information; an email address; and a user identification entry.

[3]	The method of claim 1, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the card issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count and at least one information of a set of information comprising: a device account number; device identifiers; device secrets; device keys; payment issuer secrets; payment issuer keys; user information; a time; and transaction information; and wherein further, said dynamically generating the cryptogram number results in a one-time limited-use number via the device incrementing said device transaction sequence counter count on a transaction.
[4]	The method of claim 1, wherein a limited-use number comprises a device account number, and wherein the device account number is of a limited time-duration of valid use, and wherein further a card issuing authority provides said device account number for use only by the electronic device, in place of card issuer information in performing payment transactions by the electronic device, and further comprising: performing payment transactions by the electronic device including the limited-use number; combining the limited-use number and said device account number within a device generated payment information; and conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions.
[5]	The method of claim 1, further comprising: generating a limited-use security number for use in place of a card issuer card security code by cryptographically combining information from at least one of a set of information comprising: user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; transaction information; and displaying the limited-use security number on the user-interface of the display.

[6]	The method of claim 1, wherein a payment processing authority verifies a limited-use number based on at least one information of the set of information comprising: a transaction sequence count information; a device account number; user account information; issuer secrets; issuer keys; issuer-provided device keys; transaction information; and a time of use, and further comprising: authorizing said transaction, by the payment processing authority, responsive to verifying a valid limited-use number appearing in place of card issuer information; and rejecting a limited-use number, by the payment processing authority, on at least one unverifiable condition, of a set of unverifiable conditions comprising: an invalid number generation; an invalid device account number; a use outside of a valid time window; an invalid re-use of a limited-use number; and an invalid use of an expired limited-duration number.
[7]	The method of claim 1, wherein the receiving an input at an electronic device comprises receiving an input via a user interface from one of the set of user interfaces comprising: a device button; a device touch-screen interface; a device touch ID button interface; a device optical sensor array; a device skin touch sensor; a skin-contact sensor; a device motion detection interface; a device biometric sensor interface; and a device user-interface selection.
[8]	The method of claim 1, wherein the priming operation comprises one operation of the set of operations comprising: a button press; a touch ID button press; a button double-press; a touch ID sensor touch; a touch-screen touch; a touch-input sequence; a gesture or swipe over a sensor-array; a skin-contact sense; an optical-sensor array sense; an electronic device tap; a sequence of motions of the electronic device; a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation; and, further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a touching from an identified valid user; a user entry of a valid passcode; a user entry of a valid PIN; swiping of a recognized user skin over a device sensor array; a correct user swiping or gesturing on the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motioning of the electronic device; a skin-contact sensing of an identified user; a device biometric sensing of a valid user identity; and a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user.

Petition for *Inter Partes* Review
Patent No. 10,810,579

[9.a]	The method of claim 1, further comprising: obtaining, by the electronic device, a user payment approval, through at least one device user interface of a set of interfaces comprising: a device display interface; a device touch-screen display interface; a device touch interface; device input buttons; device key-pad inputs, a device optical sensor array; a device motion detection unit; a device accelerometer; a device biometric user-sensor; and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user; and
[9.b]	displaying, on the display, at least one information of a set of information comprising: a priming status of the electronic device for payment; a default payment method; a plurality of selectable payment accounts; a payment request; transaction information; a payment amount; a merchant identification; a time; an expiration date; a location; an account balance; a payment bank logo; a card image; a payment card issuer icon; a payment card network icon; the last 4-digits of the primary account number; the last 4-digits of the device account number; and other payment iconography; and
[9.c]	receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.
[10]	The method of claim 1, further comprising: activating an NFC communication for a limited duration of time responsive to the electronic device priming; and responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction.

[11]	The method of claim 1, further comprising completing the transaction on the electronic device, wherein the completing further comprises: receiving an authorization input on the electronic device from a valid device user, in response to at least one of a set of exceptional conditions comprising: the electronic device leaving the proximity of the NFC recipient; the incomplete identifying of a valid device user; the electronic device leaving the user's possession; the electronic device leaving the proximity contact of the user; the electronic device leaving the grasp of the user; a biometric sensing the electronic device leaving the possession of a user since a last user validation; the transaction exceeding a pre-set amount limit; the transaction interval exceeding a pre-set time duration; a card issuing authority requesting a security check; and presenting the user with at least one of a set of selectable options comprising: requesting a transaction payment; continuing with the default payment method; selecting an alternate payment account; inputting an approval authorization; inputting a transaction denial; and inputting an adjustment of the transaction payment.
[12]	The method of claim 1, further comprising: subsequent to the priming operation, offering a user selection of payment options for user input selection by presenting a selection of payment options in graphical format on said touch-screen display, including at least one of: a last four digits of a payment account number portion; a last four digits of a device account number portion; an expiration date; a card issuer icon; a bank logo; a card processing network logo; a card image; a card payment network icon; graphical images associated with the payment account; accepting a user input selection of a payment option, from said payment options, via said touch-screen display; and proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options.

[13]	A method of claim 1, wherein the priming operation comprises: a button double press; and a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation; and further comprising: denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user, until after successfully re-validating a user; and wherein re-validating a user requires a correct user passcode re-entry; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.
[14]	A method of claim 1, wherein the priming operation is input after at least one of: a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device, and validating a user passcode entry on the touch-screen display of the electronic device; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.
[15.pre]	A method of performing a transaction, the method comprising:
[15.a]	receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient proximity communication request to an NFC interface of the electronic device;
[15.b]	displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device;
[15.c]	receiving, from a valid device user, a payment selection and approval authorization input on the electronic device;
[15.d]	generating a limited-use number at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and
[15.e]	transmitting said limited-use number from said electronic device to a transaction recipient via the NFC interface;

[15.f]	obtaining a user payment approval through at least one user-interface of the electronic device, of a set of user-interfaces comprising: a touch-screen interface of the touch-screen display user-interface; a touch ID button; input buttons; a touch key-pad; an optical sensor array; a sensor array operable to recognize a swiping of a recognized user skin over the sensor array; a motion detection unit; an accelerometer; a biometric user-sensor; a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user while the electronic device is coming within proximity contact of an NFC recipient;
[15.g]	displaying on said display at least one of a set of information comprising: transaction information; merchant information; a time; a location of the transaction; a payment bank logo; a card issuer icon; a payment card image; an amount; and
[15.h]	receiving a user input providing for at least one transaction action, from a set of actions comprising: approving a transaction; denying a transaction; and adjusting a transaction.
[16]	The method of claim 15, further comprising: visually conveying on the touch-screen display user-interface, information regarding the transaction, including at least one of: a payment amount requested; an indication requesting an authorization input; an indication of an authorization success; an indication of an authorization failure; an option to retry a transaction; an option to retry a user authorization; an option to retry validating a user identity; an indication of a payment successfully completed; an indication of a payment failure; and an indication of a payment retry option.
[17]	The method of claim 15, further comprising: visually presenting on the touch-screen display user-interface, a plurality of payment options, including at least one of a set of payment method information for each payment option, the set comprising: a card image; a payment issuer logo; partial payment account numbers; a card payment network icon; a graphical image-encoding of a users payment account information; an amount of currency; an account balance; a credit limit; an amount of remaining credit; an amount of cryptocurrency; a cryptocurrency server network; and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface.

[18]	The method of claim 15, further comprising: receiving a priming operation at the electronic device for priming the electronic device for imminent payment, wherein the priming operation causes the electronic device to successfully identify the user through completing at least one user-validation, of a set of user validations comprising: a touching of the device by an identified user; a user entry of a valid passcode; a user entry of a valid PIN; a swiping of a recognized user skin over a sensor array of the electronic device; a correct user swiping or gesturing on a touch sensor array of the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motions of the electronic device; a skin-contact sense of a valid user; and a device biometric recognition of a valid user.
[19.pre]	An electronic device comprising:
[19.a]	at least one processor;
[19.b]	a memory coupled to the at least one processor;
[19.c]	a display operable to present a visual user-interface comprising device inputs; display output;
[19.d]	a device input;
[19.e]	an NFC interface operable to receive a transaction request when in proximity to an NFC recipient;
[19.f]	wherein the processor is operable to execute a program to implement a method comprising:
[19.g]	accepting a priming action of the electronic device by an identified device user, from the device input;
[19.h]	enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user;
[19.i]	displaying a summary of selectable payment account options on the display;
[19.j]	receiving a payment selection and approval authorization from a valid device user via the device input; and
[19.k]	responsive to receiving an NFC transaction payment request, generating a limited-use payment information for use in place of card issuer payment information,
[19.l]	wherein the NFC interface is operable to transmit said payment information from said electronic device to the NFC recipient of the transaction; and

[19.m]	wherein further the processor is operable to cause the display to visually convey a status of the transaction.
[20]	The electronic device of claim 19, wherein the method further comprises: receiving the priming action of a valid user via the device input, wherein the device input comprises at least one of a set of device inputs comprising: a button; a touch ID button; a touch sensor array; a touch keypad; a motion detection unit; an accelerometer; an optical sensor array; and identifying a valid device user through an input detection, selected from at least one of a set comprising: a correct passcode entry sequence; a touch ID recognition of a known user; a biometric recognition of a valid user; a biometric sensing of a valid users skin; a biometric detection that the electronic device continuously remains in contact with a valid user; and receiving a correct user response input, from a security challenge presented on the display.
[21]	The electronic device of claim 19, wherein the memory is accessible to the processor, wherein said memory comprises a static device-specific device account number of limited-use that originates from a card issuing authority and is limited to use by the electronic device in place of a card issuer account information, wherein further said static device-specific device account number has an expiration date of limited duration of validity, and wherein the generating a limited-use payment information comprises the processor generating said limited-use payment information by combining said static device-specific device account number, said device account expiration date, when said issuer payment account method is selected.
[22]	The electronic device of claim 19, wherein the memory is accessible to the processor, and wherein said memory comprises: a static device-specific device account information including a device account number of limited-use; and keys, wherein said device-specific device account information originates from a card issuing authority and is for limited-use by the specific electronic device only; and wherein said static device-specific device account information is valid for a limited duration, and wherein the generating a limited-use payment information comprises the processor generating a one-time limited-use cryptogram number and combining said limited-use static device account information and said one-time use cryptogram number to produce the limited-use payment information.

[23]	The electronic device of claim 19 further comprising a cryptographic processor operable to dynamically generate a one-time limited-use cryptogram number by cryptographically combining of at least one information accessible on the electronic device, selected from a set comprising: a sequence counter; a device account number; a device secret; device keys; card issuer keys; a time; an amount; an expiration date; a card security code; a location; merchant information; NFC recipient information; payment reader information; an online location; transaction information; payment information; device information; user information; an email address; a user identification entry; a hash of transaction information; and a hashed record of transactions, and wherein said cryptogram number is operable to be used in place of at least a portion of a card issuer payment information, in a payment transaction.
------	--