

**IN THE UNITED STATES PATENT AND
TRADEMARK OFFICE**

**BEFORE THE PATENT TRIAL AND APPEAL
BOARD**

GOOGLE LLC,
Petitioner

v.

CARDWARE INC.,
Patent Owner

U.S. Patent No. 11,620,634
Issued: April 4, 2023

Title: MULTI-FUNCTION SMART
TOKENIZING ELECTRONIC PAYMENT
DEVICE

DECLARATION OF MICHAEL I. SHAMOS, PH.D.

TABLE OF CONTENTS

I.	INTRODUCTION AND QUALIFICATIONS	1
II.	SUMMARY OF MY OPINIONS	4
III.	UNDERSTANDING OF THE GOVERNING LAW	5
	A. Invalidity By Obviousness	5
	B. Relevant Time Period for the Obviousness Analysis.....	7
	C. Materials Considered.....	8
IV.	OVERVIEW OF THE '634 PATENT	8
V.	THE '634 PROSECUTION HISTORY	10
VI.	LEVEL OF ORDINARY SKILL IN THE ART IN THE RELEVANT TIMEFRAME	12
VII.	TECHNOLOGY BACKGROUND.....	14
	A. Cryptographic Hashing	15
	B. Near-Field Communication (NFC) Interfaces	16
	C. Touch Screen Displays.....	18
	D. Static and Limited-Use Numbers	20
VIII.	CLAIM CONSTRUCTION	23
IX.	OVERVIEW OF THE PRIOR ART	23
	A. U.S. Patent 9,600,808 (“Gomez”).....	23
	B. U.S. Patent 8,423,462 (“Amacker”).....	27
	C. U.S. Patent 8,255,323 (“Casey”).....	30
	D. U.S. Patent Publication 2015/0134540A1 (“Law”).....	32
	E. U.S. Patent 7,593,000 (“Chin”).....	37
X.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	39
	A. Ground 1A: Claims 1-2, 7-16, 27-34, and 36-38 of the '634 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre- AIA) by Gomez in view of Amacker and Casey	39
	1. Motivation to Combine Gomez with Amacker and Casey	39

2.	Claim 1	46
i)	[1.pre] A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:.....	46
ii)	[1.a] receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:	47
iii)	[1.b] a processor;	48
iv)	[1.c] a touch-screen display coupled to the processor; and	49
v)	[1.d] a near field communications (NFC) interface coupled to the processor;	49
vi)	[1.e] responsive to said priming operation, readying said device to perform a payment transaction by an identified user;.....	49
vii)	[1.f] receiving a payment request for the payment transaction at said electronic device;.....	50
viii)	[1.g] displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;.....	51
ix)	[1.h] dynamically generating, by the processor, limited-use payment information;	53
x)	[1.i] wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;	53
xi)	[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;	54

xii)	[1.k] transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;	55
xiii)	[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	55
xiv)	[1.m] displaying the status of said payment transaction via said touch-screen display.	57
3.	Claim 2: The method of claim 1, wherein the limited-use payment information comprises a cryptogram number.	57
4.	Claim 7: The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient.	58
5.	Claim 8	58
i)	[8.pre] The method of claim 7, wherein said readying said device to perform a payment transaction comprises:	58
ii)	[8.a] identifying said proximity NFC recipient is an NFC payment facility;	58
iii)	[8.b] successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and	59
iv)	[8.c] receiving a user approval for performing the payment transaction.	59
6.	Claim 9	60
i)	[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:	60

- ii) [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, ...61
 - iii) [9.b] disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed. 62
- 7. Claim 10.....63
 - i) [10.pre] The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: 63
 - ii) [10.a] firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, ...63
 - iii) [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. 63
- 8. Claim 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. 65
- 9. Claim 12: The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics.....65
- 10. Claim 13: The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.....66
- 11. Claim 14: The method of claim 10, wherein said predetermined user characteristics stored within the

	electronic device comprise a known user motion of the device.	67
12.	Claim 15: The method of claim 1, wherein the input comprising a priming operation is a user input.	68
13.	Claim 16.....	68
i)	[16.pre]: The method of claim 15, wherein said readying said device to perform a payment transaction comprises:	68
ii)	[16.a] successfully identifying said identified user from said user input; and, ...	68
iii)	[16.b] wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and, ...	68
iv)	[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, ...	69
v)	[16.d] wherein said user approval for performing the payment transaction further comprises:.....	70
vi)	[16.e] visually presenting information of the payment transaction on the touch screen display of said electronic device;	70
vii)	[16.f] visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and, ...	70
viii)	[16.g] subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.	70

14.	Claim 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.....	71
15.	Claim 28.....	72
i)	[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.....	72
ii)	[28a]: further wherein the at least one secret information is not exchanged when performing the payment transaction.....	73
16.	Claim 29.....	73
i)	[29.pre]: A system for completing a payment transaction, the system comprising:	73
ii)	[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:.....	73
iii)	[29.b] a processor;	74
iv)	[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, ...	74
v)	[29.d] a touch-screen display coupled to the processor, and	74
vi)	[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;.....	74

vii)	[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;	75
viii)	[29.g] wherein the electronic device is operable to store a static device-specific user account information;	75
ix)	[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;	76
x)	[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,.....	77
xi)	[29.j] wherein the touch-screen display is operable to display as indication of said status information.	77
17.	Claim 30: The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number	78
18.	Claim 31: The system of claim 29, wherein the device-specific user account information comprises static device account information.	78
19.	Claim 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.....	78
20.	Claim 33: The system of claim 32 wherein the static device account information further comprises a static device account expiration date.....	79

21.	Claim 34: The system of claim 32 wherein the sequential counter count is changed per payment transaction.	80
22.	Claim 36	80
i)	[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, ...	80
ii)	[36.a] wherein said shared information is shared by both the electronic device and a payment processing authority.....	82
23.	Claim 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.	83
24.	Claim 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.	83
B.	Ground 1B: Claims 3-6, 17-26, 35, and 39-72 of the '634 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Casey, and Law.....	83
1.	Motivation to Combine Gomez with Amacker, Casey, and Law	83
2.	Claim 3	89
i)	[3.pre] The method of claim 2, further comprising:	89
ii)	[3.a] prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and, ...	89
iii)	[3.b] in response to said transmitting issued payment information, receiving a static device	

	account information that is unique to the electronic device.	89
3.	Claim 4.....	90
	i) [4.pre] The method of claim 3 further comprising:	90
	ii) [4.a] combining said limited-use payment information and said static device account information, to reduce a combined payment information:	90
	iii) [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.....	90
	iv) [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.....	91
4.	Claim 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.....	91
5.	Claim 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.	92
6.	Claim 17.....	92
	i) [17.pre] The method of claim 1, further comprising:	92
	ii) [17.a] prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,.....	92
	iii) [17.b] in response to said transmitting issued payment information, receiving a static device	

	account information that is unique to the electronic device.	92
7.	Claim 18	93
	i) [18.pre] The method of claim 17 further comprising:	93
	ii) [18.a] combining said limited-use payment information and said static device account information, to produce a combined payment information;	93
	iii) [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.....	93
	iv) [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.....	93
8.	Claim 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.....	93
9.	Claim 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.	93
10.	Claim 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.....	93
11.	Claim 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.	94
12.	Claim 23	94

i)	[23.pre] The method of claim 1, further comprising:	94
ii)	[23.a] prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and, ...	94
iii)	[23.b] in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.....	94
13.	Claim 24: The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information.	95
14.	Claim 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.	95
15.	Claim 26: The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device.	96
16.	Claim 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.	96
17.	Claim 39.....	96
i)	[39.pre] An electronic device for completing a payment transaction, the electronic device comprising:	96
ii)	[39a] a processor;.....	96
iii)	[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;	97

iv)	[39.c] a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;.....	98
v)	[39.d] a user interface coupled to the processor;.....	98
vi)	[39.e] a user input device coupled to the processor; and,.....	98
vii)	[39f] wherein said processor is operable to:.....	98
viii)	[39.f.i] responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction, ...	99
ix)	[39.f.ii] cause the display of information associated with the payment request;.....	99
x)	[39.f.iii] cause the display of an image representing at least one user-selectable issued payment account; and, ...	99
xi)	[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,.....	99
xii)	[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;.....	100
xiii)	[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	101

xiv)	[39.h] wherein the user interface is operable to provide an indication of the status information.	101
18.	Claim 40: The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device.	101
19.	Claim 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.	101
20.	Claim 42 The device of claim 41 wherein the processing authority information comprises a static device account number.	102
21.	Claim 43: The device of claim 42 wherein the processing authority information further comprises a static device account expiration date.	102
22.	Claim 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.	103
23.	Claim 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.	103
24.	Claim 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.	104

25.	Claim 47: The device of claim 46 wherein the processing authority information comprises a static device account number.	105
26.	Claim 48: The device of claim 47 wherein the processing authority information further comprises a static device account expiration date.	105
27.	Claim 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.	105
28.	Claim 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.	106
29.	Claim 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.	107
30.	Claim 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.	108
31.	Claim 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.	108

32.	Claim 54: The device of claim 39, 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.	109
33.	Claim 55	111
i)	[55.pre]: The device of claim 39, wherein the processor is operable to:	111
ii)	[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	111
iii)	[55.b] responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and	112
iv)	[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.	112
34.	Claim 56	113
i)	[56.pre] An electronic device for completing a payment transaction, the electronic device comprising:	113
ii)	[56.a] a processor;.....	113
iii)	[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;	113

- iv) [56.c] a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; 113
- v) [56.d] a user interface coupled to the processor; 114
- vi) [56.e] a user input device coupled to the processor; and, ...114
- vii) [56.f] wherein said processor is operable to: 114
- viii) [56.f.i] responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction, ...114
- ix) [56.f.ii] cause the display of information associated with the payment request; 114
- x) [56.f.iii] cause the display of an image representing the user-selectable issued payment account; and, ...114
- xi) [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, ...114
- xii) [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; 115
- xiii) [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 115

xiv)	[56.h] wherein the user interface is operable to provide an indication of the transaction status information.	115
35.	Claim 57: The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device.	115
36.	Claim 58: The device of claim 57, wherein the payment authority information comprises a static device account number.	115
37.	Claim 59: The device of claim 58, wherein the payment authority information further comprises a static device account expiration date.	115
38.	Claim 60: The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority.	116
39.	Claim 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.	116
40.	Claim 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.	116
41.	Claim 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.	117
42.	Claim 64: The device of claim 63, wherein the payment authority information comprises a static device account number.	117
43.	Claim 65: The device of claim 64, wherein the payment authority information further comprises a static device account expiration date.	117

- 44. Claim 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. 117
- 45. Claim 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. 117
- 46. Claim 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. 118
- 47. Claim 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.....118
- 48. Claim 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.....118
- 49. Claim 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. 119
- 50. Claim 72 119

i)	[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.....	119
ii)	[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	119
iii)	[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.....	120
C.	Ground 1C: Claim 13 of the '634 Patent is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Casey, and Chin.....	120
1.	Claim 13: The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.....	120
XI.	JURAT	124

I, Dr. Michael I Shamos, declare as follows:

I. INTRODUCTION AND QUALIFICATIONS

1. I have been retained by Google LLC (“Google”) to provide my opinions concerning the validity of claims 1-72 (“Challenged Claims”), constituting all claims of U.S. Patent No. 11,620,634 (“’634 Patent” or the “Patent”) in support of Google’s Petition for Inter Partes Review of the Patent (the “Petition”).

2. I am being compensated at a rate of \$625 per hour for my work in this proceeding and my compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding or in Patent Owner. It is conceivable that I may own investments in mutual funds which themselves own shares in Patent Owner. I have no knowledge of any such holder, which, in any event, would not constitute a material portion of my net worth.

3. A detailed description of my professional qualifications, including a listing of my specialties/expertise and professional activities, is contained in my curriculum vitae, a copy of which is provided as Exhibit 1014. Below is a short summary of my professional qualifications.

4. I have a A.B. degree from Princeton University in Physics (1968), a M.A. degree from Vassar College in Physics (1970), a M.S. degree from American

Declaration of Dr. Michael I Shamos
U.S. Patent No. 11,620,634

University in Technology of Management (1972), a M.S. degree from Yale University in Computer Science (1973), a M. Phil. from Yale University in Computer Science (1974), a Ph.D. from Yale University in Computer Science (1978), and a J.D. degree from Duquesne University (1981).

5. I currently hold the title of Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. I am a member of two departments in that School, the Institute for Software Research and the Language Technologies Institute. I was a founder and Co-Director of the Institute for eCommerce at Carnegie Mellon from 1998-2004 and from 2004-2018 was Director of the eBusiness Technology graduate program in the Carnegie Mellon University School of Computer Science. Since 2018, I have been Director of the M.S. in Artificial Intelligence and Innovation degree program at Carnegie Mellon.

6. I have taught graduate courses at Carnegie Mellon in Electronic Commerce from 1999-present, including eCommerce Technology, Electronic Payment Systems, Electronic Voting, Internet of Things, Ubiquitous Computing, Electronic Payment Systems and eCommerce Law and Regulation, as well as Analysis of Algorithms. Since 2007, I have taught an annual course in Law of Computer Technology. I currently also teach Artificial Intelligence and Future Markets.

7. From 2001-2021, I was a Visiting Professor at the University of Hong Kong, where I taught an annual course in Electronic Payment Systems. This was one of only a handful of graduate courses taught on this subject in the world.

8. I was the Director of Carnegie Mellon's graduate degree program in eBusiness Technology from 1999-2018 and am now a faculty member in the Privacy Engineering degree program at Carnegie Mellon. My course on Law of Computer Technology is required for all students in that program and in the Societal Computing Ph.D. program. My principal role currently is as Director of the graduate program in Artificial Intelligence and Innovation.

9. From 1979-1987 I was the founder and president of two computer software development companies in Pittsburgh, Pennsylvania, Unilogic, Ltd. and Lexeme Corporation.

10. I am an attorney admitted to practice in Pennsylvania and have been admitted to the Bar of the U.S. Patent and Trademark Office since 1981. I have been asked to render opinions in this Declaration as a technical expert. I have not been asked to offer any opinions on patent law in this proceeding.

11. I am a named co-inventor on the following six issued patents relating to electronic commerce: U.S. Patent Nos. 7,330,839, 7,421,278, 7,747,465, 8,195,197, 8,280,773, and 9,456,299.

12. I have previously served as an expert in over 400 cases concerning computer technology. In particular, I have been involved in more than 45 cases involving electronic payment systems.

13. The statements made and opinions provided in this Declaration are based on my own personal knowledge and, if called as a witness, I could and would testify in a manner consistent with this Declaration.

II. SUMMARY OF MY OPINIONS

14. It is my understanding that the following table summarizes the grounds of challenge (“Grounds”) raised in the Petition:

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

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

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

18. After a review of the '634 Patent and the prior art asserted by Petitioner, it is my opinion that the Challenged Claims are invalid for obviousness. My opinions, and the bases therefor, are detailed throughout this Declaration.

III. UNDERSTANDING OF THE GOVERNING LAW

A. Invalidity By Obviousness

19. I understand that obviousness of a claim requires that the claim as a whole be obvious from the perspective of a person of ordinary skill in the relevant art (“POSITA”), at the time of invention. A claim is unpatentable for obviousness under 35 U.S.C. § 103 “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” Obviousness may be based upon a combination of references.

20. If a patented invention is a combination of known elements, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue by considering the teachings of prior art references, the effects of demands known to people working in the field or present in the marketplace, and the background knowledge possessed by a POSITA. Identifying a reason the elements should be combined is important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, was already known. The prior art references themselves may provide a suggestion, motivation,

or reason to combine, but the nexus linking two or more prior art references is sometimes simple common sense.

21. An obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the pertinent art; and (4) any objective indicia of non-obviousness, such as commercial success, long-felt but unresolved need, failure of others, industry recognition, copying, and unexpected results.

22. If a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond their skill.

23. Practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. A POSITA looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. An obviousness analysis therefore considers the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

24. A proper obviousness analysis focuses on what was known or obvious to a POSITA at the time of invention, not to the patentee. Accordingly, any need or

problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

25. Prior art teachings are properly combined if one of ordinary skill, having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

26. I understand that in an *inter partes* review, “the petitioner shall have the burden of proving a proposition of unpatentability,” including a proposition of obviousness, “by a preponderance of the evidence.” 35 U.S.C. §316(e).

B. Relevant Time Period for the Obviousness Analysis

27. I understand that the '634 Patent claims priority to U.S. Provisional Patent Application 61/794,891 (“’891 Provisional”), filed on March 15, 2013. I have been asked, for purposes of this proceeding only, to treat March 15, 2013 as the Critical Date in my analysis. However, my opinions as to the obviousness of claims 1-72 of the '634 Patent would remain substantially unchanged even if a later date were deemed to be the Critical Date and if post-AIA §§ 102 and 103 were to apply. I understand that Petitioner does not concede that any of the

Challenged Claims enjoy priority to the '891 Provisional. However, I have been asked to assume, for purposes of this proceeding only, that pre-AIA 35 U.S. §§ 102 and 103 apply.

28. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the '634 Patent. Unless otherwise stated, my testimony below refers to the knowledge of a POSITA as of the Critical Date, or before. Any annotated Figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the '634 Patent and the prior art discussed below.

C. Materials Considered

29. In forming my opinions, I have reviewed and am familiar with the '634 Patent and its prosecution history, the materials cited herein, and exhibits to the Petition.

IV. OVERVIEW OF THE '634 PATENT

30. The '634 Patent was filed on November 16, 2021 and issued on April 4, 2023. Through a series of continuation and divisional applications and a provisional application, it claims priority to March 15, 2013. The '634 Patent discloses “generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card.” EX1001, Abstract. However, the Challenged

Claims are not drawn to any such device, and do not claim “generating a programmed magnetic field” or any “emulation” of a “standard credit card.”

31. The '634 Patent discloses generating a “limited-duration payment number” for use in a payment transaction. EX1001, 2:28-65, 10:33-12:24, FIG 7. The claims recite, at times, generating a “limited-use payment information” to be used “in connection with the payment transaction in place of issued payment information” and transmitting this information via NFC for use in a payment transaction. FIG. 7 of the Patent is a flowchart illustrating an example process for generating a limited-use number:

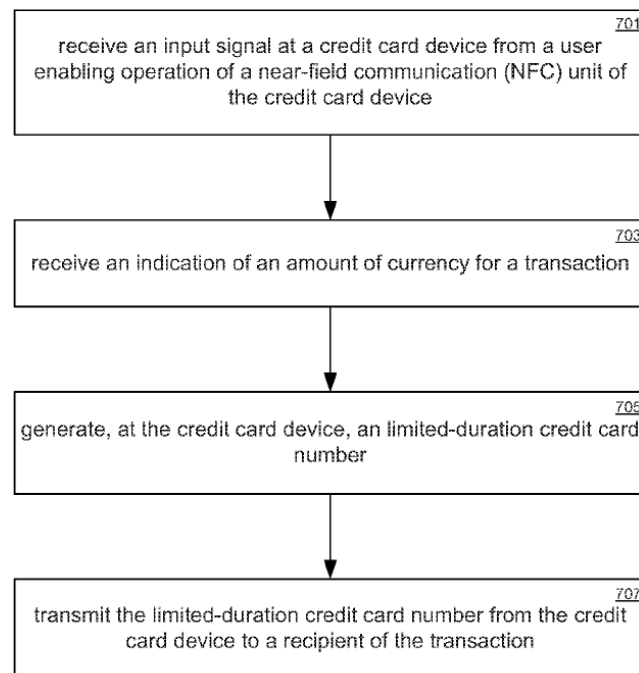


FIG. 7

EX1001, FIG. 7

32. Various other portions of the specification of the Patent (“Specification”) give further details of the generation of a limited-duration

payment number. For example, “[t]he credit card device comprises a real-time clock that is able to produce a cryptographically protected timestamp for each interaction.” EX1001, 10:37-39. “The power source is able to activate the processor unit such that a unique number may be generated by the credit card device and verified by the credit authority according to the timestamp and the transmitted user information.” *Id.*, 10:39-43. “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, a finite number of transactions, or may be limited to a specified period of time—e.g., 2 minutes, 10 minutes, 3 hours—after which time that particular limited-duration number would become invalid.” *Id.*, 10:48-53.

V. THE ’634 PROSECUTION HISTORY

33. I have reviewed the prosecution history of the ’634 Patent (EX1002). On November 16, 2021, Applicant filed continuation application 17/528,073, which became the ’634 Patent. EX1002, 1519. A Notice of Allowance was mailed November 16, 2022. Claims 15-86 were allowed. *Id.*, 1024. Issued claims 1-72 correspond to original claims 15-86. *Id.*, 22-23.

34. The Notice of Allowance stated:

None of prior art teaches a method of generating and using limited-use payment information for performing a payment transaction, the method comprising: receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises: a processor; a touch-screen display coupled to the processor; and a near field communications (NFC) interface coupled to the processor; responsive to said priming operation, readying said device to perform a payment transaction by an identified user; receiving a payment request for the payment transaction at said electronic device; displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account; dynamically generating, by the processor, limited-use payment information; wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device; 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; transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient.; responsive to

the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display, and a system of the same as set forth in the claims. *Id.*, 1029-1030.

35. Two months after the Notice of Allowance, Applicant filed its first and only IDS, which identified Gomez, Amacker, and Casey. *Id.*, 205. The Examiner subsequently mailed another Notice of Allowance on February 13, 2023. *Id.*, 14.

VI. LEVEL OF ORDINARY SKILL IN THE ART IN THE RELEVANT TIMEFRAME

36. The '634 Patent defines its field of invention as follows:

Embodiments according to the present disclosure generally relate to electronic or smart payment devices and, more specifically, to more secure, smart multi-function smart tokenizing electronic payment devices and transaction processing thereof..

EX1001, 1:27-31.

37. The '634 Specification asserts a need for security in credit cards that employ RFID technology:

A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into

the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

A concern with each of these types of credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise. Therefore, these types of credit cards have security limitations. Further, cards employing smart integrated circuit chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards.

EX1001, 1:59-2:8.

38. The Specification describes generating limited-use credit card numbers and using them to engage in secure payment transactions, including the use of cryptograph hash algorithms.

39. The claims of the '634 Patent are directed to devices and methods for communicating payment information using limited-use numbers.

40. In my opinion, in order to understand the Specification and make and use the claimed invention without undue experimentation at or near the Critical Date, one of ordinary skill in the art of the '634 Patent would have been someone with (1) a bachelor's degree in computer science, computer engineering, electrical

engineering, or a related field, and; (2) in addition, one to two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technologies such as RFID technology.

Graduate education could substitute for professional experience, or significant experience in the field could substitute for education.

41. I qualify as at least a POSITA as of March 15, 2013, and I have a sufficient level of knowledge, experience and education to provide an opinion in the field of the '634 Patent. I am familiar with what a person of ordinary skill in the art knew in 2013 because of my lengthy experience with subjects similar to those of the concepts presented in the '634 Patent. In addition, I was teaching such subjects prior to 2013.

VII. TECHNOLOGY BACKGROUND

42. In this section, I discuss the state of the art as of the Critical Date with respect to certain technologies relevant to the subject matter of the '634 Patent.

43. The art of credit card payments is extremely crowded and extensive. Prior to the Critical Date, over 50,000 U.S. patent applications and issued U.S. patents had been published containing the strings "credit card" and "payment." Furthermore, major credit-card networks, such as Visa, MasterCard, Europay and EMV ("Europay-MasterCard-Visa") had collaborated to develop industry-wide standards for credit card processing. Such standardization was necessary to enable

the use of cards at tens of millions of merchants around the world, given that many different types of point-of-sale (POS) terminals were in use at various establishments. These standards set forth requirements for equipment and software used to process card payments.

44. One major standardization effort was undertaken by the Payment Card Industry (PCI), an association of organizations that store, process and transmit cardholder data. In 2006, American Express, Discover Financial Services, Japan Credit Bureau, MasterCard and Visa International formed the Payment Card Industry Security Standards Council (PCI SSC) which, by 2014, included 688 “participating organizations.” PCI SSC issued a series of published security standards. As of the Critical Date, Version 2.0 of the PCI security standards were in effect, as described in “PCI Data Security Standard (PCI DSS) Version 2.0 January 2013,” (EX1022) and “Payment Card Industry (PCI) Data Security Standard Navigating PCI DSS Version 2.0 October 2010.” (EX1026)

A. Cryptographic Hashing

45. The PCI Standards describe the requirement of cryptographic hashing of card numbers. For example:

Protect Cardholder

Data Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

EX1026, 20.

46. A POSITA familiar with payment processing would have been familiar with these standards.

B. Near-Field Communication (NFC) Interfaces

47. A fundamental problem in electronic payments is how to communicate digital information, such as a credit card number, from the card itself or another device held by the user, to a POS device operated by a merchant. An early method was to provide the card with a magnetic stripe with encoded data including the credit card number. The user or merchant would then “swipe” the card through a magnetic reader of the POS device.

48. A later method was to build a processor chip into the card. The user or merchant would insert the card into a slot in the POS device, where electrical contact would be made with the chip, and payment data, including a credit card number, would be sent to the POS device.

49. A third method was to provide the card with a radio frequency identification (RFID) chip so that it could communicate wirelessly. The user would bring the card close to the POS device, and card information would be transmitted by radio waves over the very short distance between the card and the POS device. The '634 Patent uses the terms "radio frequency identification," "RFID," "near-field communication" and "NFC" interchangeably. It acknowledges that RFID credit cards were "in circulation":

A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

EX1001, 1:59-65.

50. Indeed, NFC credit cards were well-known in the industry. I personally was teaching about RFID credit cards in my Electronic Payment

Systems course as early as 2002. A 2009 paper by Kadambi et al., “Near-Field Communication-Based Secure Mobile Payment Service,” was published by the Association of Computing Machinery in the Proceedings of the 11th International Conference on Electronic Commerce in August 2009 (“Kadambi,” EX1025).

Kadambi notes that:

Unfortunately, innovating in the Point of Sale (PoS) space is hard because the protocols have been standardized, tightly constraining new ideas. Using mobile phones as payment devices opens up some opportunities, but any solution must minimize changes in the back-end processing. This paper describes a Near Field Communication (NFC) based mobile phone payment solution in a service-oriented environment, which provides the needed data protection without requiring costly changes to the payment processing infrastructure.

EX1025, Abstract.

51. I note that Kadambi discloses a mobile phone used as an NFC payment device.

C. Touch Screen Displays

52. The '634 Patent apparently uses the terms “touch screen” and “touch sensor array” synonymously:

A user input may be made via the touch sensor array 245, which may comprise a touch screen panel, a keypad, or a combination thereof.

EX1001, 6:39-41.

53. Mobile phones have had touchscreens for display since at least 1992, with the introduction of the IBM Simon. EX1031, 2-3. More recently, the Apple iPhone 1 in 2007 had a touchscreen. *Id.*

54. It was somewhat later that cards had touch screens, although they had them prior to the critical date. On November 9, 2012, the Sydney Morning Herald, an Australian newspaper, published an article entitled, “New credit card has LCD screen, touch-sensitive buttons” (EX1029). It states:

MasterCard is billing a new credit card it is issuing in Singapore as the “next generation of payment cards.”

With security in mind, the Display Card has an LCD screen and touch-sensitive buttons that let the user employ a one-time password (OTP). Such OTPs are often delivered via text messages or chip-based authentication devices.

The card is designed for “banking institutions that necessitate a higher level of security for their online banking services require the use of a separate authentication token or device,” according to a press release from MasterCard.

EX1029, 1-2.

55. The photo below is from the same article:



Id., 1.

D. Static and Limited-Use Numbers

56. The use of a surrogate or “token” in place of an actual credit card number was a well-known security practice long before the Critical Date. It was long known that fraud can occur if an unauthorized party obtains a user’s credit card number. Unfortunately, in older credit card transactions, there was no way to prevent the merchant itself from obtaining the user’s credit card number, as the merchant had to present that number to a credit card network in order to be paid.

57. In 2001, the idea of a token was introduced by the company TrustCommerce, which replaced the primary account number (PAN) with a randomized number, called a token. When a merchant needed to process a payment, it could use the token and TrustCommerce would process the payment on

their behalf, replacing it with the true credit card number before introducing the transaction into the credit card network. In this manner, the merchant never learns the user's credit card number.

58. Tokenization was adopted by PCI, which established a Tokenization Taskforce. In August 2011, it published "PCI DSS Tokenization Guidelines" (EX1030) to supplement Version 2.0 of the PCI Data Security Standard. It explains different ways of generating tokens, stating:

One of the primary goals of a tokenization solution should be to replace sensitive PAN values with non-sensitive token values. For a token to be considered non-sensitive, and thus not require any security or protection, the token must have no value to an attacker. Tokens come in many sizes and formats. Examples of some common token formats are included in the following table.

Table 1: Selected Examples of Token Formats*

PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cwI5x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

** Note: This table provides a selection of examples only, and does not include all possible token formats.*

EX1030, 5.

59. The Tokenization Guidelines go on to explain the difference between single-use and multi-use tokens:

Tokens can be generally identified as either single-use or multi-use. A single-use token is typically used to represent a specific, single transaction. A multi-use token represents a specific PAN, and may be used to track an individual PAN across multiple transactions. A multi-use token always maps a particular PAN value to the same token value within the tokenization system. Determining whether single-use or multi-use tokens, or a combination of both, are appropriate for a particular merchant environment will depend on the merchant's specific business need for retaining tokens.

Id.

60. I note that the last row of the table above shows generating a token by taking a portion of the credit card number (PAN) to yield a truncated PAN and replacing the middle digits with “alphabetic and numeric characters.”

61. Concluding this section, all of the technology claimed in the Challenged Claims predates the Critical Date and would have been within the knowledge of a POSITA.

VIII. CLAIM CONSTRUCTION

62. I understand that claim terms, in the absence of an express definition or disclaimer, are given their ordinary and customary meaning as would have been understood by a POSITA at the time of the alleged invention.

63. In considering the meaning of the claims, however, I understand that one must consider the language of the claims in light of “the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.” 37 C.F.R. § 42.100(b).

64. I have applied these principles in interpreting the Challenged Claims for purposes of my analysis in this Declaration.

65. I understand that Petitioner does not assert that any claim terms require express construction in this proceeding.

IX. OVERVIEW OF THE PRIOR ART

A. U.S. Patent 9,600,808 (“Gomez”)

66. Gomez Sr. et al. U.S. Patent 9,600,808 (EX1007) is entitled “Secure Payment Card, Method and System,” and lists William Gomez, Sr. as the first named inventor.

67. Gomez was filed June 22, 2012 and published on March 21, 2017. I understand that it is prior art to the '634 Patent under pre-AIA 35 U.S.C. § 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

68. Gomez discloses a payment card system that purports to address “[t]he problems of fraud and identity theft that result from the use of payment cards, such as credit and debit cards” when cardholders conduct a payment transaction that “leave[s] behind all the information necessary for another person to be able to make an unauthorized transaction.” EX1007, 1:32-48.

69. Gomez proposes a payment card “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.” *Id.*, 1:58-63. 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.

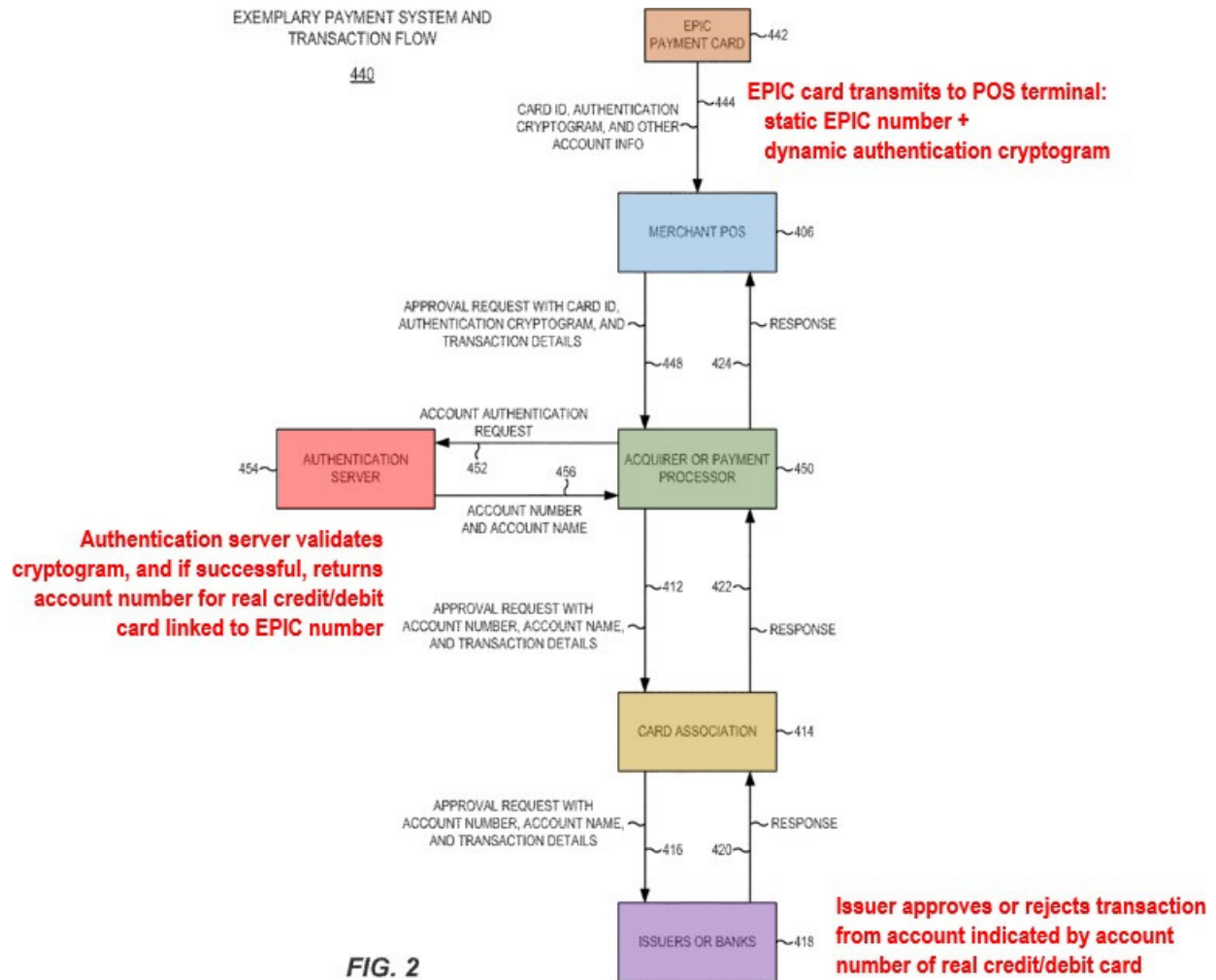
70. Customers of the system described in Gomez are issued an electronic payment card, referred to as an “EPIC” card. *Id.*, 2:19-39. The EPIC card has a static payment card identifying number corresponding to the customer’s EPIC account. *Id.* The customer can link one or more actual credit/debit cards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

stores and links to the customer's static EPIC payment card identifying number.

Id., 20:1-29. The customer can then use the EPIC card to make payment transactions with any of the linked card accounts. In this manner, "there is no need to carry the actual credit cards, they may be stored safely at home or in a safe deposit box." *Id.*, 2:35-37.

71. When a customer initiates a transaction with an EPIC card, the card dynamically generates an "authentication cryptogram" based on a unique "seed value" stored securely in the card and a "temporal signal" that changes with each attempted use or transaction. *Id.*, 7:17-48. The payment card transmits the static EPIC number and the dynamically-generated authentication cryptogram to the point-of-sale (POS) terminal, which is then conveyed to an authentication server (e.g., EPIC) before the transaction request is sent to an issuer or bank for approval. *Id.*, 7:49-8:2. The authentication server authenticates the transaction using the cryptogram, and if successful, the authentication server returns the actual account number for one of the customer's linked credit/debit cards to the acquirer or payment processor, which information is then forwarded to the appropriate card association and issuer or bank for approval. *Id.*, 18:4-42, FIGS. 17-18.

72. Below is Fig. 2 from Gomez, annotated in color, illustrating a payment transaction approval process:



73. Gomez also discloses cryptographic hash functions:

At step 294 the message is processed, such as by using a cryptographic hash function, to generate a message “digest.” A cryptographic hash function is typically viewed as a deterministic procedure that takes an arbitrary block of data, known as a “message,” and returns a fixed-size string, known as a hash value or “message digest.” Such that any change to the message will change the message digest. Such functions are well known in the art, and include MD5, SHA-1, and SHA-2. For example, MD5

returns a 128-bit message digest, while SHA-1 returns a 160-bit digest.

Id., 8:42-51.

74. Gomez also discloses a sequence code:

At step 256 a temporal signal value is generated which corresponds to the instance of attempted use. In some embodiments such a temporal signal value may reflect the date/time of the attempted use. The date and time may be determined by a real-time clock device included within the payment card, or may be communicated by the merchant POS terminal to the payment card, or by some other technique. **In some embodiments such a temporal signal value may reflect the sequence value (or sequential number) of the attempted use.**

Id., 7:17-26 (emphasis added).

B. U.S. Patent 8,423,462 (“Amacker”)

75. Amacker et al. U.S. Patent 8,423,462 (EX1008) is entitled “Real-Time Mobile Wallet Server,” and lists Matthew W. Amacker as the first named inventor.

76. Amacker was filed May 1, 2009 and issued on April 16, 2013. I understand that Amacker is prior art to the '634 Patent under pre-AIA 35 U.S.C. § 102(e) and/or AIA 35 U.S.C. § 102(a)(2).

77. Amacker discloses a “mobile wallet server” (located on a user’s device, not at a remote server location) that allows a user to “control the

distribution of personal/payment information... by selectively approving or rejecting requests for personal information using the mobile wallet server.”

EX1008, 2:13-57. “The person may respond to the request by interacting with the mobile wallet server (e.g., select ‘accept’ or ‘reject’ button, etc.) using a user interface of an application that is triggered (executed) upon receipt of the request from the entity. 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. In this way, the person may complete a complicated transaction, such as a purchase.” *Id.* The mobile wallet allows the user to select from among multiple “payment card” options. *Id.*, 5:18-41, Cl. 1. Such a selection is illustrated in FIG. 2 of Amacker, reproduced below:

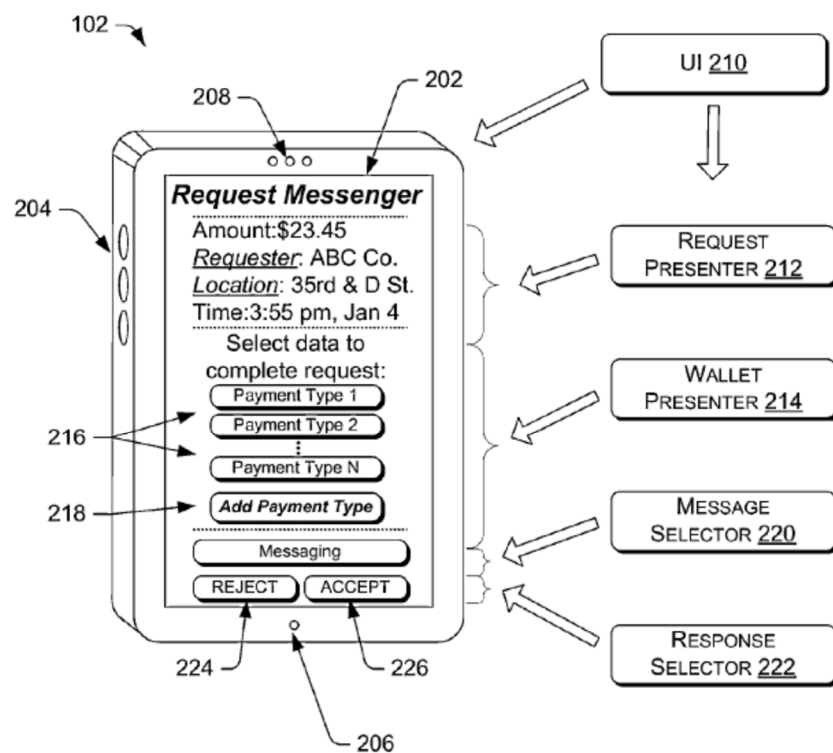


Fig. 2

78. Amacker uses the term “server” in an unusual manner. The “mobile wallet server 102” is a client-side application that hosts a “mobile wallet 108.” *Id.*, 3:4-22.

The MWS 102 may be any computing device capable of storing and processing data. For example, the MWS 102 may be a mobile server that is configured to operate on a smart telephone platform or other mobile computing device platform.

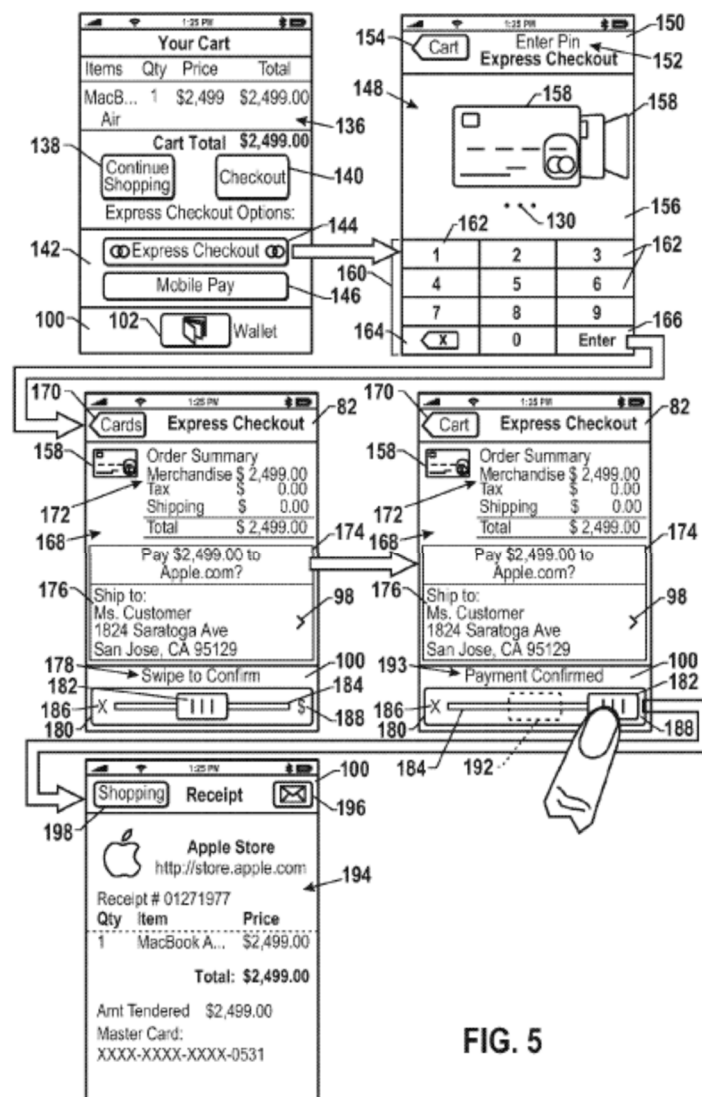
(*Id.*, 3:23-27.)

C. U.S. Patent 8,255,323 (“Casey”)

79. Casey et al. U.S. Patent 8,255,323 (EX1006) is entitled “Motion Based Payment Confirmation,” and lists Brandon J. Casey as the first named inventor.

80. Casey was filed January 9, 2009 and issued on August 28, 2012. I understand that Casey is prior art to the ’634 Patent under pre-AIA 35 U.S.C. §§ 102(a) and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

81. 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. Specifically, Casey discloses interfaces for receiving “a request for payment” via NFC or other communication, displaying payment card and transaction information, and receiving a PIN or user movement of a graphical element (slider) to confirm or deny a transaction. *Id.*, 8:52-9:36, 12:66-13:51, 14:11-49, 15:24-59; FIGs. 4-5. FIG. 5 of Casey, showing sliding by finger, is reproduced below:



82. Casey also discloses that the user device can receive input by sensing motion:

In addition to receiving user input through the input structures 60 and the touchscreen 54, the device 10 may include a motion sensing device 62 for receiving user input. The motion sensing device 62 may be any device

configured to measure motion or acceleration, Such as an accelerometer or a gyroscope. In one embodiment, the motion sensing device 40 may be a three-axis accelerometer that includes a sensing element and an integrated circuit interface for providing the measured acceleration and/or motion data to the CPU 46.

Id., 7:59-67.

83. Motion can be used to confirm a payment transaction:

Motion data acquired by the motion sensing device 62 may be used to confirm a payment transaction. As discussed further below, the motion sensing device 62 may be configured to sense motion of the device 10 and transmit motion data to the CPU 46 to adjust one or more graphical elements shown on the display 24. For example, a graphical element, such as a slide bar, may be moved across the display 24 in response to sensed motion.

Id., 8:6-11.

D. U.S. Patent Publication 2015/0134540A1 (“Law”)

84. Law et al. U.S. Patent Publication 2015/0134540A1 (EX1032) is entitled “Systems and methods for facilitating a transaction using a virtual card on a mobile device,” and lists Simon Law as the first named inventor.

85. Law was filed April 16, 2013 and issued on December 05, 2023, and Law claims priority to provisional application No. 61/673,096 (“Law Provisional”)

filed July 18, 2012 (EX1033). I understand that Law is prior art to the '634 Patent under pre-AIA 35 U.S.C. § 102(e) and/or AIA 35 U.S.C. §§ 102(a)(2).

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

Law Claim 4	Exemplary Disclosures of the Law Provisional (EX1033)
4. A computer-implemented method comprising:	To the extent the preamble is limiting, the Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0033]-[0034], [0063].
registering a funding card comprising storing a funding card number;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , 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;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[[0054], 0066]-[0072], [0079].

Law Claim 4	Exemplary Disclosures of the Law Provisional (EX1033)
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;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0072]-[0073], [0076]-[0079], [00100], [00113]-[00114].
storing the data for the virtual card in association with the funding card number;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0051]-[0052], [00109]-[00114].
sending information related to the data for the virtual card to the mobile device;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , 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	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0054], [0084]-[0088].

Law Claim 4	Exemplary Disclosures of the Law Provisional (EX1033)
requested payment amount;	
retrieving the funding card number based on the data for the virtual card;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0054], [0086]-[0091].
sending a second payment authorization request to a funding card issuer, the second payment authorization request comprising the funding card number and the requested payment amount;	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0054], [0087]-[0093].
receiving a payment authorization response from the funding card issuer; and	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0055], [0087]-[0093].
sending the payment authorization response to the merchant or the merchant acquirer.	The Law Provisional discloses this limitation. <i>See, e.g.</i> , EX1033, ¶¶[0048], [0087]-[0093].

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

88. 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 (e.g. card details include the name printed on the funding card, the PAN printed on the funding card, the expiry date printed on the funding card, and the static security code printed on the funding card),” 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. For example, the funding card identifier is a random value so that, if intercepted by an adversary, would not be able to recognize any funding card details.” 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 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].

E. U.S. Patent 7,593,000 (“Chin”)

89. Chin U.S. Patent 7,593,000 (EX1044) is entitled “Touch-based authentication of a mobile device through user generated pattern creation,” and lists David H. Chin as the named inventor.

90. Chin was filed December 24, 2008 and issued on September 22, 2009.

I understand that Chin is prior art to the '634 Patent under pre-AIA 35 U.S.C. §§ 102(a), 102(b), and 102(e) and/or AIA 35 U.S.C. §§ 102(a)(1) and 102(a)(2).

91. 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.

X. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1A: Claims 1-2, 7-16, 27-34, and 36-38 of the '634 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker and Casey

92. In my opinion, the combination of Gomez, Amacker, and Casey renders obvious as a whole claims 1-2, 7-16, 27-34, and 36-38 of the '634 Patent for at least the reasons discussed below.

1. Motivation to Combine Gomez with Amacker and Casey

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

94. 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. A POSITA would have recognized that 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 the touchscreen, such as when selecting a payment card, thereby improving the user experience. EX1008, 5:1-17, FIG. 2. Moreover, a POSITA would have recognized that a touchscreen display

would have allowed the resulting device to conserve space by allowing for the display of user input features (e.g., the PIN input keypad disclosed by Gomez) without requiring additional physical hardware (e.g., a separate physical keypad) on the phone. EX1007, 13:34-44, FIG. 14 (PIN input keypad 162).

95. Furthermore, a POSITA would have recognized that 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 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.

96. 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. 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 beneficially 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:

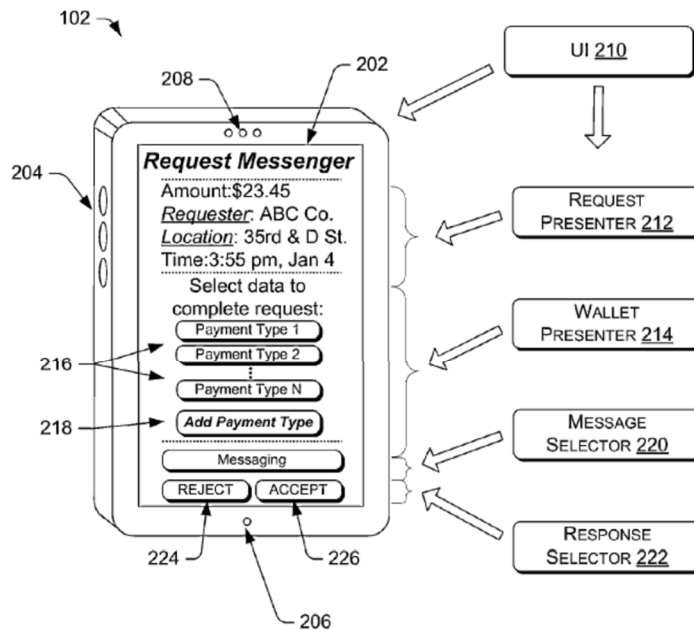


Fig. 2

Id., FIG. 2. This modification would have improved the resulting system by allowing the user to better ensure that they are approving a known, genuine payment transaction and transmitting payment information to the correct merchant terminal, which can prevent fraudulent transmittal of payment information to an incorrect terminal. 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 then visually review transaction data in the request before approving (or denying) the transaction. *Id.*; EX1008, 3:27-57, 2:37-3:3, 4:37-5:41, 6:2-15. Requiring the user to authorize the transaction (as taught by Amacker) would have allowed the

user to review transaction information (e.g., price, purchase items) prior to completing the transaction, allowed the user an extra opportunity to change their mind regarding the transaction, and provide extra assurance that the user intends to initiate a payment transaction rather than having inadvertently opened a payment application.

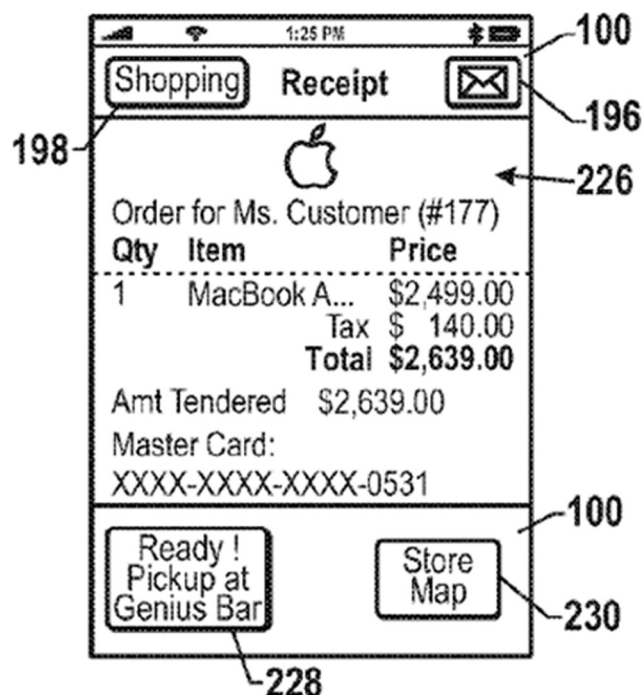
97. Third, a POSITA would have modified Gomez based on Amacker to display additional information when allowing a user to select a payment method. Gomez discloses that the user can “manually select the actual credit card that he/she wishes to use during a purchase transaction” by choosing from a list of cards that includes “description name (or nickname) and card logo.” EX1007, 20:30-59, 21:5-20. Amacker provides additional details on how a user can use a touchscreen display to view additional information about payment methods before selecting. EX1008, 5:18-41, claim 1, FIG. 2. A POSITA would have recognized that including additional information (issuer name, processor and issuer logos, account number, etc.) in the card selection process would have allowed the user to more easily identify a desired card for a particular transaction.

98. 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. 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 I described above in discussing the ’634 patent, because these user inputs prepare the device for a transaction, providing an indication that a transaction is imminent and intentional. *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 transaction, providing an indication that a transaction is imminent). A POSITA would have been motivated 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.

99. 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. Casey explains that “the receipt may identify the amount tendered, the payment recipient, and the payment instrument used.” *Id.*, 10:49-53, *see also id.*, 10:20-29, 16:3-20. 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. *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. Such a modification would have been easily implemented since Casey, 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. Receipts, of course, are universal in payment transactions.



EX1006, FIG. 8.

100. 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. 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 I described above, this detection of a user motion of the device would have to be adapted to accommodate the larger device. 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. Such a motion sensing 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 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.

101. 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.

2. Claim 1

- i) **[1.pre] A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:**

102. Whether or not the preamble is limiting, Gomez discloses it. 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. Gomez’s method “utilizes 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” (“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.

103. 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 ("method of generating and using limited-use payment information for performing a payment transaction").

ii) [1.a] receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:

104. 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 I discussed above (Section IX.A.1), in the predictable combination, the payment device can be a mobile device such as a smartphone ("electronic device"). EX1008, 2:13-25.

105. 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” (“receiving an input at an electronic device, wherein the input comprises a priming operation”). EX1007, 5:13-18; *see also id.*, 2:59-64, 7:9-16, 9:12-33, 13:40-44. As I discussed above (Section IX.A.1), in the Gomez-Amacker-Casey combination, the priming operation (which results in generation of the cryptogram) includes a user entering a valid credential (“receiving an input at an electronic device, wherein the input comprises a priming operation”) and bringing the device within proximity of an NFC terminal to receive a payment request—that is, an indication that a transaction is imminent. *See infra* Elements [1.f]-[1.g]; *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 transaction, providing an indication that a transaction is imminent).

iii) [1.b] a processor;

106. Gomez discloses that its device “includes a processor” (“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 (MWS) 102 implemented on a mobile computing device), FIG. 4 (MWS 102 includes processor(s) 402).

**iv) [1.c] a touch-screen display coupled to the processor;
and**

107. 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” (“display coupled to the processor”). EX1007, 10:34-38, 12:49-61. The display of the Gomez-Amacker-Casey device “may be a touch screen display” (“a touch-screen display coupled to the processor”). EX1008, 4:51-60; EX1006, 7:26-29; Section IX.A.1.

**v) [1.d] a near field communications (NFC) interface
coupled to the processor;**

108. The Gomez-Amacker-Casey device’s processor may include various integrated circuits, including “NFC circuits for implementing a near-field communications transceiver” (“a near field communications (NFC) interface coupled to the processor”). EX1007, 10:53-57, 7:49-54, 8:11-24, 2:40-3:3.

**vi) [1.e] responsive to said priming operation, readying
said device to perform a payment transaction by an
identified user;**

109. As I 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.1. As I discussed, when the authentication cryptogram is generated, the device is ready to be used in a transaction by a particular user (“responsive to said priming operation, readying said device to perform a payment transaction by an identified user”). *Supra* Element [1.a]; EX1007, 2:59-64, 5:13-18, 7:9-16, 9:12-33, 13:40-44. Indeed, all that is required after generation of the authentication cryptogram to perform the transaction is user acceptance of the payment request. EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; *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).

vii) [1.f] receiving a payment request for the payment transaction at said electronic device;

110. As described by Amacker, 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 (“receiving a payment request for the payment transaction at said electronic device”). EX1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; Section IX.A.1. 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] displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;**

111. As I 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. 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" ("displaying...an image representing a selected issued payment account"). *Id.*, 20:30-59, 21:5-20, FIG. 9. 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" ("image representing a selected issued payment account"). EX1007, 20:43-59.

112. Amacker confirms that, in the predictable Gomez-Amacker-Casey combination—which, as I 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 ("displaying, on the touch-screen display, information reflecting the payment request"), as shown in red in FIG. 2 below. EX1008, 5:1-17, FIG. 2; *supra* Element [1.c]; *see also* Section IX.A.1. 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 (“displaying, on the touch-screen display...an image representing a selected issued payment account”). EX1008, 5:18-41, claim 1.

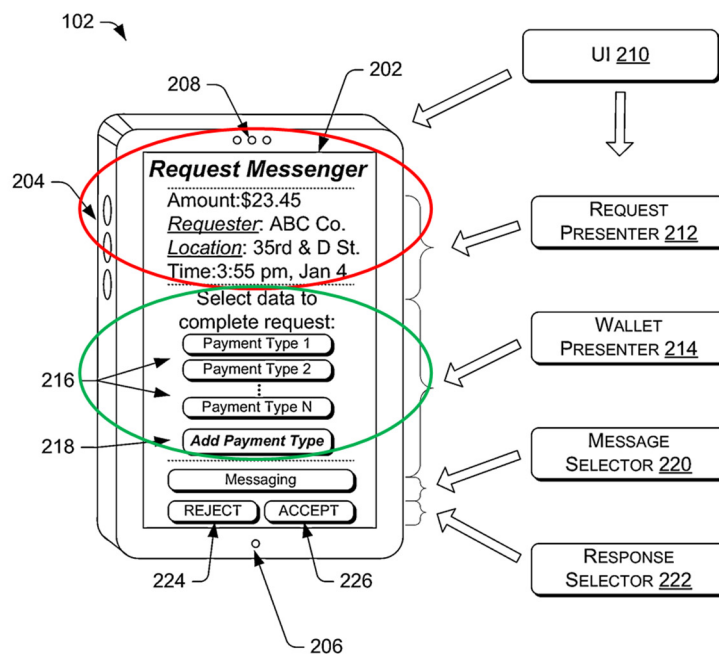


Fig. 2

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] dynamically generating, by the processor, limited-use payment information;

113. As I 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, upon verification of a valid credential, 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.

x) [1.i] wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;

114. As I 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.

- xi) [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;**

115. As I 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]. As I 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]. 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.

xii) [1.k] transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;

116. Gomez discloses “communicating a payment card identifying number to a payment processing system, and communicating the authentication cryptogram in a payment card account name field to the payment processing system”

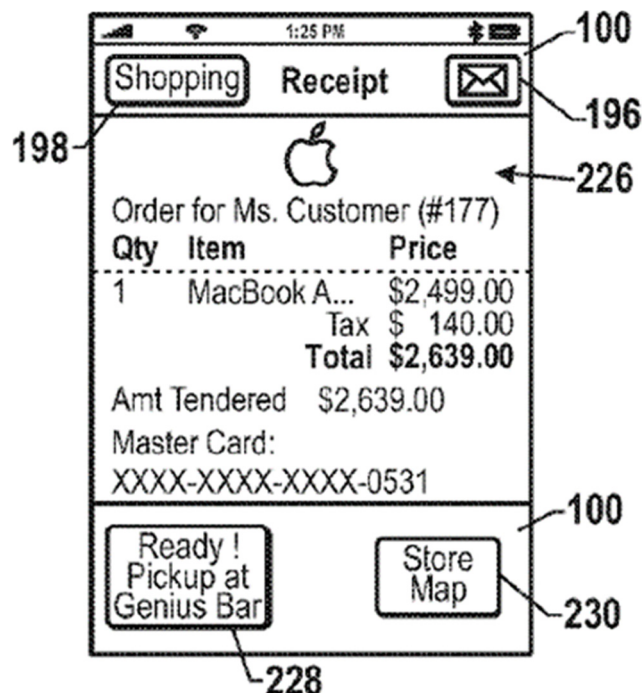
(“transmitting said limited-use payment information from said electronic device”).

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)” (“via said NFC interface for receipt by an NFC recipient”). *Id.*, 7:49-54, 8:6-24.

xiii) [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

117. As I 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.1. “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) (“responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction”). *See* Section IX.A.1.



EX1006, FIG. 8.

xiv) [1.m] displaying the status of said payment transaction via said touch-screen display.

118. As I 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 (“displaying the status of said payment transaction via said touch-screen display”). *Supra* Element [1.l]; Section IX.A.1. 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. It was obvious to provide status information concerning a payment transaction; otherwise, the user would not know whether the transaction succeeded or failed.

3. Claim 2: The method of claim 1, wherein the limited-use payment information comprises a cryptogram number.

119. As I discussed for Elements [1.pre] and [1.h], the dynamically generated limited-use payment information is an authentication cryptogram (“wherein the limited-use payment information comprises a cryptogram number”). *Supra* Elements [1.pre], [1.h]. I have reviewed the prosecution history of the ’634 Patent and originally presented claim 2 recited “wherein the generating limited-use payment information comprises dynamically generating a cryptogram number for a use by the electronic device in place of a card validation value, associated with said

card issuer payment card.” EX1002, 1506. Therefore, a POSITA would have understood that the “cryptogram number” encompasses the cryptogram itself.

4. Claim 7: The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient.

120. 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 (“wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient”). *Supra* Elements [1.a], [1.e]; Section IX.A.1.

5. Claim 8

- i) **[8.pre] The method of claim 7, wherein said readying said device to perform a payment transaction comprises:**
- ii) **[8.a] identifying said proximity NFC recipient is an NFC payment facility;**

121. The Gomez-Amacker-Casey combination’s priming operation, which readies the user’s device to perform a payment transaction (“wherein said readying said device to perform a payment transaction comprises”), involves bringing the user’s device within proximity of the NFC terminal to receive a payment request. *Supra* Claim [7]. A POSITA would have understood that an NFC terminal continuously emits a radio frequency signal, and thus, in order 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 (“identifying said proximity NFC recipient is an NFC payment facility”) by identifying this emitted signal. EX1006, 6:58-61, 8:52-64.

iii) [8.b] successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and

122. As I 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 to perform the transaction (“successfully validating the identified user as authorized to perform the payment transaction via said electronic device”).

EX1007, 9:19-39, FIG. 6 (steps 304 and 306); *supra* Element [1.e].

iv) [8.c] receiving a user approval for performing the payment transaction.

123. As I 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.1. 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 (“receiving a user approval for performing the payment transaction”). EX1008, 6:3-15.

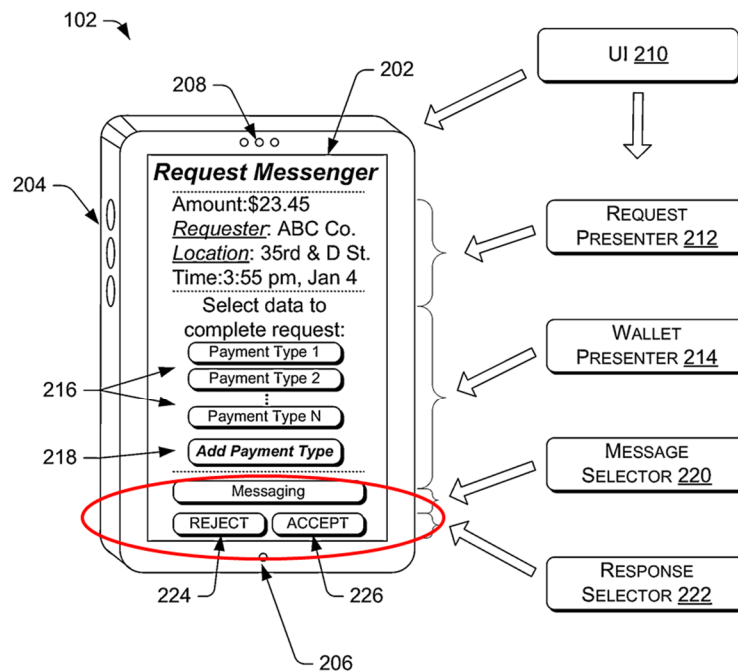


Fig. 2

EX1008, FIG. 2

6. Claim 9

- i) [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:

124. As I 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];
Section IX.A.1.

- ii) **[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,**

125. As I 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]. 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. As I discussed for Elements [1.a], [1.e], [7], and [8.a], the verification of these user credentials is required in order 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].

iii) [9.b] disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.

126. As I 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]; Section IX.A.1. In particular, Gomez explains that the card is otherwise deactivated if a user’s credentials cannot be authorized (a prerequisite to the generation of the authentication cryptogram, as I discussed for Elements [1.a] and [1.e], and part of the readying process, as I discussed for Element [8.b]), 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 (“disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed”).

7. Claim 10

- i) [10.pre] The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between:**
- ii) [10.a] firstly, a user input received via at least one of a set of user input sensors of the electronic device; and,**
- iii) [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.**

127. As I 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 determining whether the input credential matches the reference credential to determine whether an authorized user is attempting to use the device. 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] (describing a touch screen as having sensor layers that form a sensor for recognizing user's touch); Section IX.A.1.

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"). A POSITA would have understood that a PIN number entry is a "challenge-response" since it is 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"); EX1007, 13:34-44 (describing a display of the device that prompts a user to enter a PIN number); Section IX.A.1 (discussing incorporation of display into touch screen of combined device). I have been informed that Patent Owner asserts that a

PIN/password/passcode is a “challenge-response,” and that Patent Owner similarly asserts that a PIN or password entry is a “security challenge question,” and I have been asked to assume that interpretation applies to this limitation. Under that interpretation, it is my opinion that a PIN number entry is a “challenge-response.”

- 8. Claim 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.**

128. 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 (“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”).

Supra Elements [10.pre]-[10.b]; EX1007, 13:40-42; Section IX.A.1.

- 9. Claim 12: The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics.**

129. 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 (“wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch”).

characteristics”). *Supra* Elements [10.pre]-[10.b]; EX1007, 11:30-38 (referring to fingerprint data as biometric touch data).

10. Claim 13: The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.

130. A POSITA would have understood that the reference fingerprint of a known user is a “known user touch gesture.” For example, Gomez discloses 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.” 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 (“wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture”).

131. I understand that Patent Owner has asserted that a PIN or passcode entry is a “known user touch gesture,” and I have been asked to apply that interpretation to this limitation. Under Patent Owner’s interpretation of this limitation, it is my opinion that 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.” As I 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). A POSITA would have thus understood that under Patent Owner's interpretation of this limitation, Gomez's reference credential for a user PIN is a "predetermined user characteristic[] stored within the electronic device" comprising a "known user touch gesture."

11. Claim 14: The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user motion of the device.

132. As I discussed above (Section IX.A.1), in the Gomez-Amacker-Casey device, user input for the priming operations may be provided through a user motion of the device. EX1006, 7:59-8:3. As I 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]. 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 ("wherein said predetermined

user characteristics stored within the electronic device comprise a known user motion of the device”).

12. Claim 15: The method of claim 1, wherein the input comprising a priming operation is a user input.

133. As I discussed for Element [1.a], the priming operation input may be the entry of a user input such as a fingerprint or PIN (“wherein the input comprising a priming operation is a user input”). *Supra* Element [1.a].

13. Claim 16

- i) **[16.pre]: The method of claim 15, wherein said readying said device to perform a payment transaction comprises:**
- ii) **[16.a] successfully identifying said identified user from said user input; and,**

134. As I 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 (“wherein said readying said device to perform a payment transaction comprises: successfully identifying said identified user from said user input”). Element [8.b].

- iii) **[16.b] wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and,**

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

payment transaction by touching the “accept” button on the payment request displayed on the touch-screen display (“wherein said user input further comprises a user approval for performing the payment transaction received from said identified user”). Element [8.c]; Section IX.A.1.

- iv) **[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,**

136. As I 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]. 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.

- v) **[16.d] wherein said user approval for performing the payment transaction further comprises:**
- vi) **[16.e] visually presenting information of the payment transaction on the touch screen display of said electronic device;**
- vii) **[16.f] visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,**
- viii) **[16.g] subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.**

137. As I 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.1. As I 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].

14. Claim 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.

138. As I 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, 5:7-18, 7:17-8:9, FIG. 7. As I 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.

139. 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. In other words, the seed value is secret information that only the card/device itself and the EPIC payment processing authority have access to (“payment processing authority secret information”). Accordingly, “the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information” because the authentication cryptogram is dynamically generated based on the seed value and temporal signal value.

15. Claim 28

- i) [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**

140. As I discussed for Claim [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”).

- ii) **[28a]: further wherein the at least one secret information is not exchanged when preforming the payment transaction.¹**

141. As I discussed for Element [1.j] and Claim [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 (“further wherein the at least one secret information is not exchanged when [performing] the payment transaction”). *Supra* Element [1.j], Claim [27].

16. Claim 29

- i) **[29.pre]: A system for completing a payment transaction, the system comprising:**
- ii) **[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:**

142. Whether or not the preamble is limiting, it is disclosed by each of Gomez, Amacker, and Casey. *Supra* Elements [1.a] (describing “an electronic

¹ I have been instructed to assume that the claimed “preforming” is intended to read “performing.” Indeed, I have been informed that Patent Owner agreed to this construction in district court, and have been asked to apply that construction here.

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”).

iii) [29.b] a processor;

143. *Supra* Element [1.b] (reciting same limitation).

iv) [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,

144. *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”)).

v) [29.d] a touch-screen display coupled to the processor, and

145. *Supra* Element [1.c] (reciting same limitation).

vi) [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;

146. *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”)).

- vii) [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;**

147. *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”))).

- viii) [29.g] wherein the electronic device is operable to store a static device-specific user account information;**

148. As I 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 (“[T]he static payment card identifying number identifies the payment card, but does not represent a live account, in which case

one or more actual credit card accounts (or other payment card accounts) are linked to the payment card identifying number.”), 20:1-37 (“An EPIC account may be established online to link one or more actual payment card accounts with the EPIC account....”); Element [1.pre]. 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. A POSITA would have understood that when the Gomez-Amacker-Casey device is implemented as a larger, 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”). *See* Section IX.A.1; EX1008, 8:21-33 (describing storage of payment numbers on Amacker’s electronic device).

- ix) **[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;**

149. *Supra* Elements [1.j]-[1.k] (describing the user device’s transmission of the authentication cryptogram and EPIC static payment card identifying number

(“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”) via the NFC interface to the NFC terminal recipient to be used in the transaction (“to an NFC recipient via, said NFC interface for use in connection with payment transaction”) in place of the card issuer supplied payment information/actual credit card account number associated with the selected credit card account (“in place of information associated with said selected issued payment account”).

- x) **[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,**

150. *Supra* Element [1.1] (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 (“wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction”).

- xi) **[29.j] wherein the touch-screen display is operable to display as indication of said status information.**

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

- 17. Claim 30: The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number**

152. *Supra* Claim [2] (reciting similar limitation).

- 18. Claim 31: The system of claim 29, wherein the device-specific user account information comprises static device account information.**

153. *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 (“wherein the device-specific user account information comprises static device account information”).)

- 19. Claim 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.**

154. 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. 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. 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 ("wherein the static device account information comprises a static device account number that is unique to the electronic device").

20. Claim 33: The system of claim 32 wherein the static device account information further comprises a static device account expiration date.

155. 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.

21. Claim 34: The system of claim 32 wherein the sequential counter count is changed per payment transaction.

156. *Supra* Element [1.i] (temporal signal may be the sequence value/sequential number of the attempted use/transaction of the device (“wherein the sequential counter count is changed per payment transaction”))).

22. Claim 36

- i) **[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,**

157. As I discussed for Element [1.h], the device’s processor dynamically generates an authentication cryptogram (“the electronic device is further operable to dynamically generate the limited-use payment information”). Element [1.h].

158. As I 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.1. As I 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 I 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]. As I 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].) 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 I described for Claim [27], the information included in the seed value must be secret in order to prevent fraudulent transactions.

159. 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).

- ii) **[36.a] wherein said shared information is shared by both the electronic device and a payment processing authority.**

160. As I discussed for Claim [27] and Element [28.pre], the seed value (containing randomized bits) is shared by both the user's electronic device and the EPIC payment processing authority. A POSITA would have understood that 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. A POSITA would have understood that 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. Both the acceptance of the request and the manually selected credit card are user inputs to the device and are thus known to the device. 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. Accordingly, the "shared information" discussed in for Element [36.pre] is collectively "shared by both the electronic device and a payment processing authority."

- 23. Claim 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.**

161. *Supra* Claim [27] (reciting similar limitation and describing generation of cryptogram based on secret seed value), Elements [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).

- 24. Claim 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.**

162. *Supra* Claim [27] (reciting similar limitation).

B. Ground 1B: Claims 3-6, 17-26, 35, and 39-72 of the '634 Patent Are Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Casey, and Law

163. In my opinion, the combination of Gomez, Amacker, Casey, and Law renders obvious as a whole claims 3-6, 17-26, 35, and 39-72 of the '634 Patent for at least the reasons discussed below.

1. Motivation to Combine Gomez with Amacker, Casey, and Law

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

165. First, a POSITA would have further 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). It is a matter of common sense for a user having multiple cards to select one for a given transaction.

166. 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 communicated to the merchant and EPIC authentication server (i.e., the payment processing authority) 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. 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. EX1032, ¶[0082]; EX1033, ¶[0052]. Law's funding card identifier feature would have therefore been an ideal choice for implementing the transmission of selected credit/debit card information while adding an extra layer of security to the combined system.

167. A POSITA would have been motivated to incorporate Law's funding card identifier feature so that 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). In the predictable combination, a static EPIC account funding card identifier would be 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. EX1007, 2:19-39, 20:1-37; EX1032, ¶[0082]; EX1033, ¶[0052]. A POSITA would have been motivated 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). 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.

168. 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. Gomez explains that 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. 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. 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]. Law describes that it was known to compute dynamic data using random data from the funding card. 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. EX1032, ¶¶[0142]-[0155]; EX1033, ¶¶[00109]-[00122]. Amacker similarly discloses generating limited-use information for a transaction that is 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). A POSITA would have recognized that using these additional values when generating Gomez's authentication cryptogram would have increased security because the cryptogram would be based on additional values, thus making it more difficult to decrypt the cryptogram in the event the cryptogram is intercepted by a third party.

169. 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.

2. Claim 3

- i) [3.pre] The method of claim 2, further comprising:**
- ii) [3.a] prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,**
- iii) [3.b] in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.**

170. As I discussed above (Section IX.B.1), 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 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”). 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*, Claim [32] (describing uniqueness of static payment card identifying number).

3. Claim 4

- i) [4.pre] The method of claim 3 further comprising:
- ii) [4.a]² combining said limited-use payment information and said static device account information, to reduce a combined payment information:
- iii) [4.b]³ transmitting said combined payment information, in place of the issued payment account information, via said NFC for receipt by an NFC recipient; and

171. As I discussed above (Section IX.B.1), 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

² I have been instructed to assume the claimed “reduce” is intended to read “produce” as recited in similar claims, e.g., Element [18.a]. I have been informed that in district court, Patent Owner agreed to construe “reduce” to mean “produce,” and have been asked to apply that construction here. Moreover, the word “produce” appears correctly in the amendment of April 22, 2022, in which the claim was newly presented. *See* EX1002, 22 (final claim 4 is original claim 34), 1084 (newly presented claim 34).

³ I have been instructed to assume that “via said NFC for receipt by an NFC recipient” is intended to read “via said NFC [interface] for receipt by an NFC receipt.” Indeed, I have been informed Patent Owner agreed to this construction in district court, and have been asked to apply that construction here.

(“combining said limited-use payment information and said static device account information, to [produce] a combined payment information”) and sent together (“transmitting said combined payment information”) by the mobile device to the POS terminal. 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 I discussed for Element [1.j]. *Supra* Element [1.j]. The combined payment information would also be sent “via said NFC [interface] for receipt by an NFC recipient” for the same reasons as I discussed for Element [1.k]. *Supra* Element [1.k].

- iv) **[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.**

172. *Supra* Element [1.l] (reciting similar limitation).

- 4. **Claim 5⁴ The method of claim 3, wherein the dynamically generating Lather comprises dynamically generating the**

⁴ I have been instructed to assume that the claimed “Lather” is intended to read “further” as recited in similar claims, e.g., Element [19]. The word “further” appears correctly in the amendment of April 22, 2022, in which the claim was newly presented. *See* EX1002, 22 (final claim 5 is original claim 39), 1086 (newly presented claim 39). I have also been informed that in district court, Patent Owner agreed to construe “Lather” to mean “further,” and have been asked to apply that construction here.

**limited-use payment information based on payment
processing authority secret information.**

173. *Supra* Claim [27] (reciting same limitation).

- 5. Claim 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.**

174. *Supra* Element [28.a] (reciting same limitation).

6. Claim 17

- i) [17.pre] The method of claim 1, further comprising:**
- ii) [17.a] prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,**
- iii) [17.b] in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.**

175. *Supra* Elements [3.pre]-[3.b] (reciting same limitations).

7. Claim 18

- i) [18.pre] The method of claim 17 further comprising:
- ii) [18.a] combining said limited-use payment information and said static device account information, to produce a combined payment information;
- iii) [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
- iv) [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.

176. *Supra* Elements [4.pre]-[4.c] (reciting similar limitations).

- 8. Claim 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.**

177. *Supra* Claim [27] (reciting same limitation).

- 9. Claim 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.**

178. *Supra* Element [28.a] (reciting same limitation).

- 10. Claim 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.**

179. *Supra* Claim [27] (reciting same limitation).

- 11. Claim 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.**

180. *Supra* Element [28.a] (reciting same limitation).

12. Claim 23

- i) [23.pre] The method of claim 1, further comprising:
- ii) [23.a] prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and,
- iii) [23.b] in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.

181. As I discussed above (Section IX.B.1), 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”). 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 “payment processing authority supplied secret information” because it is supplied by the EPIC processing authority, and also 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].

13. Claim 24: The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information.

182. *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”).

14. Claim 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.

183. As I discussed above (Section IX.B.1), 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”). EX1032, ¶[0082]; EX1033, ¶[0052].

15. Claim 26: The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device.

184. As I discussed for Claim [25], a static EPIC account funding card identifier represents and encapsulates information such as a PAN (primary account number) that is associated with the user-selected actual credit/debit card on the mobile device (“wherein the static device account number is associated with the selected issued payment account on said electronic device”). *Supra* Claim [25]; EX1032, ¶[0082]; EX1033, ¶[0052]; Section IX.B.1.

16. Claim 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.

185. *Supra* Elements [3.pre]-[3.b] (reciting similar limitations).

17. Claim 39

i) [39.pre] An electronic device for completing a payment transaction, the electronic device comprising:

186. Whether or not the preamble is limiting, it is disclosed by each of Gomez, Amacker, Casey, and Law. *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) [39a] a processor;

187. *Supra* Element [1.b] (reciting same limitation).

- iii) [39.b]⁵ 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;

188. 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 I 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 display of the electronic device. Element [1.g]. 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”).

189. As I 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].

⁵ There is no antecedent basis for “the payment authority information.” I have been instructed to nevertheless explain how this limitation is disclosed by the prior art.

- iv) **[39.c] a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;**

190. *Supra* Element [29.c] (reciting same limitation).

- v) **[39.d] a user interface coupled to the processor;**

191. *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”)).

- vi) **[39.e] a user input device coupled to the processor; and,**

192. As I 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.

- vii) **[39f] wherein said processor is operable to:**

193. 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 also be operable to perform the following steps in Elements [39.f.i]-[39.f.v].

- viii) **[39.f.i] responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,**

194. *Supra* Elements [1.a] (describing a “priming operation”), [1.e]

(describing similar limitation to Element [39.f.i]).

- ix) **[39.f.ii] cause the display of information associated with the payment request;**

195. *Supra* Element [1.g] (reciting similar limitation).

- x) **[39.f.iii] cause the display of an image representing at least one user-selectable issued payment account; and,**

196. *Supra* Element [1.g] (reciting similar limitation).

- xi) **[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,**

197. As I 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]. As I discussed above (Section IX.B.1) for the Gomez-Amacker-Casey-Law

combination, a POSITA would have been motivated 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].

- xii) **[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;**

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

- xiii) [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**

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

- xiv) [39.h] wherein the user interface is operable to provide an indication of the status information.**

200. *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”).

- 18. Claim 40: The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device.**

201. *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”))).

- 19. Claim 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.**

202. As I discussed above (Section IX.B.1) 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
(“comprises a secret information shared by both the electronic device and a
payment processing authority”). See Element [23.b].

**20. Claim 42⁶ The device of claim 41 wherein the processing
authority information comprises a static device account
number.**

203. *Supra* Claim [25] (describing how the static EPIC account funding
card identifier (“processing authority information”) “comprises a static device
account number”).

**21. Claim 43: The device of claim 42 wherein the processing
authority information further comprises a static device
account expiration date.⁷**

204. *Supra* Claim [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

⁶ There is no antecedent basis for “the processing authority information.” I have
been instructed to assume, 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.” I have also been informed that this assumption is consistent with
Patent Owner’s assertions in district court, which I understand identified the same
information for both “payment authority information” and “processing authority
information.” I have been instructed to make the same assumption for Elements
[43]-[44], [46]-[48], and [55.b]-[55.c].

⁷ See footnote for Element [42].

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

- 22. Claim 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.⁸**

205. As I 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.1. 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.

- 23. Claim 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**

⁸ See footnote for Element [42].

**least a portion of the payment information associated with
said selected issued payment account.**

206. As I discussed for Claim [2], the authentication cryptogram (“dynamically generated limited-use payment information”) is a cryptogram number (“comprises a cryptogram number”). As I 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.1. 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].

**24. Claim 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.⁹

207. *Supra* Claim [44] (reciting same limitation).

25. Claim 47: The device of claim 46 wherein the processing authority information comprises a static device account number.¹⁰

208. *Supra* Claim [42] (reciting same limitation).

26. Claim 48: The device of claim 47 wherein the processing authority information further comprises a static device account expiration date.¹¹

209. *Supra* Claim [43] (reciting same limitation).

27. Claim 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.

210. As I 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 interface comprises a display"). *Supra* Elements [1.c], [39.d]. As I 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

⁹ See footnote for Claim [42].

¹⁰ See footnote for Claim [42].

¹¹ See footnote for Claim [42].

comprised of a touch panel/screen that “may be 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. As I 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].

28. Claim 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.

211. 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 I discussed for Element [49]. *Supra* Element [49]. As I 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”).

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.1 (discussing display of Gomez’s user input features on touch screen).

29. Claim 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.

212. As I 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]. A POSITA would have understood that in order to accurately read a fingerprint through a biometric sensor, the user would have to continuously hold their finger to the

¹² I have been informed that Patent Owner has asserted that a displayed request for a PIN is a “security challenge question,” and I have been asked to apply that interpretation for this limitation. Under that interpretation, it is my opinion that the request for a PIN in the Gomez-Amacker-Casey-Law combination is a “security challenge question.”

sensor (“biometric sensing of a continuous user touch”) until the fingerprint is fully read.

- 30. Claim 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.**

213. 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 I discussed for Claim [49]. As I discussed for Claim [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. A POSITA would have been motivated 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”) in order 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.

- 31. Claim 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.

214. 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 I discussed for Claim [49]. As I 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 sensor) matches a reference fingerprint credential of an authorized user (“by biometric recognition of a valid user identification”). *Supra* Elements [10.pre]-[10.b].

32. Claim 54: The device of claim 39, 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.¹³

215. As I discussed above (Section IX.A.1) with respect to the Gomez-Amacker-Casey device, and further for Claim [14], user input for the priming operations may be provided through a user motion of the device. EX1006, 7:59-

¹³ I have been instructed to assume the claimed “array” is intended to read “array” as recited in similar claims, e.g., Claim [71]. Furthermore, the word “array” appears correctly in the amendment of April 22, 2022, in which the claim was newly presented. *See* EX1002, 22 (final claim 54 is original claim 68), 1094 (newly presented claim 68).

8:3; *supra* Claim [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 measurements in three orthogonal directions. 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. A POSITA would have also understood that for a motion sensing device (containing an array of motion sensors, as I 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”). Accordingly, in the predictable combination, the device would have been configured such that “the processor is

operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.”

33. Claim 55

- i) [55.pre]: The device of claim 39, wherein the processor is operable to:**

216. 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].

- ii) [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**

217. As I 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]. As I discussed for Element [39.e], the “user interface [is] coupled to the processor.” *Supra* Element [39.e].

- iii) **[55.b] responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and¹⁴**
- iv) **[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.¹⁵**

218. As I discussed above (Section IX.B.1) 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]. As I 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]. 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

¹⁴ See footnote for Claim [42].

¹⁵ See footnote for Claim [42].

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].

34. Claim 56

- i) **[56.pre] An electronic device for completing a payment transaction, the electronic device comprising:**

219. *Supra* Element [39.pre] (reciting same limitation).

- ii) **[56.a] a processor;**

220. *Supra* Element [1.b] (reciting same limitation).

- iii) **[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;**

221. *Supra* Element [39.b] (reciting similar limitation).

- iv) **[56.c] a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;**

222. *Supra* Element [29.c] (reciting same limitation).

v) **[56.d] a user interface coupled to the processor;**

223. *Supra* Element [39.d] (reciting same limitation).

vi) **[56.e] a user input device coupled to the processor;
and,**

224. *Supra* Element [39.e] (reciting same limitation).

vii) **[56.f] wherein said processor is operable to:**

225. *Supra* Element [39.f] (reciting same limitation).

viii) **[56.f.i] responsive to a priming operation, wherein the
priming operation is operable to ready the device to
perform the payment transaction,**

226. *Supra* Element [39.f.i] (reciting same limitation).

ix) **[56.f.ii] cause the display of information associated
with the payment request;**

227. *Supra* Element [39.f.ii] (reciting same limitation).

x) **[56.f.iii] cause the display of an image representing the
user-selectable issued payment account; and,**

228. *Supra* Element [39.f.iii] (reciting similar limitation).

xi) **[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,**

229. *Supra* Element [39.f.iv] (reciting similar limitation).

- xii) **[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;**

230. *Supra* Element [39.f.v] (reciting similar limitation).

- xiii) **[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**

231. *Supra* Element [39.g] (reciting same limitation).

- xiv) **[56.h] wherein the user interface is operable to provide an indication of the transaction status information.**

232. *Supra* Element [39.h] (reciting similar limitation).

- 35. Claim 57: The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device.**

233. *Supra* Element [40] (reciting same limitation).

- 36. Claim 58: The device of claim 57, wherein the payment authority information comprises a static device account number.**

234. *Supra* Element [42] (reciting similar limitation).

- 37. Claim 59: The device of claim 58, wherein the payment authority information further comprises a static device account expiration date.**

235. *Supra* Element [43] (reciting similar limitation).

38. Claim 60: The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority.

236. *Supra* Element [41] (reciting similar limitation).

39. Claim 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.

237. *Supra* Element [44] (reciting same limitation).

40. Claim 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.

238. As I discussed for Claim [2], the authentication cryptogram (“dynamically generated limited-use payment information”) is a cryptogram number (“comprises a cryptogram number”). As I 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 (“is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account”). *Supra* Elements [4.pre]-[4.b].

- 41. Claim 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.**

239. *Supra* Claim [44] (reciting same limitation).

- 42. Claim 64: The device of claim 63, wherein the payment authority information comprises a static device account number.**

240. *Supra* Claim [58] (reciting same limitation).

- 43. Claim 65: The device of claim 64, wherein the payment authority information further comprises a static device account expiration date.**

241. *Supra* Claim [59] (reciting same limitation).

- 44. Claim 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.**

242. *Supra* Claim [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”).

- 45. Claim 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.

243. *Supra* Claim [50] (reciting similar limitation); Claim [66] (explaining how a touch panel is also a “touch screen interface”).

46. Claim 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.

244. *Supra* Claim [51] (reciting similar limitation).

47. Claim 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.

245. *Supra* Claim [52] (reciting similar limitation); Claim [66] (explaining how a touch panel is also a “touch screen interface”).

48. Claim 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.

246. The Gomez-Amacker-Casey-Law combination discloses “wherein said user interface comprises a display” for the same reasons as I discussed for Claim [49]. As I 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]. 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 I discussed for Claim [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”).

49. Claim 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.

247. *Supra* Claim [54].

50. Claim 72

i) [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

248. *Supra* Elements [55.pre]-[55.a] (reciting similar limitations).

ii) [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

249. *Supra* Element [55.b] (reciting similar limitation).

- iii) **[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**

250. *Supra* Claim [62] (reciting similar limitation).

C. Ground 1C: Claim 13 of the '634 Patent is Rendered Obvious Under 35 U.S.C. § 103 (pre-AIA) by Gomez in view of Amacker, Casey, and Chin

251. In my opinion, the combination of Gomez, Amacker, Casey, and Chin renders obvious as a whole claim 13 of the '634 Patent for at least the reasons discussed below.

- 1. Claim 13: The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.**

252. As I discussed for Ground 1A, the Gomez-Amacker-Casey combination renders obvious this limitation because a known fingerprint swipe gesture is a "known user touch gesture," as is a known PIN entry (under Patent Owner's interpretation of the limitation). *Supra* Ground 1A, Element [13] (Section IX.A.10).

253. 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 that given authorized user (“known user touch gesture”), to determine whether an authorized user is attempting to use the device (“wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture”).

254. 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.

255. Thus, Chin discloses that a user may generate a known security/unlocking tactile pattern (“wherein said predetermined user characteristics...comprise a known user touch gesture”) that is stored in the

phone's memory ("predetermined user characteristics stored within the electronic device") and compared to an entered tactile pattern to determine whether an authorized user is attempting to use the phone (thus unlocking the phone or certain features if the patterns match).

256. 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. 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. Accordingly, a POSITA would have been motivated to implement a tactile pattern gesture as an unlocking mechanism, e.g., as an alternative to a PIN entry, to improve speed, efficiency, and accessibility for users.

257. 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.

XI. JURAT

258. In signing this Declaration, I understand that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear remotely for cross-examination within the United States during the time allotted for cross-examination.

259. I hereby declare that all statements made in this Declaration of my own knowledge are true, that all statements made on information and belief are believed to be true, and further, that these statements are made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: July 24, 2025

By: Michael I. Shamos

Michael I. Shamos, Ph.D