UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner

v.

CARDWARE INC.,
Patent Owner

Patent No. 11,620,634

PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,620,634

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. GROUNDS FOR STANDING 4
V. PRECISE RELIEF REQUESTED AND GROUNDS RAISED 4
VI. LEVEL OF ORDINARY SKILL 5
VII. OVERVIEW OF THE ’634 PATENT 6
VIII. CLAIM CONSTRUCTION 7
IX. DETAILED EXPLANATION OF GROUNDS 8
A. Ground 1A: Gomez, Amacker, and Casey Render Claims 1-2, 7-16, 27-34, and 36-38 Obvious 8
1. Gomez 8
2. Amacker 9
3. Casey 9
4. Gomez-Amacker-Casey Combination 11
5. Claim 1 17
6. Claim 2 27
7. Claim 7 28
8. Claim 8 28
9. Claim 9 30
10. Claim 10 32
11. Claim 11 34
12. Claim 12 34
13. Claim 13 34
14. Claim 14 35
15. Claim 15 36
16. Claim 16 36

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 2 of 104

17. Claim 27 38
18. Claim 28 40
19. Claim 29 41
20. Claim 30 43
21. Claim 31 44
22. Claim 32 44
23. Claim 33 45
24. Claim 34 45
25. Claim 36 45
26. Claim 37 48
27. Claim 38 48

B. Ground 1B: Gomez, Amacker, Casey, and Law Render Claims 3-6, 17-26, 35, and 39-72 Obvious 48

1. Law 48
2. Gomez-Amacker-Casey-Law Combination 53
3. Claim 3 57
4. Claim 4 59
5. Claim 5 60
6. Claim 6 60
7. Claim 17 60
8. Claim 18 60
9. Claim 19 61
10. Claim 20 61
11. Claim 21 61
12. Claim 22 61
13. Claim 23 61
14. Claim 24 62
15. Claim 25 62
16. Claim 26 62

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 3 of 104

17. Claim 35 63
18. Claim 39 63
19. Claim 40 67
20. Claim 41 67
21. Claim 42 68
22. Claim 43 68
23. Claim 44 69
24. Claim 45 69
25. Claim 46 70
26. Claim 47 70
27. Claim 48 70
28. Claim 49 70
29. Claim 50 71
30. Claim 51 72
31. Claim 52 73
32. Claim 53 73
33. Claim 54 74
34. Claim 55 75
35. Claim 56 77
36. Claim 57 77
37. Claim 58 77
38. Claim 59 78
39. Claim 60 78
40. Claim 61 78
41. Claim 62 78
42. Claim 63 78
43. Claim 64 78
44. Claim 65 78
45. Claim 66 79

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 4 of 104

46. Claim 67 79
47. Claim 68 79
48. Claim 69 79
49. Claim 70 79
50. Claim 71 80
51. Claim 72 80
C. Ground 1C: Gomez, Amacker, Casey, and Chin Render Claim 13 Obvious 80
1. Claim 13 80
X. DISCRETIONARY DENIAL IS NOT APPROPRIATE 83
XI. CONCLUSION 83
XII. APPENDIX A (CLAIM LISTING)

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 5 of 104

LIST OF EXHIBITS

EX1001	U.S. Patent No. 11,620,634 to Wyatt ("the '634 patent")
EX1002	Prosecution History of U.S. Patent App. No. 17/528,073
EX1003	Declaration of Dr. Michael Ian Shamos, Ph.D.
EX1004-EX1005	RESERVED
EX1006	U.S. Patent No. 8,255,323 to Casey et al. ("Casey")
EX1007	U.S. Patent No. 9,600,808 to Gomez et al. ("Gomez")
EX1008	U.S. Patent No. 8,423,462 to Amacker et al. ("Amacker")
EX1009-EX1013	RESERVED
EX1014	Curriculum Vitae of Dr. Michael Ian Shamos
EX1015-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 -EX1028	RESERVED

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 6 of 104

EX1029	Todd Wasserman, New Credit Card has LCD Screen, Touch Sensitive Buttons, The Sydney Morning Herald (Nov. 9, 2012)
EX1030	PCI Data Security Standard (PCI DSS), Information Supplement: PCI DSS Tokenization Guidelines, Version 2.0 (August 2011)
EX1031	History of Phones, Georgia Southern University
EX1032	U.S. Patent Publication No. 2015/0134540 A1 to Law et al. ("Law")
EX1033	Provisional Application No. 61/673,096 ("Law Provisional")
EX1034-EX1041	RESERVED
EX1042	Joint Claim Construction Statement (Dkt. No. 85), *Cardware Inc. v. Google LLC*, Case No. 7:24-cv-00278 (W.D. Tex. July 15, 2025)
EX1043	Exhibit D to CardWare Inc.'s Preliminary Infringement Contentions, *Cardware Inc. v. Google LLC*, Case No. 7:24-cv-00278 (W.D. Tex. Feb. 13, 2025) ("'634 Patent Infringement Contentions")
EX1044	U.S. Patent No. 7,593,000 to Chin ("Chin")
EX1045	U.S. Patent Publication No. 2012/0206406 A1 to Kim et al. ("Kim")

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 7 of 104

I. INTRODUCTION

Google LLC ("Petitioner") respectfully requests *inter partes* review of claims 1-72 ("the challenged claims") of U.S. Patent No. 11,620,634 ("the '634 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 '634 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 '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 Pat. No. 11,176,538 ("the '538 patent"), which is a continuation of application No. 16/459,150, filed on July 1, 2019, now Pat. No. 10,810,579 ("the '579 patent"), which is a continuation of application No. 15/701,261, filed on September 11, 2017, now Pat. No. 10,339,520 ("the '520

[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.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 8 of 104

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, 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.)

The '538, '579, and '520 patents are also at issue in *Cardware Inc., v. Google LLC*, Case No. 7:24-cv-00278 (W.D. Tex.), and the '579 patent is at issue in *Google LLC v. Cardware Inc.*, IPR2025-01344 (PTAB).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

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 9 of 104

settled after the decision on institution of trial, while IPR2023-00210 and IPR2023-00219 were denied institution.

The ’634, ’538, ’579, and ’520 patents are also at issue in *Cardware Inc., v. Apple Inc.*, Case No. 7:24-cv-00279 (W.D. Tex.), which was filed on November 4, 2024 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 not been involved 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.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 10 of 104

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 '634 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 1-72 of the '634 patent. The challenged claims should be found unpatentable on the following grounds:

Ground 1A: Claims 1-2, 7-16, 27-34, and 36-38 are unpatentable under 35 U.S.C. §103 as being obvious in view of Gomez (EX1007), Amacker (EX1008), and Casey (EX1006).

Ground 1B: Claims 3-6, 17-26, 35, and 39-72 are unpatentable under 35 U.S.C. §103 as being obvious in view of Gomez, Amacker, Casey, and Law (EX1032).

Ground 1C: Claim 13 is unpatentable under 35 U.S.C. § 103 as being obvious in view of Gomez, Amacker, Casey, and Chin (EX1044).

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 11 of 104

The earliest possible priority date of the ’634 patent is March 15, 2013.[2]

Gomez stems from an application filed June 22, 2012 (EX1007, Cover); Amacker stems from an application filed May 1, 2009 (EX1008, Cover); and Law published from an application filed April 16, 2013 (EX1032, Cover), which claims priority to provisional application No. 61/673,096 (“Law Provisional”) filed July 18, 2012 (EX1033, Cover); and thus each qualifies as prior art under pre-AIA § 102(e).

Casey published August 28, 2012 from an application filed January 9, 2009 (EX1006, Cover), and thus qualifies as prior art under pre-AIA §§ 102(a) and (e).

Chin issued on September 22, 2009 from an application filed December 24, 2008 (EX1044, Cover), and thus qualifies as prior art under pre-AIA §§ 102(a), (b), and (e).

VI. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) at the time of the alleged invention of the ’634 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.

[2] Petitioner does not concede that the ’634 patent is entitled to a March 15, 2013 priority date.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 12 of 104

EX1003, ¶¶36-61.[3] More education can supplement practical experience and vice versa. *Id*.

VII. OVERVIEW OF THE '634 PATENT

The '634 patent describes an electronic payment card capable of generating a "limited-duration payment number" for use in a payment transaction. EX1001, 2:28-2:65, 10:33-12:24, FIG. 7. Figure 7 illustrates a process for generating and using a limited-duration number:

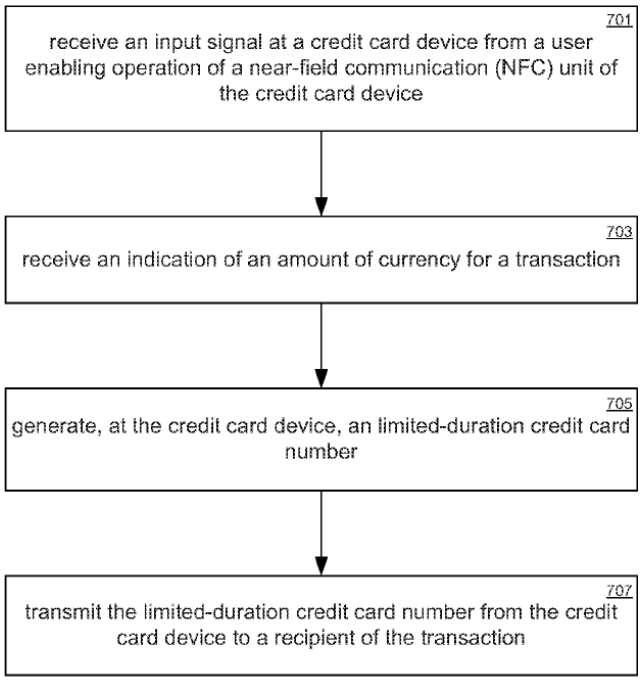


FIG. 7

EX1001, FIG. 7.

[3] Petitioner submits the declaration (EX1003) and curriculum vitae (EX1014) of Dr. Michael Shamos, an expert in the field of the '634 patent. EX1003, ¶¶1-13; EX1014.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 13 of 104

"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.*, 10:43-48. Further, the "limited-duration credit card number is able to be limited to only one transaction." *Id.*, 10:48-53.

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 '634 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, ¶¶62-65.)[4]

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

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 14 of 104

IX. DETAILED EXPLANATION OF GROUNDS

As detailed below, each of the challenged claims is unpatentable. (EX1003, ¶¶92-257.)

A. Ground 1A: Gomez, Amacker, and Casey Render Claims 1-2, 7-16, 27-34, and 36-38 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. Because the authentication cryptogram is time-limited, "the information that can be gleaned from a payment card…is rendered useless for making an unauthorized subsequent transaction." *Id.*, 5:7-11, FIG. 7.

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 EPIC static payment card identifying number and the dynamically-generated authentication cryptogram to a point-of-sale (POS) terminal, which are then conveyed to an authentication server (e.g., EPIC) before the transaction request is sent to an issuer or bank for approval. *Id.*, 7:49-8:2.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 15 of 104

2. Amacker

Amacker discloses a "mobile wallet server" stored on a user's personal mobile 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. 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. Casey's smartphone receives "a request for payment" via NFC or other communication, displays payment card and transaction information, and receives a user input to confirm or deny a transaction. *Id.*, 8:52-9:36, 12:64-13:51, 14:12-49, 15:24-59; FIGs. 4-8. For example, Casey discloses receiving a user input by entering a PIN, moving a graphical element (e.g., a slide bar) across a screen, or moving the device such that a motion sensing device (e.g., comprised of a three-axis accelerometer) is used to sense a particular motion of the

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 16 of 104

device. *Id.*, 7:50-8:14, 9:9-22, 13:36-51. FIG. 5 shows an example user interface flow for confirming a transaction:

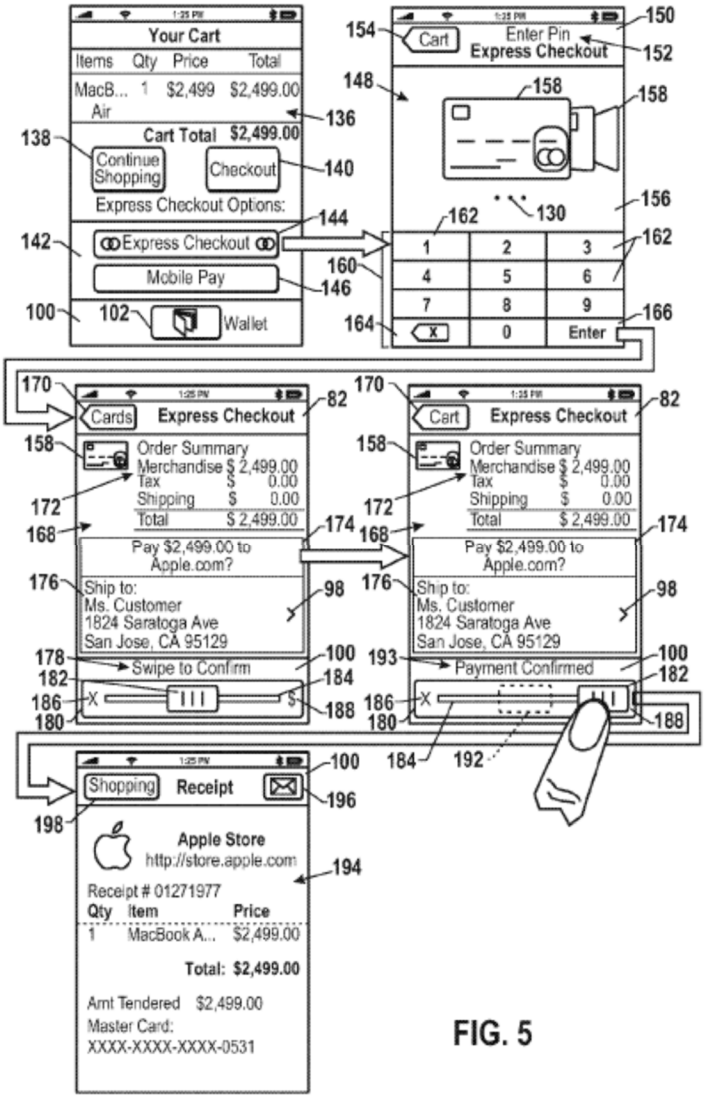


FIG. 5

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. For example, the receipt may identify the amount tendered, the payment recipient, and the payment instrument used." *Id.*, 10:47-53, 10:20-29, 16:3-20.

4. Gomez-Amacker-Casey Combination

A POSITA would have beneficially applied the teachings of Amacker and Casey to modify Gomez's mobile payment system to include multiple improvements. EX1003, ¶¶66-83, 93.

First, a POSITA would have modified Gomez such that the EPIC payment card of Gomez would include a touchscreen display and/or is integrated into a mobile device (such as a smartphone) 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, ¶94. Including a touchscreen display would have allowed the resulting device to display additional information regarding payment cards, details of a transaction, and transaction status on the device while allowing for easier, intuitive user manipulation via touchscreen. EX1003, ¶94; EX1008, 5:1-17, FIG. 2. Moreover, a touchscreen display would have allowed the resulting device to conserve space by allowing for display of user input features (e.g., the PIN input keypad disclosed by Gomez) without requiring additional physical hardware. EX1003, ¶94; EX1007, 13:34-44, FIG. 14 (PIN input keypad 162).

Furthermore, Gomez, Amacker, and Casey all disclose communicating payment information via NFC communication, and a POSITA would have recognized that integrating Gomez's EPIC payment card into a mobile device such as a smartphone would have reduced the number of devices that a user needed to

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 18 of 104

carry while also improving the user experience due to the improved user interfaces and processing power of smartphone devices at the time. EX1007, 7:49-54, 8:11-24, 10:53-57; EX1008, 3:27-34; EX1006, 1:23-27, 5:57-6:14; EX1003, ¶95.

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 resulting device. EX1008, 2:37-3:3, 3:42-57, 4:37-5:17; EX1003, ¶96. Gomez describes NFC communication with the merchant occurring by "bring[ing] the payment card in proximity to a near field communication terminal." EX1007, 8:11-24, 7:49-54, 10:53-57. Amacker discloses that such NFC communications can result in the receipt by the electronic device of a payment request. 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:

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 19 of 104

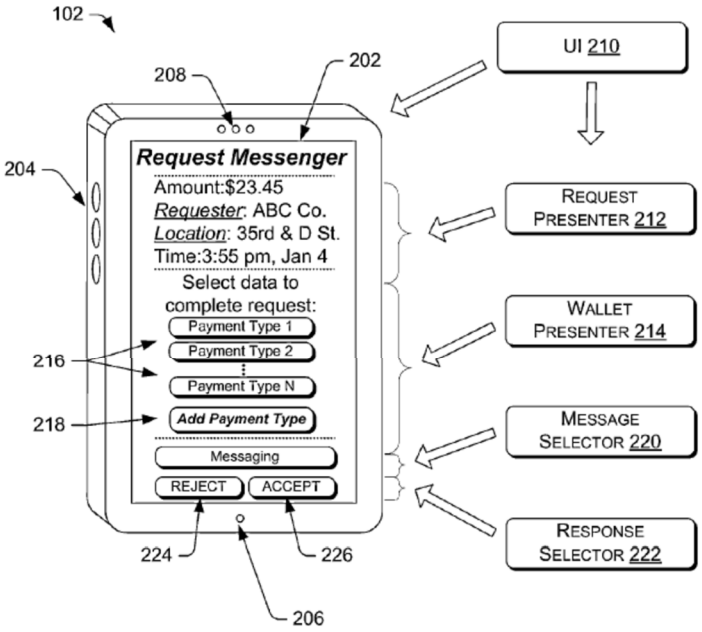


Fig. 2

Id., FIG. 2. This modification would have improved the resulting system by allowing the user to better ensure that they are approving a payment transaction and transmitting payment information to the correct merchant terminal, which can prevent fraudulent transmittal of payment information to an incorrect terminal. EX1003, ¶96. Such a modification would also allow the user to bring the NFC-enabled electronic device in proximity to an NFC terminal, receive a payment request, and 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.

Third, a POSITA would have modified Gomez based on Amacker 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" by choosing from a list of cards that includes "description name (or nickname) and card logo." EX1007, 20:30-59, 21:5-20; EX1003, ¶97. Amacker provides additional details on how a user can use a touchscreen display to view additional information about payment methods before selecting. EX1003, ¶97; EX1008, 5:18-41, claim 1, FIG. 2. A POSITA would have recognized that including additional information in the card selection process would have allowed the user to more easily identify a desired card for a particular transaction. EX1003, ¶97.

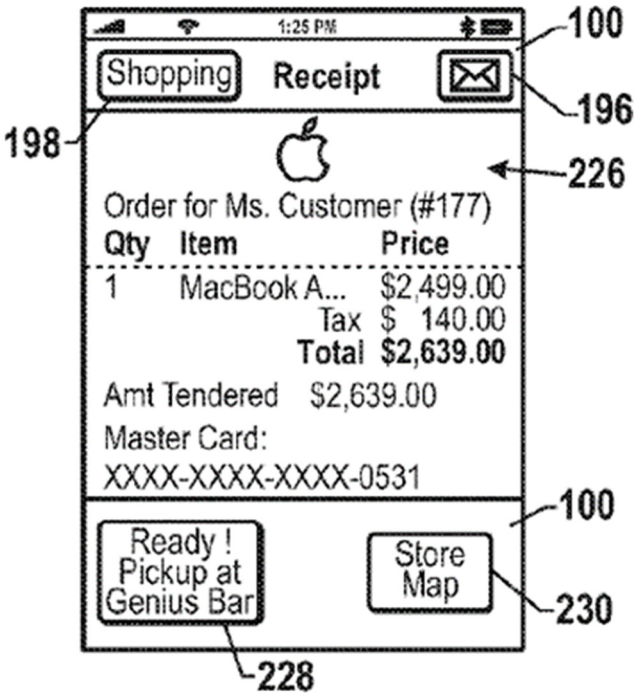
Fourth, a POSITA would have modified Gomez based on the teachings of Amacker to generate the authentication cryptogram in response to receiving the request to ensure that the limited-duration cryptogram is valid for the intended transaction. EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; EX1003, ¶98. Gomez describes priming operations such as entry of "a fingerprint or PIN number, into the payment card," upon which the cryptogram is generated if the user credentials are valid. EX1007, 5:13-18; *see also id.*, 2:59-64, 7:9-16, 9:12-33, 13:40-44. A POSITA would have understood that entry of a fingerprint or PIN number are priming operations, as described in the '634 patent, because these user inputs prepare the device for a transaction, providing an indication that a transaction is imminent. EX1003, ¶98; *see also* EX1001, 12:2-12, 12:42-46, 14:4-15 (describing a priming operation generally as an operation that "primes"/prepares the device for a

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 21 of 104

transaction, providing an indication that a transaction is imminent). A POSITA would have found it obvious to implement the priming operation (which results in generation of the cryptogram) in the combined system to include a user entering a valid credential and bringing the device within proximity of an NFC terminal to receive a payment request—that is, an indication that a transaction is imminent. EX1003, ¶98.

Fifth, a POSITA would have further modified the Gomez-Amacker combination based on the teachings of Casey such that the user's device receives and displays a receipt for the payment transaction, as shown in Casey's FIG. 8 below. EX1006, 10:47-49. A POSITA would have understood that sending a receipt would be beneficial because it would provide a user with an indication of the status of the transaction, i.e., that the transaction is complete. EX1003, ¶99; *see also generally* EX1001 (specification does not define "status"). Furthermore, such a modification would have beneficially provided a user with assurance that the correct amount, recipient, and payment instrument were involved in the transaction and to provide proof that the transaction has been completed. EX1003, ¶99. Such a modification would have been easily implemented since Casey, like Gomez and Amacker, also describes sending and receiving information at the mobile device through an NFC interface. EX1006, 1:23-27, 5:57-6:14, 6:58-61, 8:52-58, 10:41-43, 16:21-26, 17:66-18:2.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 22 of 104



EX1006, FIG. 8.

Sixth, a POSITA would have further modified the Gomez-Amacker-Casey device based on the teachings of Casey such that the user input of the priming operations may involve a detected user motion of the device. EX1003, ¶100. Gomez discloses snap sensors in the payment device to detect motion/manipulations adapted to activate the device. EX1007, 7:4-8. However, a POSITA would have understood that, when implementing Gomez's payment card as a mobile device, as described above, this detection of a user motion of the device would have to be adapted to accommodate the larger device. EX1003, ¶100. Casey discloses that a mobile phone may accommodate user input through a detected user motion of the device by incorporating a motion sensing device into the mobile phone. EX1006, 7:59-8:3. A

POSITA would have recognized that adding this capability to detect user motion of the device would have enhanced user experience by providing another way to perform the user input of the priming operations, while also enhancing security if the motion detection is implemented in conjunction with other user input features such as fingerprint, PIN, or similar features. EX1003, ¶100.

Finally, a POSITA would have recognized that applying the teachings of Amacker and Casey 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, ¶101. *KSR Int'l. Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

5. Claim 1

i) [1.pre][5]

To the extent limiting, Gomez discloses the preamble of claim 1. EX1003, ¶102. Gomez describes a mobile payment system and method for "purchase transaction approval at a retail merchant" ("method…for performing a payment transaction"). EX1007, 3:65-67, 5:65-6:4, 2:45-54; EX1003, ¶102. Gomez's method "utilizes a secure authentication cryptogram which is generated uniquely for

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

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 24 of 104

each attempted use of the payment card, and which expires within a short period of time thereafter" ("generating and using limited-use payment information"). EX1007, 1:58-63, 7:17-48. The device generates an "authentication cryptogram for each attempted transaction only after the cardholder successfully presents a credential." *Id.*, 5:13-18; *see also id.*, 7:26-8:9. Because the authentication cryptogram is time-limited ("limited-use payment information"), "the information that can be gleaned from a payment card…is rendered useless for making an unauthorized subsequent transaction." *Id.*, 5:7-11, FIG. 7.

Gomez further describes an EPIC card having a static payment card identifying number, which identifies the specific card/device corresponding to the customer's EPIC account, but is linked to one or more actual credit/debit card accounts. *Id.*, 2:19-39, 20:1-37. The payment card transmits the EPIC static payment card identifying number and the dynamically-generated authentication cryptogram to the point-of-sale (POS) terminal, which are 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. Accordingly, Gomez's method involves generating and using an authentication cryptogram for each payment transaction. EX1003, ¶103.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 25 of 104

ii) [1.a]

Gomez discloses performing the method using an "EPIC payment card." EX1007, 11:19-38, 2:55-3:3, FIG. 9. Gomez describes the payment card as having electronic features ("electronic device") such as a processor, electronic circuit, and electronic display. *Id.*, 10:27-11:6, 12:49-63. As discussed above (Section IX.A.4), in the predictable combination, the payment device can be a mobile device such as a smartphone ("electronic device"). EX1008, 2:13-25; EX1003, ¶104.

Gomez explains that the card cannot be used until a cardholder performs a priming input operation such as entry of "a fingerprint or PIN number, into the payment card." EX1007, 5:13-18; *see also id.*, 2:59-64, 7:9-16, 9:12-33, 13:40-44; EX1003, ¶105. As discussed above (Section IX.A.4), in the Gomez-Amacker-Casey combination, the priming operation (which results in generation of the cryptogram) includes a user entering a valid credential and bringing the device within proximity of an NFC terminal to receive a payment request—that is, an indication that a transaction is imminent. EX1003, ¶105; *see infra* Elements [1.f]-[1.g]; *see also* EX1001, 12:2-12, 12:42-46, 14:4-15.

iii) [1.b]

Gomez discloses that its device "includes a processor." EX1007, 10:34-38, 2:59-64. Amacker confirms that when a payment card is implemented as a mobile phone, that device also includes a processor. EX1008, 3:23-27 (mobile wallet server

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 26 of 104

(MWS) 102 implemented on a mobile computing device), FIG. 4 (MWS 102 includes processor(s) 402); EX1003, ¶106.

iv) [1.c]

Gomez discloses that its payment card device includes a "processor 342 coupled to…an activation input device 350…one or more displays 354, and an interface device 356." EX1007, 10:34-38, 12:49-61. The display of the Gomez-Amacker-Casey device "may be a touch screen display." EX1008, 4:51-60; EX1006, 7:26-29; Section IX.A.4; EX1003, ¶107.

v) [1.d]

The Gomez-Amacker-Casey device's processor may include various integrated circuits, including "NFC circuits for implementing a near-field communications transceiver." EX1007, 10:53-57, 7:49-54, 8:11-24, 2:40-3:3; EX1003, ¶108.

vi) [1.e]

As discussed for Element [1.a], the Gomez-Amacker-Casey combination involves priming the payment card device by inputting a fingerprint or PIN and then bringing the device within proximity of an NFC terminal to receive a payment request, at which point the authentication cryptogram is generated. *Supra* Element [1.a]; *see infra* Elements [1.f]-[1.g]; *see also* Section IX.A.4. As discussed, when the authentication cryptogram is generated, the device is ready to be used in a

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 27 of 104

transaction by a particular user. *Supra* Element [1.a]; EX1007, 2:59-64, 5:13-18, 7:9-16, 9:12-33, 13:40-44; EX1003, ¶109. Indeed, all that is required after generation of the authentication cryptogram to perform the transaction is acceptance of the payment request. EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; EX1003, ¶109; *see infra* Elements [1.f]-[1.g]. A POSITA would have understood that the user for which the device is readied to perform a transaction is an "identified user" because Gomez discloses "compar[ing] the credential entered by the card user against a reference credential stored within the card," i.e., a pre-identified user, to determine if the credential is valid. EX1007, 9:19-39, FIG. 6 (steps 304 and 306); EX1003, ¶109.

vii) [1.f]

In the Gomez-Amacker-Casey combination, 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; Section IX.A.4; EX1003, ¶110. The communication occurs via the NFC interface. EX1007, 7:49-54, 8:11-24, 10:53-57; EX1008, 3:27-34; *supra* Element [1.d].

viii) [1.g]

As described above (Section IX.A.1), Gomez explains that a customer's EPIC card (and EPIC account) may be linked to one or more actual credit/debit cards.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 28 of 104

EX1007, 2:19-39, 20:1-37. Gomez further explains that its 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." *Id.*, 20:30-59, 21:5-20, FIG. 9; EX1003, ¶111. The customer can "select the card they wish to use on their next transaction" by choosing from a list of cards that includes "description name (or nickname) and card logo." EX1007, 20:43-59.

Amacker confirms that, in the Gomez-Amacker-Casey combination—which as discussed for Element [1.c], includes a touch screen—the mobile device's "UI 210 may include…a request presenter 212 to identify information related to a request," including request amount, location, and time and requester information, as shown in red in FIG. 2 below. EX1008, 5:1-17, FIG. 2; *supra* Element [1.c]; *see also* Section IX.A.4. Amacker also discloses 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.)," as shown in green in FIG. 2 below. EX1008, 5:18-41, claim 1; EX1003, ¶112.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 29 of 104

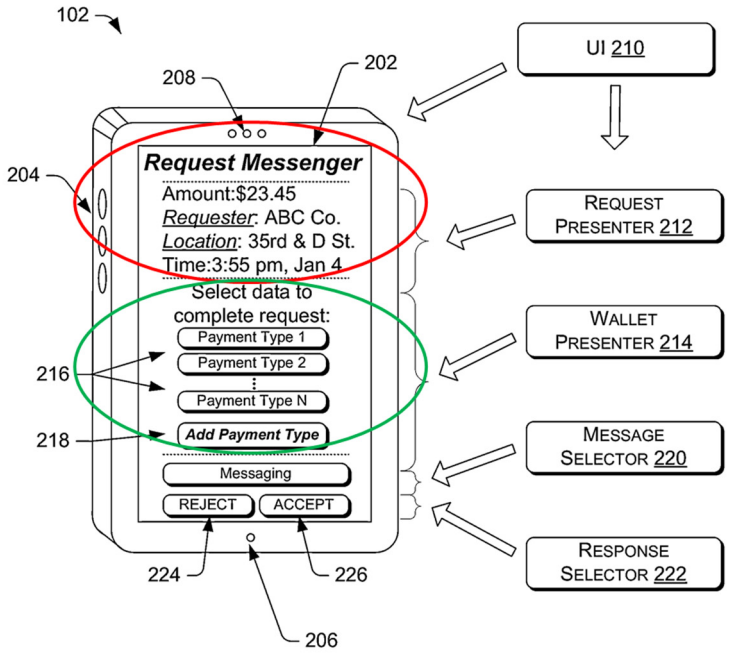


Fig. 2

EX1008, FIG. 2. The display of this information allows the user to determine whether to select "a reject option 224 [or] an accept option 226" on the screen to reject or approve the transaction. *Id.*, 6:3-15.

ix) [1.h]

As discussed for Element [1.pre], Gomez describes the generation of a time-limited "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" ("generating…limited-use payment information"). EX1007, 1:58-63,

7:17-48; *see also id.*, 5:7-18, 7:26-8:9, FIG. 7; *supra* Element [1.pre]. Gomez further describes a "seed value stored within the payment card" and a dynamically generated "temporal signal value which changes for each attempted use of the payment card." EX1007, 1:64-2:4. Gomez explains that the payment card's "processor [is] operable to verify the credential for the payment card user and … to generate an authentication cryptogram based at least in part on the seed value and the temporal signal value" ("dynamically generating, by the processor, limited-use payment information"). *Id.*, 2:59-64; EX1003, ¶113.

x) [1.i]

As discussed for Element [1.h], Gomez discloses that the authentication cryptogram is dynamically generated ("wherein said limited-use payment information is dynamically generated") based on a seed value and a temporal signal value that changes dynamically for each attempted use of the card. *Supra* Element [1.h]; EX1007, 2:59-64. Gomez further discloses that the authentication cryptogram is dynamically generated on the device by combining a seed value with a temporal signal such as "the sequence value (or sequential number) of the attempted use" (attempted transaction) of the device ("based on a per-transaction sequential parameter originating from the electronic device"). EX1007, 1:58-2:4, 7:41-43, 21:37-48, 7:17-26, 8:36-41, 10:58-11:6, FIG. 7; EX1003, ¶114.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 31 of 104

xi) [1.j]

As discussed for Elements [1.h]-[1.i], an authentication cryptogram ("limited-use payment information") is generated for each payment transaction. *Supra* Elements [1.h]-[1.i]; EX1003, ¶115. As discussed for Element [1.pre], Gomez describes that the payment card/device transmits the EPIC static payment card identifying number and the dynamically-generated authentication cryptogram to the POS terminal. *Supra* Element [1.pre]; EX1003, ¶115. A POSITA would have understood that the authentication cryptogram for a given payment transaction would be used ("using limited-use payment information in connection with the payment transaction") in place of the card issuer supplied payment information (the "actual credit card account number" disclosed by Gomez) ("in place of issued payment information") associated with the selected actual credit card account (*see* Element [1.g]) ("associated with said selected issued payment account") because the authentication cryptogram is combined with the EPIC static payment card identifying number, which are together 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, ¶115.

xii) [1.k]

Gomez discloses "communicating a payment card identifying number to a payment processing system, and communicating the authentication cryptogram in a

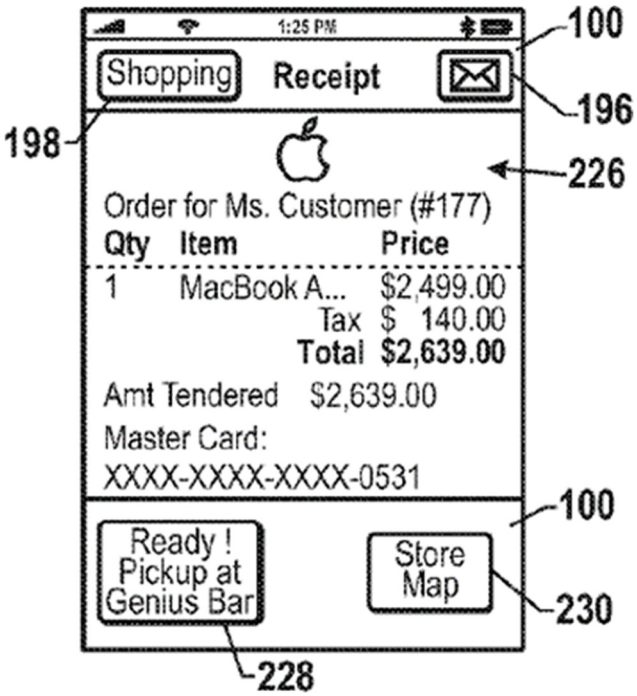
CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 32 of 104

payment card account name field to the payment processing system." EX1007, 2:50-54, 8:16-20. Gomez explains that the transmission of the authentication cryptogram and static payment card identifying number to the payment processing system may occur "using near field communication (NFC)." *Id.*, 7:49-54, 8:6-24; EX1003, ¶116.

xiii) [1.l]

As described by Casey, in the Gomez-Amacker-Casey combination, "the device 10 may receive and display (block 78) a receipt for the payment transaction," as shown in FIG. 8 below. EX1006, 10:47-49; *see also* Section IX.A.4. "For example, the receipt may identify the amount tendered, the payment recipient, and the payment instrument used." EX1006, 10:49-53, *see also id.*, 10:20-29, 16:3-20. Like Gomez and Amacker, Casey also describes sending and receiving information at the mobile device through an NFC interface. EX1006, 1:23-27, 5:57-6:14, 6:58-61, 8:52-58, 10:41-43, 16:21-26, 17:66-18:2; *see also* Elements [1.d], [1.f], [1.k]. A POSITA would have thus understood that a receipt indicating that the transaction is complete (i.e., a completion status) would have been received in same manner as the cryptogram (limited-use payment information) and EPIC static payment card identifying number are transmitted (i.e., via the NFC interface). EX1003, ¶117; Section IX.A.4.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 33 of 104



EX1006, FIG. 8.

xiv) [1.m]

As discussed for Element [1.l], in the Gomez-Amacker-Casey device, a receipt is displayed on the device screen indicating that the transaction is complete. *Supra* Element [1.l]; EX1003, ¶118; Section IX.A.4. Casey confirms that this receipt is suitable for display on an "electronic device that includes a touch screen." EX1006, 3:10-12, 10:54-61.

6. Claim 2

As discussed for Elements [1.pre] and [1.h], the dynamically generated limited-use payment information is an authentication cryptogram. *Supra* Elements [1.pre], [1.h]; EX1003, ¶119.

7. Claim 7

The Gomez-Amacker-Casey combination's priming operation involves receiving a user input of a user credential and bringing the user's device within proximity of the NFC point-of-sale terminal. *Supra* Elements [1.a], [1.e]; Section IX.A.4; EX1003, ¶120.

8. Claim 8

i) [8.pre], [8.a]

The Gomez-Amacker-Casey combination's priming operation, which readies the user's device to perform a payment transaction, involves bringing the user's device within proximity of the NFC terminal to receive a payment request. *Supra* Element [7]. A POSITA would have understood that an NFC terminal continuously emits a radio frequency signal, and thus, for a payment request to be received through NFC, the user's device would have identified the nearby NFC terminal recipient as an NFC payment facility by identifying this emitted signal. EX1003, ¶121; EX1006, 6:58-61, 8:52-64.

ii) [8.b]

As discussed for Element [1.e], Gomez discloses "compar[ing] the credential entered by the card user against a reference credential stored within the card," i.e., a pre-identified user, to determine if the credential is valid and the user is authorized

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 35 of 104

to perform the transaction. EX1007, 9:19-39, FIG. 6 (steps 304 and 306); *supra* Element [1.e]; EX1003, ¶122.

iii) [8.c]

As discussed for Elements [1.f]-[1.g], Amacker discloses that the device may display information related to a request. EX1008, 5:1-17; Elements [1.f]-[1.g]; *see also* Section IX.A.4. Amacker further discloses that the device's UI includes a "response selector 222 [which] may enable the user 110 to respon[d] to the request shown by the request presenter 212" by selecting on the touch screen (as shown in red below) either a "reject option 224" to reject the transaction or an "accept option 226" to approve the transaction. EX1008, 6:3-15; EX1003, ¶123.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 36 of 104

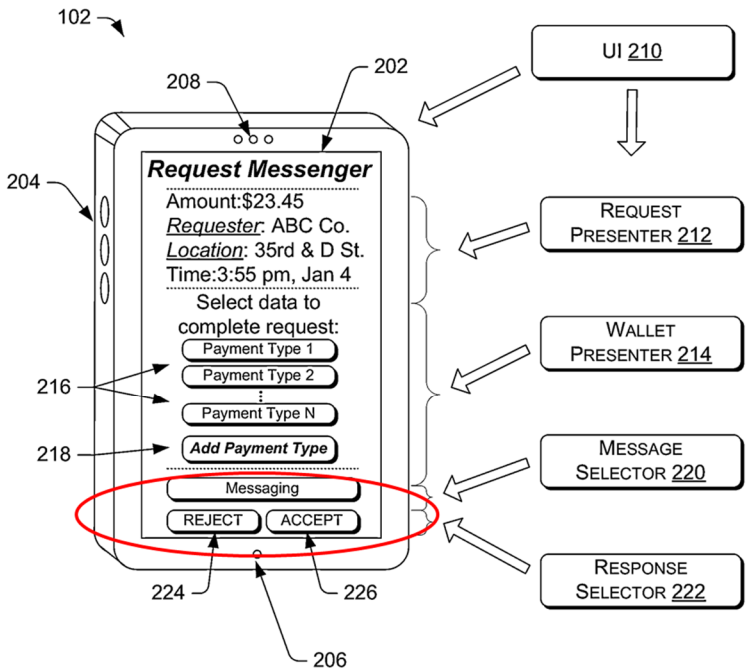


Fig. 2

EX1008, FIG. 2

9. Claim 9

i) [9.pre]

As discussed for Elements [1.g] and [8.c], in the Gomez-Amacker-Casey combination, when a user approves a transaction via the mobile device's displayed payment request ("wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device"), that payment request displays information pertaining to the request including the requester (i.e., the requesting NFC terminal) ("for both said identifying") as well as

options/buttons for approving the payment transaction ("and said user approval of said payment transaction"). Elements [1.g], [8.c]; EX1003, ¶124; Section IX.A.4.

ii) [9.a]

As discussed for Element [1.e], Gomez discloses "compar[ing] the credential entered by the card user against a reference credential stored within the card," i.e., a pre-identified, known authorized user of the device, to determine if the credential is valid and the user is authorized to perform the transaction. EX1007, 9:19-39, FIG. 6 (steps 304 and 306); *supra* Element [1.e]; EX1003, ¶125. A POSITA would have understood that this comparison is performed by the Gomaz-Amacker-Casey device's processor, since Gomez explains that "[t]he processor may be configured to verify the credential for the payment card user" ("the processor identifying that said user input matches a known authorized user of the electronic device"). EX1007, 10:47-50; EX1003, ¶125. As discussed for Elements [1.a], [1.e], [7], and [8.a], the verification of these user credentials is required to ready the device to perform a payment transaction (i.e., by generating an authentication cryptogram in response to receipt of a payment request) ("before said readying said device to perform a payment transaction"). Elements [1.a], [1.e], [7], [8.a]; EX1003, ¶125.

iii) [9.b]

As discussed for Elements [1.a], [1.e], and [9.a], the Gomez-Amacker-Casey device cannot perform the transaction ("disallowing the payment transaction by the

device") until the device is readied to perform the transaction by generating the authentication cryptogram in response to receiving the payment request ("until said readying said device to perform the payment transaction is successfully completed"). Elements [1.a], [1.e], [9.a]; EX1003, ¶126; Section IX.A.4. In particular, Gomez explains that the card is otherwise deactivated if a user's credentials cannot be authorized, if payment has already occurred, or if payment has not occurred within a certain time period after the authentication cryptogram has been generated. EX1007, 8:11-24, 9:33-37, 10:27-33, FIG. 4 (step 266), FIG. 6 (steps 306, 308, 310, 324, 326). A POSITA would have thus understood that the device disallows the payment transaction capability before the readying steps are completed. EX1003, ¶126.

10. Claim 10

i) [10.pre], [10.a], [10.b]

As discussed for Elements [1.a], [1.e], and [9.a], Gomez discloses that the processor verifies a user's input credential (e.g., a fingerprint or PIN) and compares the credential to a reference credential stored in the user's device to determine if the input credential is valid. EX1007, 5:13-18, 7:9-16, 9:19-39, 10:18-22, 10:47-50, FIG. 6 (steps 304 and 306). A POSITA would have understood from these disclosures that a stored reference credential is, for example, the known fingerprint or known PIN of an authorized user, such that a validity comparison involves

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 39 of 104

determining whether the input credential matches the reference credential to determine whether an authorized user is attempting to use the device. EX1003, ¶127. Gomez further explains that a user's fingerprint is read through a fingerprint/biometric sensor included within the device. *Id.*, 7:10-13, 9:21-23, 11:30-35. A POSITA would have understood that the touch screen of the Gomez-Amacker-Casey device also uses sensors to sense user touch (the very essence of a "touch screen"), and thus the input of a PIN would also be through sensors included within the device. *See, e.g.*, EX1008, 4:51-60; EX1045, ¶[0036]; EX1003, ¶127; Section IX.A.4. Thus, a POSITA would have understood that verifying a user's credentials requires that the processor determine a match between ("wherein said successfully validating the identified user comprises the processor successfully determining a match between") the user's input credential (i.e., a fingerprint or PIN which is input through a fingerprint/biometric sensor or touch sensor of the device) ("firstly, a user input received via at least one of a set of user input sensors of the electronic device") and a reference credential stored on the device and representing either a known fingerprint ("predetermined user characteristics") or a known PIN ("challenge-responses") of an authorized user ("and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device"). EX1003, ¶127. A POSITA would have understood that a PIN number entry is a "challenge-response" since it is

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 40 of 104

a response to a displayed request to enter a PIN (i.e., a challenge). *See* EX1001 ('634 patent does not discuss a "challenge" or a "challenge-response"); EX1003, ¶127; EX1007, 13:34-44; Section IX.A.4 (discussing incorporation of display into touch screen of combined device). This interpretation is consistent with that presented in Patent Owner's infringement contentions, which identify a PIN/password/passcode as a "challenge-response." EX1043, 73-77, 111.

11. Claim 11

When a user inputs a personal identification number (PIN) on the touch-screen display of the Gomez-Amacker-Casey device, that user is entering a passcode sequence via touch-screen display. *Supra* Elements [10.pre]-[10.b]; EX1007, 13:40-42; Section IX.A.4; EX1003, ¶128.

12. Claim 12

The known reference credentials stored on the Gomez-Amacker-Casey device representing fingerprints of authorized users are fingerprints electronically sensed by touch, and therefore would be understood to be biometric touch characteristics. *Supra* Elements [10.pre]-[10.b]; EX1007, 11:30-38 (referring to fingerprint data as biometric touch data); EX1003, ¶129.

13. Claim 13

A POSITA would have understood that the reference fingerprint of a known user is a "known user touch gesture." EX1003, ¶130. For example, Gomez discloses

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 41 of 104

that the entry of a fingerprint can be performed "by swiping a fingerprint across a fingerprint sensor included within the card." EX1007, 7:10-13. A POSITA would have understood that a swiping motion of a fingerprint is a "known user touch gesture." EX1003, ¶130. Thus, when the fingerprint reader of the Gomez-Amacker-Casey device is implemented as a sensor detecting the swipe of a certain authorized user's fingerprint, the fingerprint credentials stored on the device would also represent known fingerprint swipe gestures. *Id.*, ¶130.

Under Patent Owner's interpretation of this limitation, Gomez's disclosure of a known PIN for a given user is also a "predetermined user characteristic[] stored within the electronic device [that] comprise[s] a known user touch gesture." EX1003, ¶131. In Patent Owner's infringement contentions, Patent Owner interprets this limitation such that a PIN or passcode entry is a "known user touch gesture." EX1043, 77. As discussed for Elements [1.a], [1.e], and [9.a], Gomez discloses that the processor verifies a user's input credential (e.g., a PIN) and compares the credential to a reference credential (e.g., a reference PIN) stored in the user's device to determine if the input credential is valid. EX1007, 5:13-18, 7:9-16, 9:19-39, 10:18-22, 10:47-50, FIG. 6 (steps 304 and 306).

14. Claim 14

As discussed above (Section IX.A.4), in the Gomez-Amacker-Casey device, user input for the priming operations may be provided through a user motion of the

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 42 of 104

device. EX1006, 7:59-8:3. As discussed for Element [1.e], Gomez discloses "compar[ing] the credential entered by the card user against a reference credential stored within the card," i.e., a pre-identified, known authorized user of the device, to determine if the credential is valid and the user is authorized to perform the transaction. EX1007, 9:19-39, FIG. 6 (steps 304 and 306); *supra* Element [1.e]; EX1003, ¶132. Thus, in the combination, a POSITA would have understood that the reference credential stored on the device would correspond to a known user motion of the device for a particular authorized user. EX1003, ¶132.

15. Claim 15

As discussed for Element [1.a], the priming operation input may be the entry of a user input such as a fingerprint or PIN. *Supra* Element [1.a]; EX1003, ¶133.

16. Claim 16

i) [16.pre], [16.a]

As discussed for Element [8.b], readying the Gomez-Amacker-Casey device to perform a transaction involves determining that the user's input matches that of a known identified user, thus identifying that the user is authorized to perform the transaction. Element [8.b]; EX1003, ¶134.

ii) [16.b]

As discussed for Element [8.c], in the Gomez-Amacker-Casey device, the identified/authorized user may provide further user input to approve the payment

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 43 of 104

transaction by touching the "accept" button on the payment request displayed on the touch-screen display. Element [8.c]; Section IX.A.4; EX1003, ¶135.

iii) [16.c]

As discussed for Elements [10.pre]-[10.b], successfully identifying a user involves the device's processor validating the user as an authorized user of the device ("wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device") by comparing the user's input (e.g., a fingerprint entered via the device's fingerprint touch sensor or a PIN entered by the touch-screen display, which contains touch sensors) ("by comparing a user-touch input received via a touch input sensor on the electronic device") with a known reference user input credential (i.e., a recognized fingerprint or PIN) stored in the device ("with a recognized valid user-touch, stored in a memory of the electronic device"). Elements [10.pre]-[10.b]; EX1003, ¶136. A POSITA would have further understood that the reference credentials stored in the device are "stored in a memory of the electronic device" because Gomez discloses that the payment "card 340 includes a processor 342 coupled to a memory 344," which a POSITA would have understood is used to store information used by the processor in executing the steps of the transaction. EX1007, 10:34-38; EX1003, ¶136.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 44 of 104

iv) [16.d], [16.e], [16.f], [16.g]

As discussed for Elements [1.g] and [8.c], a user of the Gomez-Amacker-Casey device indicates their approval of the transaction by ("wherein said user approval for performing the payment transaction further comprises") clicking accept on the displayed payment request on the touch-screen display, where the payment request includes information about the transaction ("visually presenting information of the payment transaction on the touch screen display of said electronic device") as well as options/buttons allowing the user to approve the transaction ("visually presenting a request for user approval of the payment transaction via touch input at said electronic device"). Elements [1.g], [8.c]; Section IX.A.4; EX1003, ¶137. As discussed, the transaction is approved after the user selects the "accept" button on the display ("subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device"). Elements [1.g], [8.c]; EX1003, ¶137.

17. Claim 27

As discussed for Element [1.h], the secure authentication cryptogram ("limited-use payment information") is generated uniquely for each attempted use of the Gomez-Amacker-Casey device, based on a seed value stored within the device and a dynamically generated temporal signal value which changes for each attempted use of the device. *Supra* Element [1.h]; EX1007, 1:58-2:4, 2:59-64, 5:7-

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 45 of 104

18, 7:17-8:9, FIG. 7; EX1003, ¶138. As discussed for Element [1.j], the authentication cryptogram is combined with the EPIC static payment card identifying number and together 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, ¶138.

Gomez explains that the seed value is both secret and known by the payment processing authority that processes the transaction. For example, Gomez explains that an authentication cryptogram is secure because an unauthorized party would have to know the seed value (which is not directly sent in the transaction) in order to generate a new authentication cryptogram and authorize a future fraudulent transaction. EX1007, 5:43-47. Gomez also explains that when the authentication cryptogram and EPIC static payment card identifying number are shared with the merchant, this information is eventually communicated to an EPIC authentication server, which "determines whether the authentication cryptogram is valid for the transaction…by independently generating a 'reference' authentication cryptogram based on the seed value corresponding to the EPIC account number, and based upon the date/time of the transaction (or other temporal signal value…)." *Id.*, 5:61-6:38. Accordingly, "<u>the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret</u>

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 46 of 104

information" because the authentication cryptogram is dynamically generated based on the seed value and temporal signal value. EX1003, ¶139.

18. Claim 28

i) [28.pre]

As discussed for Element [27], the authentication cryptogram is based on a seed value which is secret and shared by the card/device and the EPIC payment processing authority ("wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority"). *Supra* Element [27]; EX1003, ¶140.

ii) [28.a][6]

As discussed for Elements [1.j] and [27], the authentication cryptogram is combined with the EPIC static payment card identifying number and together provided to the merchant rather than the issuer supplied payment information, but the seed value is not exchanged when performing the transaction. *Supra* Elements [1.j], [27]; EX1003, ¶141.

[6] Petitioner assumes that the claimed "preforming" is intended to read "performing." *See* Section XII. Patent Owner agreed to this construction in district court. EX1042, 3.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 47 of 104

19. Claim 29

i) [29.pre], [29.a]

Supra Elements [1.a] (describing "an electronic device operable to receive a priming operation"), [1.e] (describing "wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user").

ii) [29.b]

Supra Element [1.b].

iii) [29.c]

Supra Elements [1.d] (reciting "a near field communications (NFC) interface coupled to the processor"), [1.f] (describing receiving a payment request via the NFC interface ("and operable to receive a payment request associated with the payment transaction")).

iv) [29.d]

Supra Element [1.c].

v) [29.e]

Supra Elements [1.e] (describing how an authentication cryptogram is generated upon receipt of a payment request, and thus the request "reflect[s] device readiness"), [1.g] (describing the display of the payment request on the user's device ("wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request") which also contains an image

representing a selected credit card for the transaction ("and an image representing at least one selected issued payment account").

vi) [29.f]

Supra Elements [1.h] (describing the dynamic generation of a limited-use cryptogram ("wherein the electronic device is operable to dynamically generate limited-use payment information")), [1.i] (describing the generation of the cryptogram based on a temporal signal such as the sequence value/sequential number of the attempted use of the device ("based on a sequential counter count from the electronic device")).

vii) [29.g]

As discussed for Element [1.pre], Gomez describes that the payment card has a static payment card identifying number, which identifies the specific card/device ("static device-specific user account information") corresponding to the customer's EPIC account, but may be linked to multiple actual credit/debit card accounts. EX1007, 2:19-39, 20:1-37; Element [1.pre]; EX1003, ¶148. Gomez further discloses that the static payment card identifying number is stored on the card, explaining that "[a]n exemplary EPIC payment card 442 includes a re-writable magnetic stripe on which the payment card identifying number is encoded in the account number field." EX1007, 5:50-57; EX1003, ¶148. A POSITA would have understood that when the Gomez-Amacker-Casey device is implemented as a larger,

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 49 of 104

touch-screen device (e.g., a mobile phone), as contemplated by Amacker (*see* Element [1.a]), the EPIC static payment card identifying number would be stored on the electronic device ("wherein the electronic device is operable to store a static device-specific user account information"). EX1003, ¶148; Section IX.A.4; EX1008, 8:21-33 (describing storage of payment numbers on Amacker's electronic device).

viii) [29.h]

Supra Elements [1.j]-[1.k] (describing the user device's transmission of the authentication cryptogram and EPIC static payment card identifying number via the NFC interface to the NFC terminal recipient to be used in the transaction in place of the card issuer supplied payment information/actual credit card account number associated with the selected credit card account).

ix) [29.i]

Supra Element [1.l] (describing how a receipt is received, reflecting a completed status of the transaction, in response to the transmission of the card identifying number and cryptogram).

x) [29.j]

Supra Element [1.m] (reciting similar limitation).

20. Claim 30

Supra Element [2] (reciting similar limitation).

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 50 of 104

21. Claim 31

Supra Element [29.g] (the EPIC static payment card identifying number is "static device account information" because it (a) is "static" (b) corresponds to a particular "device" (i.e., the static payment card identifying number identifies the specific card/device associated with an EPIC account), and (c) provides EPIC "account information" because it corresponds to the user's EPIC account).

22. Claim 32

A POSITA would have understood that the Gomez-Amacker-Casey device's static payment card identifying number ("static device account information"), which is a number identifying the user's EPIC account ("comprises a static device account number"), is also "unique to the electronic device" because Gomez describes the card identifying number as identifying the specific card/device, i.e., it is unique to that device. EX1007, 2:19-39, 20:1-37; EX1003, ¶154. While Gomez explains that a given EPIC card/device may be linked to multiple *actual* credit/debit card accounts, the card identifying number still identifies a specific *EPIC* card and corresponds to the customer's EPIC account. EX1007, 2:19-39, 20:1-37; EX1003, ¶154. Thus, even though a user has the ability to link one EPIC card to multiple actual credit/debit card accounts, the EPIC card itself is still uniquely identified by the static payment card identifying number. EX1003, ¶154.

23. Claim 33

Gomez discloses that "[a]n exemplary EPIC payment card 442 includes…[a] payment card identifying number…encoded in the account number field, …[and] the payment card expiration date [which] is encoded in the expiration date field." EX1007, 5:50-60, 11:19-27, 12:41-44, 13:34-50. Gomez further explains that "[i]n some embodiments, a 19-digit payment card identifying number may be represented by the 16-digit account number field along with the 3-digit security code field." *Id.*, 13:56-61. In other embodiments, "the expiration date field may also be used to represent a portion of the payment card identifying number." *Id.*, 13:61-63. Gomez describes sending this entire static payment card identifying number ("static device account information"), which includes the static expiration date field ("further comprises a static device account expiration date"), to the merchant's NFC terminal during a transaction. *Id.*, 13:45-14:2; EX1003, ¶155.

24. Claim 34

Supra Element [1.i] (temporal signal may be the sequence value/sequential number of the attempted use/transaction of the device).

25. Claim 36

i) [36.pre]

As discussed for Element [1.h], the device's processor dynamically generates an authentication cryptogram ("the electronic device is further operable to

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 52 of 104

dynamically generate the limited-use payment information"). Element [1.h]; EX1003, ¶157.

As discussed for Elements [1.g] and [1.j], in the Gomez-Amacker-Casey combination, the user manually selects the actual credit card they wish to use in the transaction ("information: from said user" and "information associated with said selected, issued payment account"). Elements [1.g], [1.j]; Section IX.A.4; EX1003, ¶158. As discussed for Elements [1.f]-[1.g], a user manually approves a transaction by clicking a button on the payment request display (also "information: from said user"), and as discussed for Element [1.e], the authentication cryptogram in the Gomez-Amacker-Casey combination is generated only upon approval of the payment request. Elements [1.e]-[1.g]; EX1003, ¶158. As discussed for Element [1.h], the authentication cryptogram is then generated based on the seed value, which is both unique to the device ("information associated with said electronic device") and a secret shared only between the device and the EPIC payment processing authority ("at least one secret"). Element [1.h]; EX1003, ¶158.) The seed value used in generation of the authentication cryptogram may further include, in addition to a randomized bit string that is unique to the payment card, "non-random customer specific information, such as a unique customer key." EX1007, 7:34-39. A POSITA would have understood that this unique customer key is also secret ("at least one secret") because as described for Element [27], the information included in the seed

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 53 of 104

value must be secret in order to prevent fraudulent transactions. Element [27]; EX1003, ¶158.

Thus, the generation of the authentication cryptogram ("limited-use payment information") is "based on a shared information: from said user" (manually selected credit card and manual acceptance of request), "information associated with said electronic device" (seed value), "information associated with said selected, issued payment account" (manually selected credit card), "and at least one secret" (the randomized portion of the seed value and additional secret unique customer key that may be incorporated in the seed value). EX1003, ¶159.

ii) [36.a]

As discussed for Elements [27] and [28.pre], the seed value (containing randomized bits) is shared by both the user's electronic device and the EPIC payment processing authority. Elements [27], [28.pre]; EX1003, ¶160. The unique customer key, which may be part of the seed value, would have been shared by both the user's electronic device and the EPIC payment processing authority for the same reasons, so that the EPIC payment processing authority may recreate a reference authentication cryptogram. EX1003, ¶160. The acceptance of the request and the manually selected credit card would both also be shared by the electronic device and the EPIC payment processing authority. *Id.*, ¶160. Both the acceptance of the request and the manually selected credit card are user inputs to the device and are

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 54 of 104

thus known to the device. *Id.*, ¶160. Further, when payment information is sent to the merchant's NFC terminal and ultimately the EPIC authentication server, the EPIC authentication server is receiving information that the request has been accepted and that a certain credit card is to be used in the transaction. *Id.*, ¶160. Accordingly, the "shared information" discussed in for Element [36.pre] is collectively "shared by both the electronic device and a payment processing authority." *Id.*, ¶160.

26. Claim 37

Supra Elements [27] (reciting similar limitation and describing generation of cryptogram based on secret seed value), [36.pre]-[36.a] (describing how seed value used in generating the cryptogram may include multiple "payment processing authority secrets," i.e., a randomized component and a non-random unique customer key).

27. Claim 38

Supra Element [27].

B. Ground 1B: Gomez, Amacker, Casey, and Law Render Claims 3-6, 17-26, 35, and 39-72 Obvious

1. Law

Law is entitled to the filing date of the Law Provisional because (1) at least one claim of Law is supported by the Law Provisional, and (2) the subject matter relied upon in Law is also described by the Law Provisional. EX1003, ¶86. The

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 55 of 104

following chart demonstrates the enabling support found in the Law Provisional for claim 4 of Law. The analysis for each claim element in the Grounds also includes supporting citations to the Law Provisional.

Law Claim 4	**Exemplary Disclosures of the Law Provisional (EX1033)**
4. A computer-implemented method comprising:	EX1033, ¶¶[0033]-[0034], [0063].
registering a funding card comprising storing a funding card number;	EX1033, ¶¶[0050]-[0053], [00110], FIG. 10.
receiving a message from a mobile device indicating a desire to make a payment using the registered funding card;	EX1033, ¶¶[[0054], 0066]-[0072], [0079].
computing data for a virtual card, wherein the data for the virtual card comprises a virtual card number that is different than the funding card number;	EX1033, ¶¶[0072]-[0073], [0076]-[0079], [00100], [00113]-[00114].

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 56 of 104

Law Claim 4	Exemplary Disclosures of the Law Provisional (EX1033)
storing the data for the virtual card in association with the funding card number;	EX1033, ¶¶[0051]-[0052], [00109]-[00114].
sending information related to the data for the virtual card to the mobile device;	EX1033, ¶¶[0051]-[0052], [0062], [0070]-[0073], [00111]-[00113].
receiving a first payment authorization request from a merchant or a merchant acquirer, the first payment authorization request comprising the data for the virtual card and a requested payment amount;	EX1033, ¶¶[0054], [0084]-[0088].
retrieving the funding card number based on the data for the virtual card;	EX1033, ¶¶[0054], [0086]-[0091].
sending a second payment authorization	EX1033, ¶¶[0054], [0087]-[0093].

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 57 of 104

Law Claim 4	Exemplary Disclosures of the Law Provisional (EX1033)
request to a funding card issuer, the second payment authorization request comprising the funding card number and the requested payment amount;	
receiving a payment authorization response from the funding card issuer; and	EX1033, ¶¶[0055], [0087]-[0093].
sending the payment authorization response to the merchant or the merchant acquirer.	EX1033, ¶¶[0048], [0087]-[0093].

Law describes "facilitating a payment transaction at a merchant location using a virtual card on a mobile device." EX1032, ¶[0002]; EX1033, ¶[0001]. Law describes that an "NFC-enabled mobile device can be equipped with a 'software payment card' … application running inside the mobile device. The software payment card uses the compatible contactless communication capabilities of the

device to interact with contactless-enabled POS terminal to facilitate payment transactions." EX1032, ¶[0062]; EX1033, ¶[0034]. Law explains that when a funding card is used in a payment transaction, the "transaction…includes dynamic data from the card to securely authenticate the payment credential," where the "dynamic data changes values every time the credential is used." EX1032, ¶[0069]; EX1033, ¶[0041].

Law further describes a funding card identifier, which is a static number that is acquired by and stored on the mobile device and used in place of a user's actual credit card number in transactions. EX1032, ¶[0082]; EX1033, ¶[0052]. Law explains that, when registering the funding card, "the user enters in (e.g. types in) card details into the mobile device," which is then sent along with a "user provided PIN and the mobile device ID to the payment gateway server." EX1032, ¶[0082]; EX1033, ¶[0052]. "[T]he payment gateway server computes a funding card identifier which identifies the given funding card," "stores the funding card identifier in association with the funding card details, mobile device ID and PIN," and "sends the funding card identifier to the mobile device for storage." EX1032, ¶[0082]; EX1033, ¶[0052]. Law explains that "the funding card identifier is a value that is different from the PAN, expiry date or static security code of the funding card." EX1032, ¶[0082]; EX1033, ¶[0052]. "The mobile device stores the funding card identifier, which it sends to the payment gateway server to indicate a specific funding

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 59 of 104

card." EX1032, ¶[0082]; EX1033, ¶[0052]. Law explains that "[i]f multiple funding cards are registered, each of the associated funding card identifiers are stored on the mobile device," with associated "details of each individual funding card…stored on the payment gateway server." EX1032, ¶[0083]; EX1033, ¶[0053].

2. Gomez-Amacker-Casey-Law Combination

A POSITA would have beneficially applied the teachings of Law to further modify the Gomez-Amacker-Casey mobile device to include multiple improvements. EX1003, ¶¶84-88, 164.

First, a POSITA would have modified the Gomez-Amacker-Casey device such that the static payment number transmitted to the POS terminal along with an authentication cryptogram during a transaction not only includes the customer's EPIC account information (as taught by Gomez), but also includes information identifying the actual credit/payment card selected for the transaction (as taught by Law). EX1003, ¶165.

Gomez describes an EPIC card having a static payment card identifying number corresponding to and identifying the customer's EPIC account, which is linked to multiple actual credit/debit cards. EX1007, 2:19-39, 20:1-37. Gomez also describes how a user may manually choose which of the actual credit/debit cards to use at the moment of a transaction. *Id.*, 20:30-42. However, Gomez does not explicitly disclose how the selected actual credit/debit card payment information is

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 60 of 104

communicated to the merchant and EPIC authentication server during a transaction. A POSITA would have thus been motivated to consider Law's disclosure of generating a funding card identifier based on funding (payment) card details, storing the funding card identifier on the mobile device and at the payment gateway server (i.e., a payment processing authority), and sending the funding card identifier from the mobile device to the payment gateway server to indicate which funding card of multiple registered funding cards is to be used in a transaction. EX1003, ¶166; EX1032, ¶¶[0082]-[0083]; EX1033, ¶¶[0052]-[0053]. A POSITA would have understood the benefits of Law's method of sharing funding/payment card details because Law explains that the funding card identifier is linked to a specific funding card's PAN (primary account number), expiration date, and security code, but is designed as a randomized code to prevent fraudulent use if intercepted by an adversary. EX1003, ¶166; EX1032, ¶[0082]; EX1033, ¶[0052].

A POSITA would have been motivated to incorporate Law's funding card identifier feature so there is a static EPIC account funding card identifier for each actual credit/debit card, such that the static EPIC account funding card identifier incorporates both a component identifying the EPIC account information (like Gomez's static payment card identifying number) and a component identifying the actual credit/debit card (like Law's funding card identifier). EX1003, ¶167. In the predictable combination, a static EPIC account funding card identifier would be

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 61 of 104

generated when an actual credit/debit card is registered with a user's EPIC account, such that (1) a user enters the actual card details (PAN, expiration date, and security code) into the mobile device along with a user-provided PIN, (2) the mobile device sends that information and a mobile device ID to the EPIC payment processing authority, and (3) the EPIC payment processing authority returns a static EPIC account funding card identifier that captures both the EPIC account information and a static, secret funding identifier that identifies the particular credit/debit card. *Id.*, ¶167; EX1007, 2:19-39, 20:1-37; EX1032, ¶[0082]; EX1033, ¶[0052]. A POSITA would have found it obvious to implement the Gomez-Amacker-Casey-Law device such that it transmits the static EPIC account funding card identifier (rather than Gomez's static payment card identifying number) and authenticated cryptogram to the merchant's POS terminal (and ultimately a payment processing authority). EX1003, ¶167; EX1007, 7:49-8:82. Such a modification would have allowed the payment processing authority to receive the EPIC account information, funding card identifier (and thus actual credit/debit card information), and the authenticated cryptogram necessary to complete the transaction. EX1003, ¶167.

Second, a POSITA would have further modified the combined device such that the authentication cryptogram is generated not only based on a seed value and temporal signal value, but also based on secret information associated with the actual credit/debit card selected for the transaction. EX1003, ¶168. Gomez explains that

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 62 of 104

when "generating the authentication cryptogram…the seed value and the temporal signal value are combined to form a 'message'" which is then "processed…using a cryptographic hash function, to generate a message 'digest.'" EX1007, 8:25-51. The "message digest is encoded using an alpha-numeric code to form the authentication cryptogram." *Id.*, 8:52-9:11. Gomez explains that "a message that is 'based upon' certain information (e.g., a seed value is not necessarily based only upon the certain information, but may also be based upon other information." *Id.*, 22:15-18. Thus, a POSITA would have been motivated to consider other implementations in which additional information is used to form the message used to generate the authentication cryptogram. EX1003, ¶168. Both Law and Amacker describe sending dynamic/limited-use information (similar to Gomez's limited-use authentication cryptogram) that is based on secret information associated with the actual credit/debit card selected for the transaction. *Id.*, ¶168. For example, Law describes that, when a "contactless funding card credential is used to facilitate a payment transaction, the transaction most often includes dynamic data…[that] changes values every time the credential is used." EX1032, ¶[0069]; EX1033, ¶[0041]; *see also* EX1032, ¶[0070]; EX1033, ¶[0042]. Further, Law describes that a mobile device may compute "discretionary data," which is itself "dynamic data," based on digits of the funding card PAN and other secret information included in the registration response associated with the registration of a specific funding card.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 63 of 104

EX1032, ¶¶[0142]-[0155]; EX1033, ¶¶[00109]-[00122]. Amacker similarly discloses generating limited-use information for a transaction associated with a specific payment card stored on the mobile device. EX1008, 8:16-33, 11:42-57. Accordingly, a POSITA would have been motivated to implement the Gomez-Amacker-Casey-Law combination such that the authentication cryptogram is also based on secret information associated with the actual credit/debit card selected for the transaction (e.g., the funding card identifier or similar information). EX1003, ¶168.

Finally, a POSITA would have recognized that applying the teachings of Law and Amacker to the Gomez-Amacker-Casey combination 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, ¶169. *KSR*, 550 U.S. at 416.

3. Claim 3

i) [3.pre], [3.a], [3.b]

As discussed above (Section IX.B.2), in the Gomez-Amacker-Casey-Law combination, when an actual credit/debit card is registered before a transaction takes place ("prior to the priming operation"), the actual credit/debit card information is sent ("transmitting the issued payment information") along with a user PIN and mobile device ID to the EPIC payment processing authority ("for receipt by a

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 64 of 104

payment processing authority"), and the EPIC payment processing authority returns a static EPIC account funding card identifier ("in response to said transmitting issued payment information, receiving a static device account information"). EX1003, ¶170; EX1007, 2:19-39, 20:1-42; EX1032, ¶¶[0082]-[0083]; EX1033, ¶¶[0052]-[0053]. A POSITA would have understood that the static EPIC account funding card identifier would have been "unique to the electronic device" because it would contain parts similar to Gomez's static payment card identifying number, which Gomez describes as unique to the EPIC device, and Law's funding card identifier, which Law describes as unique to a mobile device since it is generated based on a mobile device ID. EX1007, 2:19-39, 20:1-37; EX1032, ¶[0082]; EX1033, ¶[0052]; *see also supra*, Element [32] (describing uniqueness of static payment card identifying number); EX1003, ¶170.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 65 of 104

4. Claim 4

i) [4.pre], [4.a][7], [4.b][8]

As discussed above (Section IX.B.2), in the Gomez-Amacker-Casey-Law combination, the authentication cryptogram ("limited-use payment information") and static EPIC account funding card identifier ("static device account information") for a selected credit/debit card would be combined and sent together ("transmitting said combined payment information") by the mobile device to the POS terminal. EX1003, ¶171; EX1007, 7:49-8:82; EX1032, ¶[0082]; EX1033, ¶[0052]. This combined payment information would be sent "in place of the issued payment account information" (i.e., in place of the actual selected credit/debit card information) for the same reasons as discussed for Element [1.j]. *Supra* Element

[7] Petitioner assumes the claimed "reduce" is intended to read "produce" as recited in similar claims, e.g., Element [18.a]. *See* Section XII. The word "produce" appears correctly in prosecution. EX1002, 22 (final claim 4 is original claim 34), 1084 (newly presented claim 34). In district court, Patent Owner agreed to construe "reduce" to mean "produce." EX1042, 2.

[8] Petitioner assumes that "via said NFC for receipt by an NFC recipient" is intended to read "via said NFC [interface] for receipt by an NFC receipt." *See* Section XII. Patent Owner agreed to this construction in district court. EX1042, 2.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 66 of 104

[1.j]; EX1003, ¶171. The combined payment information would also be sent "via said NFC [interface] for receipt by an NFC recipient" for the same reasons as discussed for Element [1.k]. *Supra* Element [1.k]; EX1003, ¶171.

ii) [4.c]

Supra Element [1.l].

5. Claim 5[9]

Supra Element [27].

6. Claim 6

Supra Element [28.a].

7. Claim 17

i) [17.pre], [17.a], [17.b]

Supra Elements [3.pre]-[3.b].

8. Claim 18

i) [18.pre], [18.a], [18.b], [18.c]

Supra Elements [4.pre]-[4.c].

---

[9] Petitioner assumes the claimed "Lather" is intended to read "further" as recited in similar claims, e.g., Element [19]. *See* Section XII. The word "further" appears correctly in prosecution. EX1002, 22 (final claim 5 is original claim 39), 1086 (newly presented claim 39). In district court, Patent Owner agreed to construe "Lather" to mean "further." EX1042, 3.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 67 of 104

9. Claim 19

Supra Element [27].

10. Claim 20

Supra Element [28.a].

11. Claim 21

Supra Element [27].

12. Claim 22

Supra Element [28.a].

13. Claim 23

i) [23.pre], [23.a], [23.b]

As discussed above (Section IX.B.2), in the Gomez-Amacker-Casey-Law combination, when an actual credit/debit card is registered before a transaction takes place ("prior to the priming operation"), the actual credit/debit card information is sent ("transmitting the issued payment information") along with a user PIN ("user information") and mobile device ID ("device-specific information") to the EPIC payment processing authority, which returns a static EPIC account funding card identifier ("in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information"). EX1003, ¶181; EX1007, 2:19-39, 20:1-42; EX1032, ¶¶[0082]-[0083]; EX1033, ¶¶[0052]-[0053]. A POSITA would have understood that the static EPIC account funding card identifier would have been

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 68 of 104

"payment processing authority supplied secret information" because it is supplied by the EPIC processing authority, and because Law similarly describes a funding identifier as known to only the mobile device and payment processing authority, and not intended to be disclosed to other parties/systems (e.g., adversaries). EX1032, ¶[0082]; EX1033, ¶[0052]; EX1003, ¶181.

14. Claim 24

Supra Elements [3.pre]-[3.b] (describing how the static EPIC account funding card identifier ("payment processing authority supplied secret information") is "static device account information").

15. Claim 25

As discussed above (Section IX.B.2), in the Gomez-Amacker-Casey-Law combination, a static EPIC account funding card identifier of the mobile device represents and encapsulates ("static device account information comprises") certain information associated with the user-selected actual credit/debit card for a particular transaction, including the card's static PAN (primary account number) ("static device account number") and the card's expiration date ("static device-specific expiration date"). EX1003, ¶183; EX1032, ¶[0082]; EX1033, ¶[0052].

16. Claim 26

As discussed for Element [25], a static EPIC account funding card identifier represents and encapsulates information such as a PAN (primary account number)

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 69 of 104

that is associated with the user-selected actual credit/debit card on the mobile device. *Supra* Element [25]; EX1003, ¶184; EX1032, ¶[0082]; EX1033, ¶[0052]; Section IX.B.2.

17. Claim 35

Supra Elements [3.pre]-[3.b].

18. Claim 39

i) [39.pre]

Supra Elements [1.pre] and [29.pre] (describing method and system "for completing a payment transaction"), [1.b] (describing an "electronic device" for completing the transaction).

ii) [39.a]

Supra Element [1.b].

iii) [39.b][10]

The predictable combination "includes a processor 342 coupled to a memory 344" ("a memory coupled to the processor"). EX1007, 10:34-38, FIG. 7. As discussed for Element [1.g], in the resulting combination, a user may manually select the actual credit card they wish to use during the transaction ("information associated with use of an issued payment account") from a list displayed on a payment request

[10] There is no antecedent basis for "the payment authority information." *See* Section XII. Petitioner nevertheless explains how this feature is disclosed by the prior art.

display of the electronic device. Element [1.g]; EX1003, ¶188. A POSITA would have understood that this information associated with the actual card (e.g., a corresponding static EPIC account funding card identifier) would have been stored in memory in order to access and display the available credit card accounts for each payment request ("wherein the memory is operable to store information associated with use of an issued payment account"). EX1003, ¶188.

As discussed for Elements [3.pre]-[3.b], the Gomez-Amacker-Casey-Law device stores for each card a payment processing authority-supplied static EPIC account funding card identifier which is secret ("wherein the payment authority information comprises a secret information"). Elements [3.pre]-[3.b]; EX1003, ¶189.

iv) [39.c]

Supra Element [29.c].

v) [39.d]

Supra Element [1.c] (describing how a touch-screen display ("user interface") is "coupled to the processor"), [1.g] (describing display features of the touch-screen display that allow a user to interact with the device through the display ("user interface").

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 71 of 104

vi) [39.e]

As discussed for Element [10.b], the user's device in the predictable combination includes a fingerprint/biometric sensor and a touch sensor on the touch-screen display (each sensor a "user input device") to receive fingerprints and PINs, respectively. as part of a priming operation. *Supra* Element [10.b]; *see also infra* Element [39.f.i]. Gomez explains that these sensors are both user-credential input devices and coupled to the processor ("a user input device coupled to the processor"). EX1007, 10:34-38; EX1003, ¶192.

vii) [39.f]

A POSITA would have understood that "said processor is operable to" perform the device's tasks in performing a transaction in the Gomez-Amacker-Casey-Law combination, and thus would be operable to perform the following steps in Elements [39.f.i]-[39.f.v]. EX1003, ¶193.

viii) [39.f.i]

Supra Elements [1.a] (describing a "priming operation"), [1.e] (describing similar limitation to Element [39.f.i]).

ix) [39.f.ii]

Supra Element [1.g].

x) [39.f.iii]

Supra Element [1.g].

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 72 of 104

xi) [39.f.iv]

As discussed for Elements [1.h]-[1.i], the mobile device dynamically generates an authentication cryptogram ("dynamically generate a limited-use payment information") based on a temporal signal value such as the sequential number of attempted use of the device ("based on a per-transaction sequential parameter originating from the electronic device"). *Supra* Elements [1.h]-[1.i]; EX1003, ¶197. As discussed above (Section IX.B.2) for the Gomez-Amacker-Casey-Law combination, a POSITA would have found it obvious to implement the device such that the authentication cryptogram is also generated based on secret information associated with the actual credit/debit card a user selects for the transaction ("dynamically generate a limited-use payment information based on…secret information associated with a selected issued payment account"). EX1007, 8:25-9:11, 22:15-18; EX1008, 8:16-33, 11:42-57; EX1032, ¶¶[0069]-[0070], [0142]-[0155]; EX1033, ¶¶[0041]-[0042], [00109]-[00122]; EX1003, ¶197.

xii) [39.f.v]

Supra Elements [4.pre]-[4.b] (describing the transmission from the electronic device to the POS terminal via the NFC interface ("cause the transmission, via said NFC interface") of a combination of ("a payment information combination comprising") both the authentication cryptogram ("the dynamically generated limited-use payment information") and the static EPIC account funding card

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 73 of 104

identifier ("and said payment authority information") for receipt by the NFC-enabled POS terminal ("for receipt by an NFC recipient")).

xiii) [39.g]

Supra Element [4.c] (reciting similar limitation).

xiv) [39.h]

Supra Elements [29.j] (describing how touch-screen display is "operable to provide an indication of the status information"), [39.d] (touch-screen display provides a "user interface").

19. Claim 40

Supra Elements [3.pre]-[3.b] (describing how the payment processing authority-supplied static EPIC account funding card identifier ("payment authority information" is unique to the mobile device ("comprises information that is unique to the electronic device")).

20. Claim 41

As discussed above (Section IX.B.2) for the Gomez-Amacker-Casey-Law combination, and above for Element [23.b], the static EPIC account funding card identifier ("payment authority information") is secret information shared by the mobile device and the EPIC payment processing authority. EX1003, ¶202; Element [23.b].

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 74 of 104

21. Claim 42[11]

Supra Element [25] (describing how the static EPIC account funding card identifier ("processing authority information") "comprises a static device account number").

22. Claim 43

Supra Element [25] (describing how the static EPIC account funding card identifier ("processing authority information") represents and encapsulates certain information associated with the user-selected actual credit/debit card for a particular

[11] There is no antecedent basis for "the processing authority information." *See* Section XII. Petitioner assumes, based on the use of this term interchangeably with "payment authority information" in claims depending from claim 39, that "processing authority information" is intended to refer to "payment authority information." This assumption is consistent with Patent Owner's infringement contentions, which identify the same information for both "payment authority information" and "processing authority information." *Compare* EX1043, 97, 108-109, 118, 120-122 (identifying DPAN, associated expiration date, and keys as "payment authority information"), *with id.*, 109-110, 115 (identifying same information as "processing authority information"). Petitioner makes the same assumption for Elements [43]-[44], [46]-[48], and [55.b]-[55.c].

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 75 of 104

transaction, including the card's expiration date ("further comprises a static device account expiration date")).

23. Claim 44

As discussed for Elements [3.pre]-[3.b], the Gomez-Amacker-Casey-Law device transmits the actual credit/debit card information ("transmission of issued payment account information") along with a user PIN and mobile device ID to the EPIC payment processing authority, and in return receives a corresponding static EPIC account funding card identifier ("in response thereto, to receive the processing authority information"). *Supra* Elements [3.pre]-[3.b]; Section IX.B.2; EX1003, ¶205. A POSITA would have understood that the device's "processor is operable to cause the" transmission of the payment information because the device's processor would be operable to perform the device's tasks associated with performing a transaction in the Gomez-Amacker-Casey-Law combination. EX1003, ¶205.

24. Claim 45

As discussed for Element [2], the authentication cryptogram ("dynamically generated limited-use payment information") is a cryptogram number ("comprises a cryptogram number"). *Supra* Element [2]; EX1003, ¶206. As discussed for Elements [4.pre]-[4.b], [39.f], and [39.f.v], the device's processor is operable to cause transmission from the device to the POS terminal via the NFC interface ("the processor is operable to cause transmission, via said NFC interface") of a

combination of ("of a payment information combination comprising") of both the authentication cryptogram ("the dynamically generated limited-use payment information") and the static EPIC account funding card identifier ("and at least a portion of said payment authority information") corresponding to a selected actual credit/debit card in order to perform the payment transaction ("in connection with the payment transaction"). *Supra* Elements [4.pre]-[4.b], [39.f], [39.f.v]; Section IX.B.2; EX1003, ¶206. As further discussed for Elements [4.pre]-[4.b], this combined information is transmitted in place of the payment information associated with the actual credit/debit card selected for the transaction ("in place of at least a portion of the payment information associated with said selected issued payment account"). *Supra* Elements [4.pre]-[4.b]; EX1003, ¶206.

25. Claim 46

Supra Element [44].

26. Claim 47

Supra Element [42].

27. Claim 48

Supra Element [43].

28. Claim 49

As discussed for Elements [1.c] and [39.d], the Gomez-Amacker-Casey-Law device's touch screen display ("user interface") has a display ("wherein said user

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 77 of 104

interface comprises a display"). *Supra* Elements [1.c], [39.d]; EX1003, ¶210. As discussed for Element [39.e], the touch-screen display includes touch sensors ("user input device") through which user input, e.g., a PIN, can be received. *Supra* Element [39.e]. A POSITA would have understood that these touch sensors are comprised of a touch panel/screen "positioned in front of or behind the display" ("wherein said user input device comprises a touch panel disposed adjacent to said display"). EX1006, 7:26-29; EX1003, ¶210. As discussed for Elements [10.pre]-[10.b], the device's processor validates an identified/authorized user ("wherein further the processor is operable to identify an authorized user") by determining whether a user's credentials, e.g., a user's PIN input to the touch-screen display, match a known reference credential stored on the device ("by validating a valid user passcode input to the touch panel"). *Supra* Elements [10.pre]-[10.b]; EX1003, ¶210.

29. Claim 50

The Gomez-Amacker-Casey-Law combination discloses "wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display" for the same reasons as discussed for Element [49]. *Supra* Element [49]; EX1003, ¶211. As discussed for Elements [10.pre]-[10.b], the device's processor validates an identified/authorized user ("wherein further the processor is operable to identify an authorized user") by displaying a request for a PIN ("by displaying a security challenge question

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 78 of 104

presented on the display")[12] and determining whether the PIN user input matches a known reference credential ("and receiving a correct user response thereto"). *Supra* Elements [10.pre]-[10.b]; Section IX.A.4 (discussing display of Gomez's user input features on EX1003, ¶211.

30. Claim 51

As discussed for Element [39.e], the user's device in the predictable combination includes a fingerprint/biometric sensor for user input ("wherein said user input device comprises a biometric sensor") which detects the touch of a user's fingerprint on the device's sensor ("operable to detect a user touch of said electronic device"), upon which the processor determines whether the user's fingerprint matches the reference fingerprint credential of an authorized user ("wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch"). *Supra* Element [39.e]; EX1003, ¶212. A POSITA would have understood that to accurately read a fingerprint through a biometric sensor, the user would have to continuously hold their finger to the sensor ("biometric sensing of a continuous user touch") until the fingerprint is fully read. EX1003, ¶212.

[12] In Patent Owner's infringement contentions, Patent Owner interprets a displayed request for a PIN as a "security challenge question." EX1043, 111.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 79 of 104

31. Claim 52

The Gomez-Amacker-Casey-Law combination discloses "wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display" for the same reasons as discussed for Element [49]. *Supra* Element [49]; EX1003, ¶213. As discussed for Element [51], which recites similar limitations, "the processor is operable to identify an authorized user by biometric sensing of a user touch" through a fingerprint/biometric sensor. *Supra* Element [51]; EX1003, ¶213. A POSITA would have found it obvious to integrate the biometric sensor into the touch sensor layer (touch panel) of the touch screen display ("biometric sensing of a user touch at the touch panel") to save space on the display of the mobile device and to arrange the various user input devices (e.g., for fingerprint or PIN input) on the same layer of the display. EX1003, ¶213.

32. Claim 53

The Gomez-Amacker-Casey-Law combination discloses "wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display" for the same reasons as discussed for Element [49]. *Supra* Element [49]; EX1003, ¶214. As discussed for Elements [10.pre]-[10.b], the device's processor validates an identified/authorized user ("wherein further the processor is operable to identify an authorized user") by determining whether a user's fingerprint (input through a fingerprint/biometric

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 80 of 104

sensor) matches a reference fingerprint credential of an authorized user ("by biometric recognition of a valid user identification"). *Supra* Elements [10.pre]-[10.b]; EX1003, ¶214.

33. Claim 54[13]

As discussed above (Section IX.A.4) with respect to the Gomez-Amacker-Casey device, and further for Element [14], user input for the priming operations may be provided through a user motion of the device. EX1006, 7:59-8:3; *supra* Element [14]. Such a user input may be detected through a motion sensing device ("user input device") may include a three-axis accelerometer for providing the measured acceleration or motion data to the device's processor, allowing for the sensing of various types of motion such as velocity, acceleration, rotation, and direction. *Id.* A POSITA would have understood that the motion sensing device's three-axis accelerometer is an array of motion sensors ("wherein said user input device comprises an [array] of motion sensors") since a three-axis accelerometer consists of an array of three individual accelerometers providing simultaneous

[13] Petitioner assumes the claimed "army" is intended to read "array" as recited in similar claims, e.g., Element [71]. *See* Section XII. Furthermore, the word "array" appears correctly in prosecution. EX1002, 22 (final claim 54 is original claim 68), 1094 (newly presented claim 68).

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 81 of 104

measurements in three orthogonal directions. EX1003, ¶215. Gomez discloses that the processor is configured to verify an entered user credential by comparing the credential to a reference credential, and thus a POSITA would have understood that in the combined device, the processor would be able to identify an authorized user by detecting a recognized user motion ("wherein further the processor is operable to identify an authorized user"). EX1007, 9:30-39, 10:47-50; EX1003, ¶215. A POSITA would have also understood that for a motion sensing device (containing an array of motion sensors, as discussed above) that measures changes in velocity, acceleration, rotation, and direction, detection of a recognized user motion involves detecting a recognized change in position of the motion sensor array ("detecting a recognized user displacement of the array of motion sensors"). EX1003, ¶215.

34. Claim 55

i) [55.pre]

A POSITA would have understood that "said processor is operable to" perform the device's tasks associated with performing a transaction in the Gomez-Amacker-Casey-Law combination, and thus would also be operable to perform the following steps in Elements [55.a]-[55.c]. EX1003, ¶216.

ii) [55.a]

As discussed for Element [1.g], in the predictable combination, the device receives a user selection of an actual credit/debit card to be used in the transaction

("receive a user-selection of an issued payment account") via a payment request presented on the touch-screen display ("presented on the user interface"), where the user selects an actual credit/debit card by touching the screen (i.e., providing a user input to the touch sensors of the display) ("received [via] the user input device"). *Supra* Element [1.g]; EX1003, ¶217. As discussed for Element [39.e], the "user interface [is] coupled to the processor." *Supra* Element [39.e]; EX1003, ¶217.

iii) [55.b], [55.c]

As discussed above (Section IX.B.2) for the Gomez-Amacker-Casey-Law combination, and for Elements [4.pre]-[4.b], after a user selects an actual credit/debit card to use in the transaction, the device selects the specific static EPIC account funding card identifier corresponding to that selected card ("responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information"). A POSITA would have known that an actual credit/debit card requires processing by a specific processing authority (e.g., Visa, MasterCard, etc.). *Supra* Elements [4.pre]-[4.b]; EX1003, ¶218. As discussed for Element [39.b], each static EPIC account funding card identifier is stored in memory, and thus the correct identifier would be "select[ed] from the memory." *Supra* Element [39.b]; EX1003, ¶218. As further discussed for Elements [4.pre]-[4.b], the static EPIC account funding card identifier for the selected card is used in place of the actual credit/debit card information ("use at least

a portion of said specific processing authority information in place of at least a portion of the issued payment account information"), combined with the dynamically-generated authentication cryptogram ("to generate a combined payment information"), and sent to the POS terminal "to complete a payment transaction per the input user-selection." *Supra* Elements [4.pre]-[4.b]; EX1003, ¶218.

35. Claim 56

i) [56.pre]

Supra Element [39.pre].

ii) [56.a]

Supra Element [1.b].

iii) [56.b]

Supra Element [39.b].

iv) [56.c]

Supra Element [29.c].

v) [56.d]-[56.h]

Supra Elements [39.d]-[39.h].

36. Claim 57

Supra Element [40].

37. Claim 58

Supra Element [42].

38. Claim 59

Supra Element [43].

39. Claim 60

Supra Element [41].

40. Claim 61

Supra Element [44].

41. Claim 62

As discussed for Element [2], the authentication cryptogram ("dynamically generated limited-use payment information") is a cryptogram number. *Supra* Element [2]; EX1003, ¶238. As discussed for Elements [4.pre]-[4.b], the authentication cryptogram is combined with a static EPIC account funding card identifier associated with a selected actual credit/debit card ("further payment information combination") and sent to the POS terminal in place of the information (i.e., fixed PAN, expiration date, security code) associated with the actual selected credit/debit card information. *Supra* Elements [4.pre]-[4.b]; EX1003, ¶238.

42. Claim 63

Supra Element [44].

43. Claim 64

Supra Element [58].

44. Claim 65

Supra Element [59].

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 85 of 104

45. Claim 66

Supra Element [49] (describing similar limitation with respect to a "touch panel" through which a user provides input, which a POSITA would have understood is a "touch screen interface").

46. Claim 67

Supra Element [50] (reciting similar limitation); [66] (explaining how a touch panel is a "touch screen interface").

47. Claim 68

Supra Element [51].

48. Claim 69

Supra Element [52]; [66] (explaining how a touch panel is a "touch screen interface").

49. Claim 70

The Gomez-Amacker-Casey-Law combination discloses "wherein said user interface comprises a display" for the same reasons as discussed for Element [49]. *Supra* Element [49]; EX1003, ¶246. As discussed for Element [39.e], the device's fingerprint/biometric sensor is used to receive a touch input (e.g., fingerprint) at the mobile device ("wherein said user input device comprises a touch input of the electronic device"). *Supra* Element [39.e]; EX1003, ¶246. The Gomez-Amacker-Casey-Law combination discloses "wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification'

for the same reasons as discussed for Element [53], and as further discussed for that limitation, the user's fingerprint ("valid user identification") is received via a touch sensor input ("via the touch input"). *Supra* Element [53]; EX1003, ¶246.

50. Claim 71

Supra Element [54].

51. Claim 72

i) [72.pre]

Supra Elements [55.pre]-[55.a].

ii) [72.a]

Supra Element [55.b].

iii) [72.b]

Supra Element [62].

C. Ground 1C: Gomez, Amacker, Casey, and Chin Render Claim 13 Obvious

1. Claim 13

To the extent that the fingerprint swipe of the Gomez-Amacker-Casey combination is not found to be a "known user touch gesture," a POSITA would have applied the teachings of Chin to further modify the Gomez-Amacker-Casey mobile device such that a user may enter a tactile pattern on a touch screen, after which the pattern is compared to a stored reference credential (e.g., a known tactile pattern for

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 87 of 104

that given authorized user), to determine whether an authorized user is attempting to use the device. EX1003, ¶¶252-253.

Chin discloses a "method of a mobile device" that includes "recognizing a tactile pattern (e.g., the tactile pattern 106 of FIG. 1) on a touch screen (e.g., the touchscreen 108 of FIG. 1.) without any visual aid on the touch screen 108." EX1044, 4:23-27, FIG. 1. Chin explains that the tactile pattern may be "associated with a security gesture (e.g., may be a user-generated gesture that may be stored in a memory that is internal to the mobile device), permitting access to a set of applications of the mobile device 100 when an association is made between the tactile pattern 106 and the security gesture, and denying access to the set of applications of the mobile device 100 when the association fails to be made between the tactile pattern 106 and the security gesture." *Id.*, 4:27-35. Chin discloses that the tactile pattern may also be an unlocking gesture, such that the mobile device transforms from an initial state to an unlocked state if the tactile pattern matches the stored gesture. *Id.*, 4:11-22.

Thus, Chin discloses that a user may generate a known security/unlocking tactile pattern ("<u>wherein said predetermined user characteristics…comprise a known user touch gesture</u>") that is stored in the phone's memory ("<u>predetermined user characteristics stored within the electronic device</u>") and compared to an entered tactile pattern to determine whether an authorized user is attempting to use the phone

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 88 of 104

(thus unlocking the phone or certain features if the patterns match). EX1003, ¶¶89-91, 254-255.

A POSITA would have been motivated to implement an unlocking mechanism involving a tactile pattern, similar to that disclosed by Chin, as an alternative to entering a PIN. *Id.*, ¶256. Chin describes a prior art "touchscreen mobile device [which] may include a virtual keypad," where "[t]he user may use the virtual keypad to enter a pass code to access information." EX1044, 1:41-44. Chin explains that the "process may be slow and/or cumbersome" if, for example, a user's fingertip is the same size as an area of the virtual keypad or if the virtual keypad does not have a good tactile feel (e.g., not as good as a physical keypad). *Id.*, 1:44-48. Virtual PIN/passcode entry may also be "inconvenient and/or dangerous when an attention of the user is diverted (e.g., walking, working, eating, etc.)" *Id.*, 1:48-51. In addition, "[a] handicapped user (e.g., a sight-impaired person, a person with out fingers or hands, a person with impaired dexterity, etc.) may have difficulty inputting information with the virtual keypad." *Id.*, 1:51-54; *see also* EX1003, ¶256.

A POSITA would have recognized that applying the teachings of Chin to the Gomez-Amacker-Casey combination 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, ¶257. *KSR*, 550 U.S. at 416.

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 89 of 104

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 1-72 of the '634 patent based on the grounds specified in this petition.

Respectfully submitted,

Dated: July 29, 2025

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

CARDWARE EXHIBIT 2025
GOOGLE v. CARDWARE IPR2025-01344
Page 90 of 104

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. 11,620,634 contains, as measured by the word-processing system used to prepare this paper, 13,984 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 29, 2025

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

CERTIFICATE OF SERVICE

I hereby certify that on July 29, 2025, I caused a true and correct copy of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 11,620,634 and supporting exhibits to be served via express mail on the Patent Owner at the following correspondence address of record as listed on Patent Center:

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)

XII. APPENDIX A (CLAIM LISTING)

[1.pre]	A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:
[1.a]	receiving an input at an electronic device, wherein the input comprises a priming operation, 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]	responsive to said priming operation, readying said device to perform a payment transaction by an identified user;
[1.f]	receiving a payment request for the payment transaction at said electronic device;
[1.g]	displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;
[1.h]	dynamically generating, by the processor, limited-use payment information;
[1.i]	wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;
[1.j]	using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account;
[1.k]	transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;
[1.l]	responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and
[1.m]	displaying the status of said payment transaction via said touch-screen display.
[2]	The method of claim 1, wherein the limited-use payment information comprises a cryptogram number.
[3.pre]	The method of claim 2, further comprising:

[3.a]	prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,
[3.b]	in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.
[4.pre]	The method of claim 3 further comprising:
[4.a]	combining said limited-use payment information and said static device account information, to reduce a combined payment information;
[4.b]	transmitting said combined payment information, in place of the issued payment account information, via said NFC for receipt by an NFC recipient; and
[4.c]	receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.
[5]	The method of claim 3, wherein the dynamically generating Lather comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
[6]	The method of claim 5, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.
[7]	The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient.
[8.pre]	The method of claim 7, wherein said readying said device to perform a payment transaction comprises:
[8.a]	identifying said proximity NFC recipient is an NFC payment facility;
[8.b]	successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and
[8.c]	receiving a user approval for performing the payment transaction.
[9.pre]	The method of claim 8, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:
[9.a]	the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and,
[9.b]	disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.

[10.pre]	The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between:
[10.a]	firstly, a user input received via at least one of a set of user input sensors of the electronic device; and,
[10.b]	secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.
[11]	The method of claim 10, wherein said user input received via at least one of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display.
[12]	The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics.
[13]	The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.
[14]	The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user motion of the device.
[15]	The method of claim 1, wherein the input comprising a priming operation is a user input.
[16.pre]	The method of claim 15, wherein said readying said device to perform a payment transaction comprises:
[16.a]	successfully identifying said identified user from said user input; and,
[16.b]	wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and,
[16.c]	wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and,
[16.d]	wherein said user approval for performing the payment transaction further comprises:
[16.e]	visually presenting information of the payment transaction on the touch screen display of said electronic device;
[16.f]	visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,

[16.g]	subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.
[17.pre]	The method of claim 1, further comprising:
[17.a]	prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,
[17.b]	in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.
[18.pre]	The method of claim 17 further comprising:
[18.a]	combining said limited-use payment information and said static device account information, to produce a combined payment information;
[18.b]	transmitting said combined payment information, in place of the issued payment account information said NFC interface for receipt by an NFC recipient; and
[18.c]	receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.
[19]	The method of claim 18, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
[20]	The method of claim 19, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.
[21]	The method of claim 17, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
[22]	The method of claim 21, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.
[23.pre]	The method of claim 1, further comprising:
[23.a]	prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and,
[23.b]	in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.

[24]	The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information.
[25]	The method of claim 24 wherein said static device account information comprises a static device account number and a static device-specific expiration date.
[26]	The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device.
[27]	The method of claim 1, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
[28.pre]	The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and
[28.a]	further wherein the at least one secret information is not exchanged when preforming the payment transaction.
[29.pre]	A system for completing a payment transaction, the system comprising:
[29.a]	an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:
[29.b]	a processor;
[29.c]	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,
[29.d]	a touch-screen display coupled to the processor, and
[29.e]	wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;
[29.f]	wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;
[29.g]	wherein the electronic device is operable to store a static device-specific user account information;

[29.h]	wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;
[29.i]	wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and,
[29.j]	wherein the touch-screen display is operable to display as indication of said status information.
[30]	The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number.
[31]	The system of claim 29, wherein the device-specific user account information comprises static device account information.
[32]	The system of claim 31, wherein the static device account information comprises a static device account number that is unique to the electronic device.
[33]	The system of claim 32 wherein the static device account information further comprises a static device account expiration date.
[34]	The system of claim 32 wherein the sequential counter count is changed per payment transaction.
[35]	The system of claim 34 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information.
[36.pre]	The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected, issued payment account, and at least one secret; and,
[36.a]	wherein said shared information is shared by both the electronic device and a payment processing authority.
[37]	The system of claim 36 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.
[38]	The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.

[39.pre]	An electronic device for completing a payment transaction, the electronic device comprising:
[39.a]	a processor;
[39.b]	a memory coupled to the processor, wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;
[39.c]	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;
[39.d]	a user interface coupled to the processor;
[39.e]	a user input device coupled to the processor; and,
[39.f]	wherein said processor is operable to:
[39.f.i]	responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,
[39.f.ii]	cause the display of information associated with the payment request;
[39.f.iii]	cause the display of an image representing at least one user-selectable issued payment account; and,
[39.f.iv]	dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,
[39.f.v]	cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;
[39.g]	wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and
[39.h]	wherein the user interface is operable to provide an indication of the status information.
[40]	The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device.
[41]	The device of claim 39 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority.

[42]	The device of claim 41 wherein the processing authority information comprises a static device account number.
[43]	The device of claim 42 wherein the processing authority information further comprises a static device account expiration date.
[44]	The device of claim 39 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information.
[45]	The device of claim 39 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account.
[46]	The device of claim 45 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information.
[47]	The device of claim 46 wherein the processing authority information comprises a static device account number.
[48]	The device of claim 47 wherein the processing authority information further comprises a static device account expiration date.
[49]	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel.
[50]	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto.
[51]	The device of claim 39, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch.

[52]	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel.
[53]	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification.
[54]	The device of claim 39, wherein said user input device comprises an army of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.
[55.pre]	The device of claim 39, wherein the processor is operable to:
[55.a]	receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and
[55.b]	responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and
[55.c]	use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.
[56.pre]	An electronic device for completing a payment transaction, the electronic device comprising:
[56.a]	a processor;
[56.b]	a memory coupled to the processor, wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;
[56.c]	a near field communications (NFC) interface coupled to the processor

	and operable to receive a payment request associated with the payment transaction;
[56.d]	a user interface coupled to the processor;
[56.e]	a user input device coupled to the processor; and,
[56.f]	wherein said processor is operable to:
[56.f.i]	responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,
[56.f.ii]	cause the display of information associated with the payment request;
[56.f.iii]	cause the display of an image representing the user-selectable issued payment account; and,
[56.f.iv]	dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and,
[56.f.v]	cause the transmission, via said NFC interface, of a payment information combination comprising, the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;
[56.g]	wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and
[56.h]	wherein the user interface is operable to provide an indication of the transaction status information.
[57]	The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device.
[58]	The device of claim 57, wherein the payment authority information comprises a static device account number.

[59]	The device of claim 58, wherein the payment authority information further comprises a static device account expiration date.
[60]	The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority.
[61]	The device of claim 56, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information.
[62]	The device of claim 56, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account.
[63]	The device of claim 62, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information.
[64]	The device of claim 63, wherein the payment authority information comprises a static device account number.
[65]	The device of claim 64, wherein the payment authority information further comprises a static device account expiration date.
[66]	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface.
[67]	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display.
[68]	The device of claim 56, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device

	and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch.
[69]	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface.
[70]	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification via the touch input.
[71]	The device of claim 56, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.
[72.pre]	The device of claim 56, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and
[72.a]	in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and
[72.b]	is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account.