

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: David Wyatt
U.S. Patent No.: 10,810,579 Attorney Docket No.: 39843-0145IP1
Issue Date: October 20, 2020
Appl. Serial No.: 16/459,150
Filing Date: July 1, 2019
Title: SMART TOKENIZING PAYMENT CARD AND DEVICE AND
TRANSACTION PROCESSING THEREOF, SYSTEM AND
METHOD

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES
PATENT NO. 10,810,579 PURSUANT TO 35 U.S.C. §§ 311–319,
37 C.F.R. § 42

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
A.	Grounds for Standing	1
B.	Challenge and Relief Requested	1
C.	Claim Construction	3
II.	THE '579 PATENT	3
A.	Brief Description	3
B.	Level of Ordinary Skill in the Art	5
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE	5
A.	[GROUND 1A] – Obviousness based on Royyuru-Phillips-Casey (Claims 1-4, 6-9, 11-12, 15-20, 22-23)	5
1.	Royyuru	5
2.	Phillips	7
3.	Casey	8
4.	Royyuru-Phillips-Casey Combination	10
5.	Application of Royyuru-Phillips-Casey	16
B.	[GROUND 1B] – Obviousness based on Royyuru-Phillips-Casey-Gomez (Claim 5)	47
1.	Royyuru-Phillips-Casey-Gomez Combination	47
2.	Application of Royyuru-Phillips-Casey-Gomez	49
C.	[GROUND 1C] – Obviousness based on Royyuru-Phillips-Casey-Deibert (Claims 10, 14)	50
1.	Royyuru-Phillips-Casey-Deibert Combination	50
2.	Application of Royyuru-Phillips-Casey-Deibert	52
D.	[GROUND 1D] – Obviousness based on Royyuru-Phillips-Casey-Deibert-Power (Claim 13)	55
E.	[GROUND 1E] – Obviousness based on Royyuru-Phillips-Casey-Carlson (Claims 4, 21, 22)	57
1.	Royyuru-Phillips-Casey-Carlson Combination	57
2.	Application of Royyuru-Phillips-Casey-Carlson	58
F.	[GROUND 2A] – Obviousness based on Gomez-Amacker-Mullen-Smith (Claims 1-9, 11-12)	59
1.	Gomez	59
2.	Amacker	60
3.	Mullen	61
4.	Smith	62
5.	Gomez-Amacker-Mullen-Smith Combination	63

G.	[GROUND 2B] – Obviousness based on Gomez-Amacker-Mullen-Smith-Deibert (Claims 10, 14)	83
H.	[GROUND 2C] – Obviousness based on Gomez-Amacker-Mullen-Smith-Deibert-Power (Claim 13)	84
I.	[GROUND 2D] – Obviousness based on Gomez-Amacker-Mullen (Claims 15-20, 22-23).....	85
J.	[GROUND 2E] – Obviousness based on Gomez-Amacker, Mullen-Smith-Carlson (Claim 4).....	90
K.	[GROUND 2F] – Obviousness based on Gomez-Amacker-Mullen-Carlson (Claim 22).....	91
L.	[GROUND 2G] – Obviousness based on Gomez-Amacker-Mullen-Carlson-Royyuru (Claim 21)	92
IV.	DISCRETIONARY CONSIDERATIONS	93
V.	CONCLUSION AND FEES	95
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	95
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	95
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2).....	95
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	96
D.	Service Information	96

EXHIBITS

- SAMSUNG-1001 U.S. Patent No. 10,810,579 to Wyatt (“the ’579 Patent”)
- SAMSUNG-1002 Excerpts from the Prosecution History of the ’579 Patent (“the Prosecution History”)
- SAMSUNG-1003 Declaration and Curriculum Vitae of Dr. Michael Ian Shamos
- SAMSUNG-1004 U.S. Patent Publication No. 2010/0185545 to Royyuru et al. (“Royyuru”)
- SAMSUNG-1005 U.S. Patent Publication No. 2012/0310760 to Phillips et al. (“Phillips”)
- SAMSUNG-1006 U.S. Patent No. 8,255,323 to Casey et al. (“Casey”)
- SAMSUNG-1007 U.S. Patent No. 9,600,808 to Gomez, Sr. et al. (“Gomez”)
- SAMSUNG-1008 U.S. Patent No. 8,423,462 to Amacker et al. (“Amacker”)
- SAMSUNG-1009 PCT Publication No. WO2012/154915 to Mullen et al. (“Mullen”)
- SAMSUNG-1010 U.S. Patent Publication No. 2013/0232083 to Smith et al. (“Smith”)
- SAMSUNG-1011 U.S. Patent Publication No. 2008/0017704 A1 to VanDeburg et al. (“VanDeburg”)
- SAMSUNG-1012 U.S. Patent Publication No. 2008/0172317 to Deibert et al. (“Deibert”)
- SAMSUNG-1013 U.S. Patent Publication No. 2008/0319905 to Carlson (“Carlson”)
- SAMSUNG-1014-1015 [RESERVED]
- SAMSUNG-1016 U.S. Patent No. 8,052,052 to Power (“Power”)

SAMSUNG-1017-1021 [RESERVED]

SAMSUNG-1022 PCI Data Security Standard (PCI DSS), Information Supplement: PCI DSS E-commerce Guidelines (January 2013)

SAMSUNG-1023-1024 [RESERVED]

SAMSUNG-1025 Kadambi et al., *Near-Field Communication-Based Secure Mobile Payment Service*, ACM 11th International Conference on Electronic Commerce 2009

SAMSUNG-1026 PCI Data Security Standard, Navigating PCI DSS: Understanding the Intent of the Requirements, Version 2.0 (October 2010)

SAMSUNG-1027-1028 [RESERVED]

SAMSUNG-1029 Todd Wasserman, *New Credit Card has LCD Screen, Touch-Sensitive Buttons*, The Sydney Morning Herald (Nov. 9, 2012)

SAMSUNG-1030 PCI Data Security Standard (PCI DSS), Information Supplement: PCI DSS Tokenization Guidelines, Version 2.0 (August 2011)

SAMSUNG-1031-1099 [RESERVED]

SAMSUNG-1100 Complaint for Patent Infringement, *Cardware Inc. v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-cv-00141 (E.D. Tex. May 11, 2022)

SAMSUNG-1101 Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022)

SAMSUNG-1102 Exhibit A to CardWare Inc.'s P.R. 3-1 Disclosure of Asserted Claims and Infringement Contentions, *Cardware Inc. v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-cv-00141 (E.D. Tex. (Sept. 8, 2022)

- SAMSUNG-1103 United States District Courts National Judicial Caseload Profile, *available at* https://www.uscourts.gov/sites/default/files/fcms_na_distprofile0630.2022_0.pdf (retrieved November 11, 2022)
- SAMSUNG-1104 Sample Docket Control Order for Patent Cases, *Cardware Inc. v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-cv-00141 (E.D. Tex.)
- SAMSUNG-1105 Plaintiff CardWare Inc's Disclosure of Asserted Claims and Infringement Contentions, *Cardware Inc. v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-cv-00141 (E.D. Tex. (Sept. 8, 2022))

LIST OF CHALLENGED CLAIMS

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

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

Claim Element	Claim Language
	one unverifiable condition, of a set of unverifiable conditions comprising: an invalid number generation; an invalid device account number; a use outside of a valid time window; an invalid re-use of a limited-use number; and an invalid use of an expired limited-duration number.
[7]	The method of claim 1, wherein the receiving an input at an electronic device comprises receiving an input via a user interface from one of the set of user interfaces comprising: a device button; a device touch-screen interface; a device touch ID button interface; a device optical sensor array; a device skin touch sensor; a skin-contact sensor; a device motion detection interface; a device biometric sensor interface; and a device user-interface selection.
[8]	The method of claim 1, wherein the priming operation comprises one operation of the set of operations comprising: a button press; a touch ID button press; a button double-press; a touch ID sensor touch; a touch-screen touch; a touch-input sequence; a gesture or swipe over a sensor-array; a skin-contact sense; an optical-sensor array sense; an electronic device tap; a sequence of motions of the electronic device; a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation; and, further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a touching from an identified valid user; a user entry of a valid passcode; a user entry of a valid PIN; swiping of a recognized user skin over a device sensor array; a correct user swiping or gesturing on the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motioning of the electronic device; a skin-contact sensing of an identified user; a device biometric sensing of a valid user identity; and a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user.
[9.a]	The method of claim 1, further comprising: obtaining, by the electronic device, a user payment approval, through at least one device user interface of a set of interfaces comprising: a device display interface; a device touch-screen display interface; a device touch interface; device input buttons; device key-pad inputs, a device optical sensor array; a device motion detection unit; a device accelerometer; a device biometric user-sensor; and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user; and

Claim Element	Claim Language
[9.b]	displaying, on the display, at least one information of a set of information comprising: a priming status of the electronic device for payment; a default payment method; a plurality of selectable payment accounts; a payment request; transaction information; a payment amount; a merchant identification; a time; an expiration date; a location; an account balance; a payment bank logo; a card image; a payment card issuer icon; a payment card network icon; the last 4-digits of the primary account number; the last 4-digits of the device account number; and other payment iconography; and
[9.c]	receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.
[10]	The method of claim 1, further comprising: activating an NFC communication for a limited duration of time responsive to the electronic device priming; and responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction.
[11]	The method of claim 1, further comprising completing the transaction on the electronic device, wherein the completing further comprises: receiving an authorization input on the electronic device from a valid device user, in response to at least one of a set of exceptional conditions comprising: the electronic device leaving the proximity of the NFC recipient; the incomplete identifying of a valid device user; the electronic device leaving the user's possession; the electronic device leaving the proximity contact of the user; the electronic device leaving the grasp of the user; a biometric sensing the electronic device leaving the possession of a user since a last user validation; the transaction exceeding a pre-set amount limit; the transaction interval exceeding a pre-set time duration; a card issuing authority requesting a security check; and presenting the user with at least one of a set of selectable options comprising: requesting a transaction payment; continuing with the default payment method; selecting an alternate payment account; inputting an approval authorization; inputting a transaction denial; and inputting an adjustment of the transaction payment.
[12]	The method of claim 1, further comprising: subsequent to the priming operation, offering a user selection of payment options for user input selection by presenting a selection of payment options in graphical format on said touch-screen display, including at least one of: a last four

Claim Element	Claim Language
	digits of a payment account number portion; a last four digits of a device account number portion; an expiration date; a card issuer icon; a bank logo; a card processing network logo; a card image; a card payment network icon; graphical images associated with the payment account; accepting a user input selection of a payment option, from said payment options, via said touch-screen display; and proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options.
[13]	A method of claim 1, wherein the priming operation comprises: a button double press; and a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation; and further comprising: denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user, until after successfully re-validating a user; and wherein re-validating a user requires a correct user passcode re-entry; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.
[14]	A method of claim 1, wherein the priming operation is input after at least one of: a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device, and validating a user passcode entry on the touch-screen display of the electronic device; disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.
[15.pre]	A method of performing a transaction, the method comprising:
[15.a]	receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient proximity communication request to an NFC interface of the electronic device;
[15.b]	displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device;
[15.c]	receiving, from a valid device user, a payment selection and approval authorization input on the electronic device;

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

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

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

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

Samsung Electronics Co., Ltd. (“Petitioner” or “Samsung”) petitions for *In-ter Partes* Review (“IPR”) of claims 1-23 (“the Challenged Claims”) of U.S. Patent No. 10,810,579 (“the ’579 Patent”).

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the ’579 Patent is available for IPR and that Samsung is not estopped from requesting IPR.

B. Challenge and Relief Requested

Petitioner requests IPR of the Challenged Claims on the grounds listed below. A declaration of Dr. Michael Shamos (SAMSUNG-1003) supports this Petition.

Ground	Claim(s)	35 U.S.C. § 103
1A	1-4, 6-9, 11-12, 15-23	Royyuru-Phillips-Casey
1B	5	Royyuru-Phillips-Casey-Gomez
1C	10, 14	Royyuru-Phillips-Casey-Deibert
1D	13	Royyuru-Phillips-Casey-Deibert-Power
1E	4, 21, 22	Royyuru-Phillips-Casey-Carlson
2A	1-9, 11-12	Gomez-Amacker-Mullen-Smith
2B	10, 14	Gomez-Amacker-Mullen-Smith-Deibert
2C	13	Gomez-Amacker-Mullen-Smith-

Ground	Claim(s)	35 U.S.C. § 103
		Deibert-Power
2D	15-20, 22-23	Gomez-Amacker-Mullen
2E	4	Gomez-Amacker-Mullen-Smith-Carlson
2F	22	Gomez-Amacker-Mullen-Carlson
2G	21	Gomez-Amacker-Mullen-Carlson-Royyuru

The '579 patent claims priority to a provisional application filed on March 15, 2013 (“Critical Date”). Petitioner has applied prior art that predates this date and has used the Critical Date as the date of invention for purposes of this IPR.¹

The references are prior art under 35 U.S.C. §102.

Reference	Filing Date	Publication Date
Royyuru	01/22/2009	07/22/2010
Phillips	09/01/2011	12/06/2012
Casey	01/09/2009	08/28/2012

¹ Petitioner does not concede that any of the Challenged Claims enjoy priority to March 15, 2013. SAMSUNG-1003, ¶¶24-25. The analysis here remains the same regardless of whether March 15, 2013 or March 17, 2014 is used as the date of invention.

Reference	Filing Date	Publication Date
Gomez	06/22/2012	03/21/2012
Amacker	05/01/2009	04/16/2013
Mullen	05/10/2012	11/15/2012
Smith	03/01/2013	09/05/2013
Deibert	01/09/2008	07/17/2008
Carlson	06/24/2008	12/25/2008
Power	12/04/2008	11/08/2011

C. Claim Construction

No formal claim constructions are presently necessary since “claim terms need only be construed to the extent necessary to resolve the controversy.” *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); *SAMSUNG-1003*, ¶75-78.²

II. THE '579 PATENT

A. Brief Description

The '579 patent describes an electronic payment card capable of generating

² Petitioner does not concede that the Challenged Claims satisfy all statutory requirements including 35 U.S.C. § 112.

a “limited-duration number” for use in a payment transaction. SAMSUNG-1001, 2:23-61, 10:4-11:55, FIG. 7. Figure 7 illustrates a process for generating and using a limited-duration number:

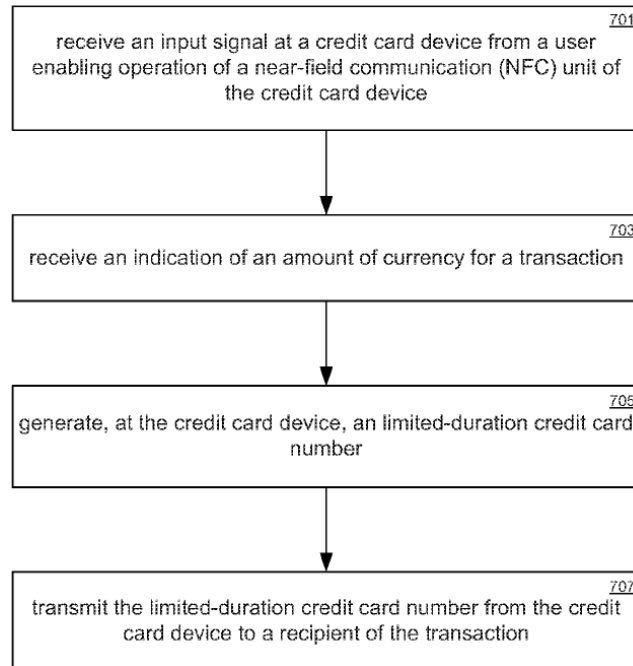


FIG. 7

SAMSUNG-1001, FIG. 7.

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

B. Level of Ordinary Skill in the Art

A person of ordinary skill as of the Critical Date of the '579 patent (“POSITA”) would have had (1) a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) one to two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technologies. SAM-SUNG-1003, ¶¶43-49. Graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

Id.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1A] – Obviousness based on Royyuru-Phillips-Casey (Claims 1-4, 6-9, 11-12, 15-20, 22-23)

1. Royyuru³

Royyuru describes a system for conducting contactless financial transactions between a smartphone or other device, and a Point-of-Sale (POS) device. SAM-SUNG-1004, [0034]-[0035], [0047]. The user device generates “a set of dynamic cryptograms that are valid for a single transaction” including a “Dynamic Transaction Cryptogram (DTC)” and a “dynamic PAN” using various information stored

³ All descriptions of the references and combinations thereof are incorporated into the mapping of each claim element throughout the petition.

on or received by the device. SAMSUNG-1004, [0005]-[0010], [0032]-[0034], [0047]-[0048], [0051], [0057]. The DTC and dynamic PAN are provided to the POS such that “[t]he transaction can be authenticated based on the DTC at the payment processor system or at the financial institution” and the real PAN can be determined to process the transaction. *Id.* FIG. 3 shows the communication flow of the system:

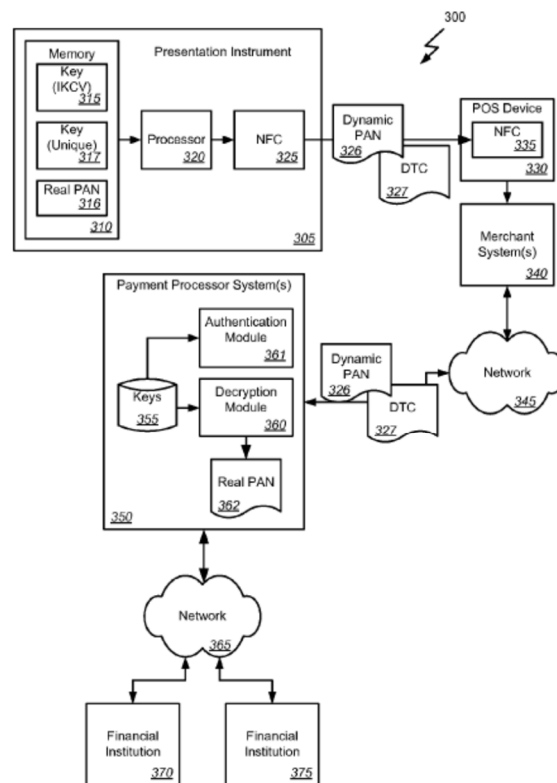


FIG. 3

SAMSUNG-1004, FIG. 3.

2. Phillips

Phillips describes a mobile telephone having a virtual wallet that allows a user to select from among multiple payment options or use “an automatic card selection option.” SAMSUNG-1005, [0017], [0029], [0033]-[0035], [0059].

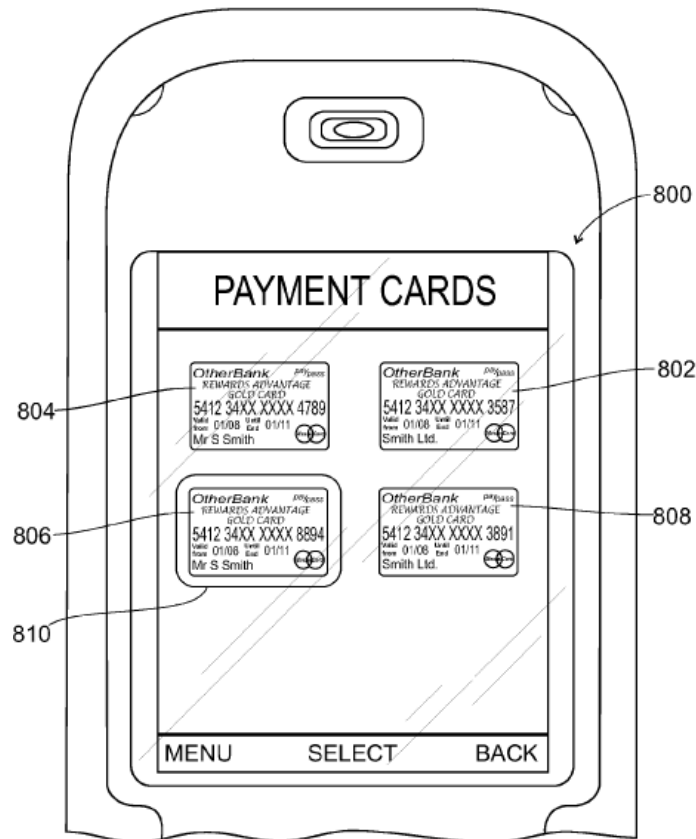


FIG. 8

SAMSUNG-1005, FIG. 8. A payment card sub-menu provides information on available payment options for user selection. SAMSUNG-1005, [0039]-[0041],

[0036]. “[T]he user may be required to enter a PIN or code before selecting a payment card” or to otherwise approve a financial transaction. SAMSUNG-1005, [0038]-[0039], [0059], [0066].

Phillips describes receiving “a payment request that includes a merchant identifier (merchant ID)” to initiate the card selection and payment transaction functions. SAMSUNG-1005, [0072]. The request can take the form of “interrogation signals” received from a POS terminal via NFC. *Id.*, [0023], [0027], [0057].

3. Casey

Casey describes a mobile payment system that allows a user “to confirm or decline a payment transaction using a selected payment instrument” before transmitting “payment information for the payment transaction...to a merchant or payment recipient.” SAMSUNG-1006, Abstract. Casey’s smartphone receives “a request for payment” via NFC or other communication, displays payment card and transaction information, and receives a PIN or user movement of a graphical element (slider) to confirm or deny a transaction. SAMSUNG-1006 8:52-9:36, 12:64-13:51, 14:12-49, 15:24-59; FIGs. 4-8. FIG. 5 shows an example user interface flow for confirming a transaction:

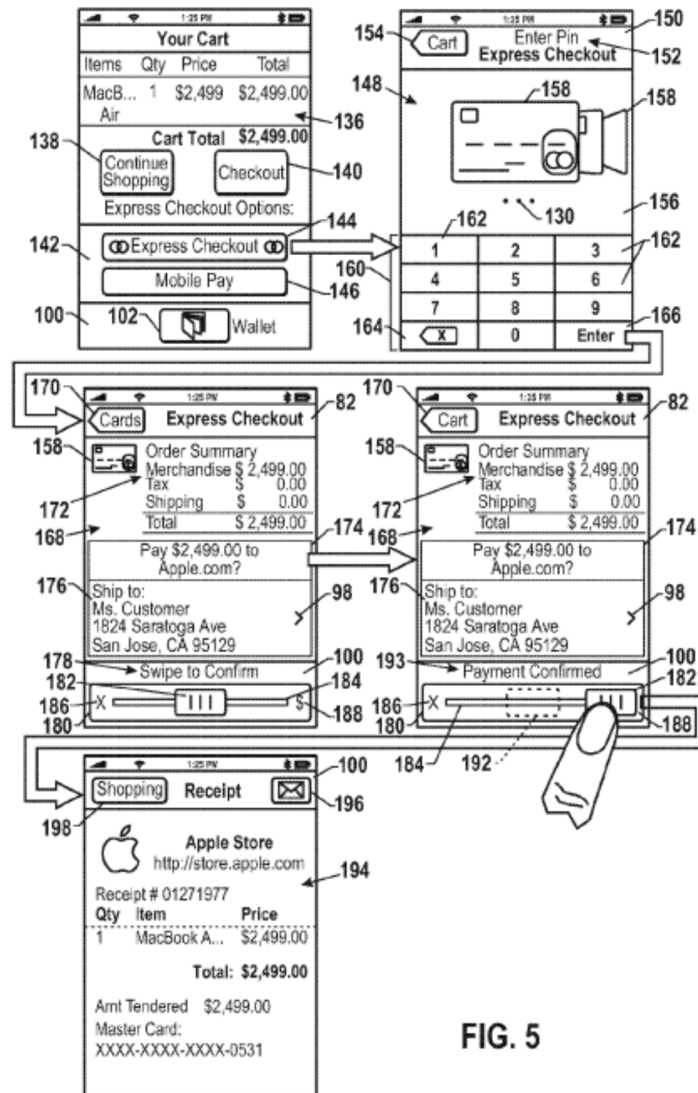


FIG. 5

After confirmation of the payment information by the payment processor, “device 10 may receive and display (block 78) a receipt for the payment transaction. For example, the receipt may identify the amount tendered, the payment recipient, and the payment instrument used.” SAMSUNG-1006, 10:47-53, 10:20-29, 16:3-20.

4. Royyuru-Phillips-Casey Combination

A POSITA would have beneficially applied the teachings of Phillips and Casey to Royyuru to modify Royyuru's mobile payment system to include multiple improvements, including additional user interface and authentication features that complement Royyuru's focus on secure cryptogram generation. SAMSUNG-1003, ¶¶130-138. First, a POSITA would have modified Royyuru based on Phillips and Casey such that the mobile device receives a payment request from a POS terminal or other merchant device that includes information regarding the merchant and transaction. SAMSUNG-1005, [0072]; SAMSUNG-1006 8:52-9:8, FIGs. 5-8; SAMSUNG-1003, ¶¶132-133. Royyuru already discloses NFC communication between the user device and merchant device and Phillips beneficially discloses that such NFC communications can include a payment request for initiating a payment transaction from a POS terminal including transaction information such as a merchant identifier. SAMSUNG-1004, [0022], [0044], [0047]; SAMSUNG-1005, [0072], [0023], [0027], [0057]. Casey discloses the additional benefit of displaying such request information including the merchant, products being purchased, price, tax, etc. on the user device as shown in FIG. 5:

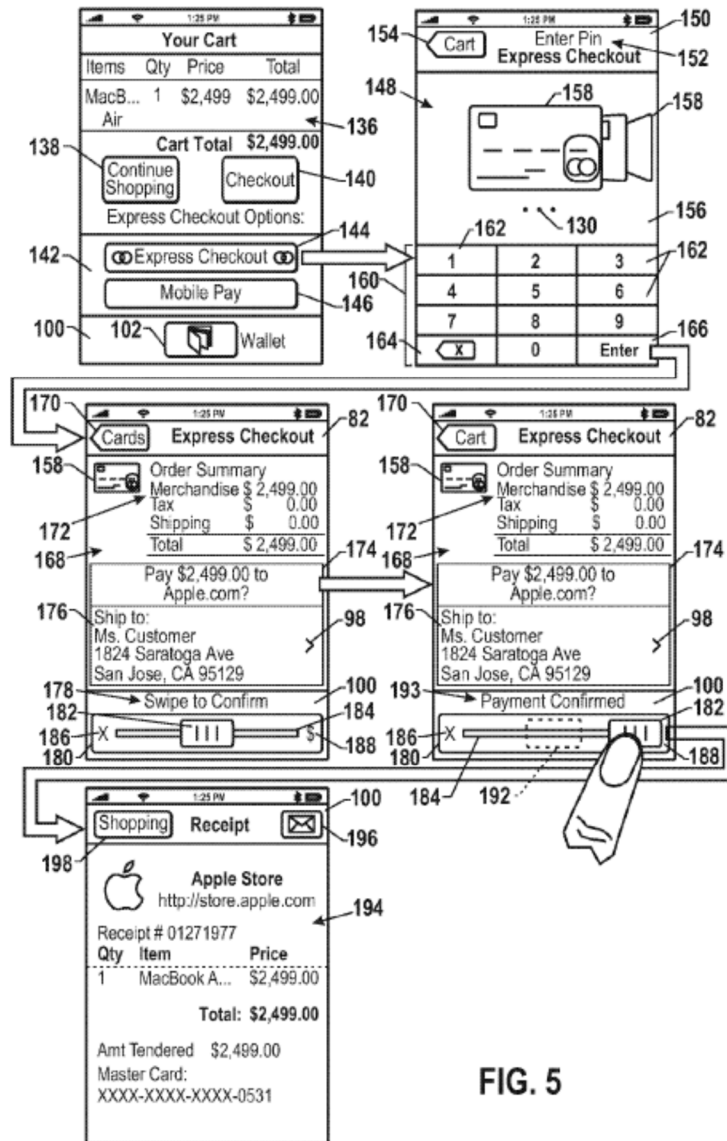


FIG. 5

SAMSUNG-1006, FIG. 5, 8:52-9:8.

Modifying Royyuru's system such that the user device receives a payment request from a merchant device would have improved the resulting system by providing information to the device that could be used to complete the payment transaction. SAMSUNG-1005, [0057]; SAMSUNG-1003, ¶¶132-133. Such a modification would have allowed the user to better ensure that they are approving a

payment transaction and transmitting payment information to a correct merchant terminal, to prevent fraudulent transmittal of payment information to an incorrect terminal. SAMSUNG-1003, ¶133. Such a modification would also allow the user to visually review transaction data before approving the transaction. SAMSUNG-1003, ¶133; SAMSUNG-1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49. Additionally, Royyuru discloses using any information “received by the presentation instrument 305...from the POS device 330 via the NFC modules” to generate the DTC and dynamic PAN and the request from the POS terminal would include such information for use in generating these cryptograms. SAMSUNG-1004, [0051]; SAMSUNG-1003, ¶133.

Second, a POSITA would have modified Royyuru based on well-known authentication and confirmation techniques as taught by Phillips and Casey such that the user authorizes the payment transaction prior to payment information being provided to the merchant terminal such as by entering a PIN (Phillips and Casey) or moving a graphical element to confirm or deny the transaction (Casey). SAMSUNG-1003, ¶134; SAMSUNG-1005, [0035], [0038]-[0039], [0047], [0059], [0066], [0061]-[0062], [0068]; SAMSUNG-1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49. Requiring the user to enter a PIN “adds a layer of security to the process” by verifying that the current user is “the owner of a selected payment card

account.” SAMSUNG-1005, [0035], [0038], [0062]; SAMSUNG-1003, ¶134. Requiring user authorization/confirmation would have provided multiple distinct improvements:

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

SAMSUNG-1003, ¶134; SAMSUNG-1005, [0035], [0047]; SAMSUNG-1006, 3:20-35, 9:9-36.

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

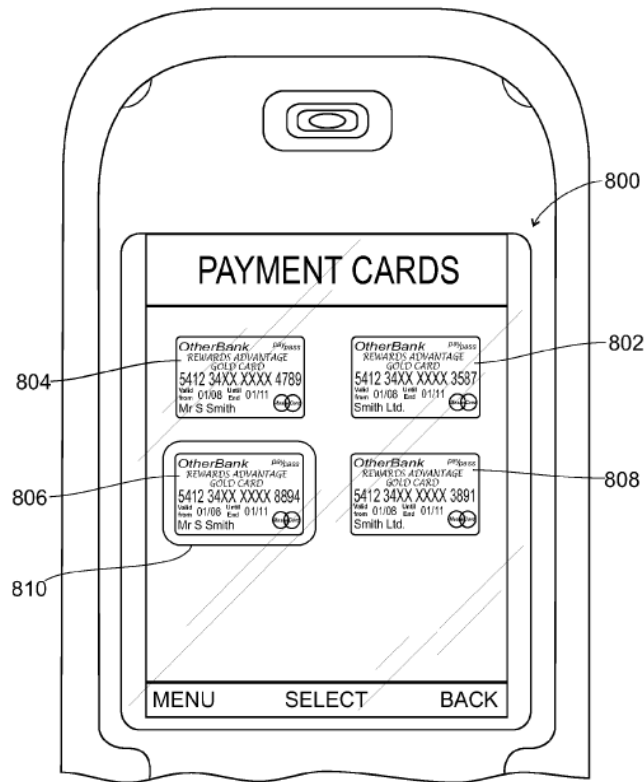


FIG. 8

SAMSUNG-1003, ¶135; SAMSUNG-1005, [0036]-[0041]; SAMSUNG-1006, 9:4-28, 9:58-10:2, 12:46-65; FIGs. 5-8. Allowing a user to select among multiple payment options would have provided more choices and options with respect to how the user spent their money, would have allowed the user to select payment options that are the most appropriate for a given scenario (e.g., due to budgeting or credit card rewards considerations), and reduced or eliminated the need for the user to carry additional physical payment options. SAMSUNG-1003, ¶135. Displaying payment method information, including card indicia, as taught by Phillips and Casey would have allowed the user to more readily recognize a desired card and

would have provided assurances that the user was selecting the correct card. SAMSUNG-1003, ¶135. A POSITA would have recognized that, in at least some and likely in most implementations, such benefits would have outweighed any minor increases in memory usage to store the additional cards and information. *Id.*

Fourth, a POSITA would have modified Royyuru based on Phillips to allow the user to preselect one or more default payment options for different transaction scenarios to “enhance[] the speed and convenience of transactions” in those specific scenarios by allowing the user to make some payments using a default payment option (thus eliminating the need to select a payment option) while providing full flexibility to select a payment option in other scenarios when the user so desires. SAMSUNG-1003, ¶136; SAMSUNG-1005, [0005], [0017], [0059], [0066], [0017], [0029].

Fifth, a POSITA would have modified Royyuru based on Casey such that the resulting device displays transaction status information, including received payment receipt information. SAMSUNG-1006, 10:47-53, 14:25-36, 16:3-20; SAMSUNG-1003, ¶137. Such a modification would have allowed the user to “confirm” that the correct transaction occurred, or more quickly take steps to correct an incorrect transaction, thus increasing user satisfaction and eventually increasing the customer base. *Id.*; SAMSUNG-1003, ¶137. The receipt could include such useful information as notification “when an order is ready to be picked

up” and maps of the pickup location. SAMSUNG-1006, 16:3-20. Such a modification would have also allowed the user to more easily keep digital records of financial transactions. *Id.*; SAMSUNG-1003, ¶137.

Finally, a POSITA would have modified Royyuru based on Phillips and Casey because doing so would have been merely the application of known techniques to a known system ready for improvement to yield predictable results. SAMSUNG-1003, ¶138; *see KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). Here, all three references describe aspects of conducting wireless payment transactions using payment information stored on or generated by a mobile device and Phillips and Casey describe improvements that would have been beneficially applied to Royyuru’s system. SAMSUNG-1003, ¶138, 131. A POSITA would have furthermore had a reasonable expectation of success in modifying the mobile payment system of Royyuru based on Phillips and Casey as they all are directed toward similar mobile payment systems with Phillips and Casey simply providing additional details on known user interfaces and security measures. *Id.*

5. Application of Royyuru-Phillips-Casey

[1.pre]

To the extent the preamble is treated as limiting, Royyuru describes “method[s] of processing a financial transaction” using “a mobile device.” SAMSUNG-1004, [0005]-[0010], [0002], [0035]. SAMSUNG-1003, ¶139.

[1.a]

Royyuru describes “[w]hen the cardholder wishes to execute a transaction, such as a financial transaction...[he] *passes or taps the presentation instrument 305 on or near the point-of-sale device 330.*” SAMSUNG-1004, [0047], *see also* [0005], [0044], [0050], [0053]; SAMSUNG-1003, ¶140. Phillips teaches that in the resulting combination the user is required to “enter a PIN” to initiate a financial transaction and “add[] a layer of security to the process.” SAMSUNG-1005, [0035], [0038]-[0039], [0066]. A POSITA would have recognized that entry of a correct “personal identification number” identifies the user as valid. SAMSUNG-1003, ¶140; SAMSUNG-1005, [0035], [0038].

[1.b]

The “device for initiating a financial transaction related to a financial account can comprise *a processor.*” SAMSUNG-1004, [0007]; SAMSUNG-1003, ¶141.

[1.c]

Royyuru describes “a mobile device” such as “a cellular telephone [or] Personal Digital Assistant (PDA).” SAMSUNG-1004, [0021], [0040]. Royyuru incorporates by reference a patent publication that describes that the mobile device “include[s] a touch screen” display. SAMSUNG-1004, [0021]; SAMSUNG-1011, [0006]; SAMSUNG-1005, [0018]; SAMSUNG-1006, 3:10-19; SAMSUNG-1003, ¶¶142, 60-63.

[1.d]

Royyuru's mobile device includes "an NFC module 325 communicatively coupled with the processor 320." SAMSUNG-1004, [0051], [0046], [0002], [0022]; SAMSUNG-1003, ¶¶143, 55-59.

[1.e]

Royyuru's device can "detect initiation of the transaction." SAMSUNG-1004, [0009]. The device uses NFC for "close proximity...short range communications between [the] mobile device and [the] POS device." *Id.*, [0022], [0044], [0047], [0057] (describing transmission of UN to device via NFC); SAMSUNG-1005, [0023]. Phillips discloses that in the resulting combination "the mobile device...receives 1302 a payment request that includes a merchant identifier (merchant ID)" from a POS terminal via NFC. SAMSUNG-1005, [0072], [0023], [0027], [0057]; *see also* SAMSUNG-1006 8:52-9:8; FIGs. 5-8; SAMSUNG-1003, ¶144.

[1.f]

FIG. 8 of Phillips shows "a 'Payment Cards' sub-menu" showing faces of "payment card account[s] issued to" the user to allow "selection of the payment card account that corresponds to the payment card represented by the card-face image." SAMSUNG-1005, [0039]-[0041]; SAMSUNG-1003, ¶¶145-148.

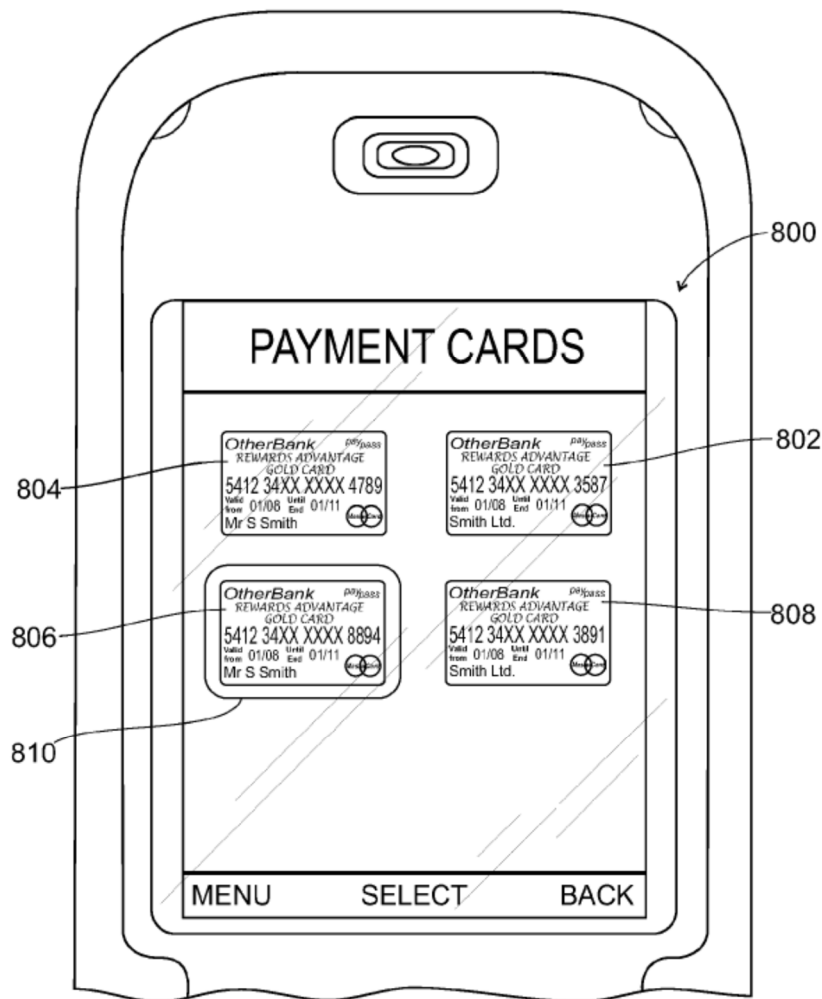


FIG. 8

SAMSUNG-1005, FIG. 8. The menu allows a user to “select one of the payment cards...to use in a current transaction.” *Id.*, [0037], [0039]; *see also* SAMSUNG-1006, 9:4-28, 9:58-10:2, 12:46-65. The displayed payment cards “include information such as the payment card account number [and] issuer bank name.” SAMSUNG-1005, [0039], [0036]. As shown in FIG. 8, the displayed issuer card account numbers are partial numbers with the last four digits displayed. *Id.*, FIGs. 8,

11; SAMSUNG-1003, ¶146. To the extent this element is interpreted narrowly, it would have been obvious to a POSITA to display *only* the last four digits of the issuer card account numbers to further enhance security by obscuring a larger portion of the credit card number while providing enough of the number to facilitate easy card recognition/selection by a user. SAMSUNG-1003, ¶¶147-148; SAMSUNG-1004, [0032] (describing displaying only the last four digits of “the real PAN” on a payment receipt for security purposes).

[1.g]

As shown in FIGs. 8 and 11 of Phillips, the Royyuru-Phillips-Casey combination provides that an “issuer logo” is displayed on the touchscreen. SAMSUNG-1005, [0039], [0036], [0041], [0058], [0065]; SAMSUNG-1003, ¶¶149-151.

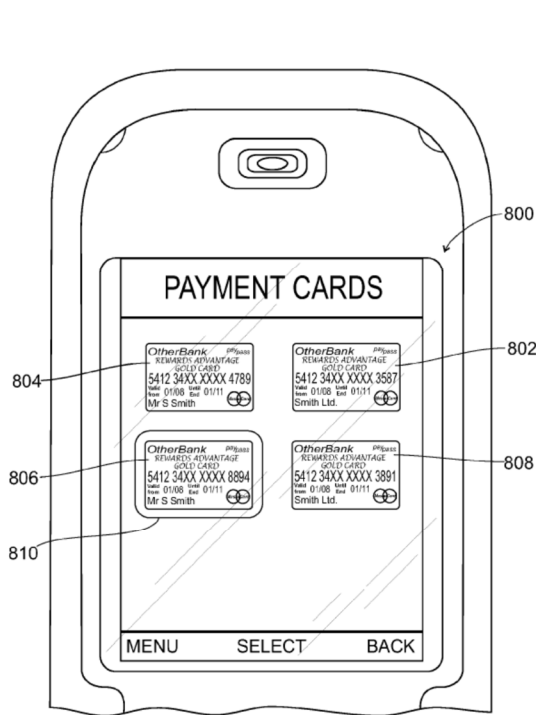


FIG. 8

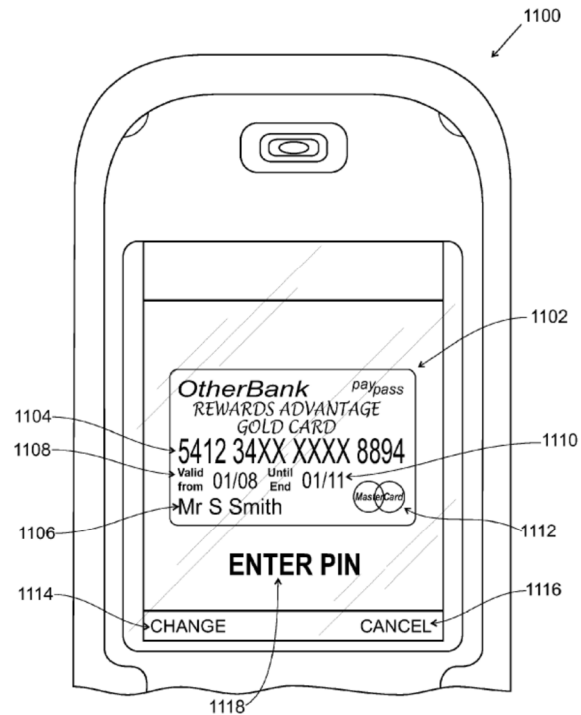


FIG. 11

SAMSUNG-1005, FIGs. 8, 11.

[1.h]

As shown in FIGs. 8 and 11 of Phillips, *supra*, the displayed card-face “include[s] information such as the payment card account number, issuer bank name, issuer logo, card account holder name, the expiration date, a unique color or color combination, and/or other pertinent data.” SAMSUNG-1005, [0039], [0041], [0036]; SAMSUNG-1003, ¶¶152-154.

[1.i]

Royyuru provides at least two examples of the claimed “limited-use payment information”: the “Dynamic Transaction Cryptogram (DTC)” and the “dy-

namic PAN.” SAMSUNG-1004, [0005]-[0010], [0032]-[0033], [0047]; SAMSUNG-1003, ¶¶155-156. “A Dynamic Transaction Cryptogram (DTC) can be *generated at the device*, using a unique card level key stored on the device.” SAMSUNG-1004, [0005]. In another example, “[t]he DTC can be computed by the device by combining several fields including the PAN, service code, expiration date, unpredictable number, and ATC and encrypting them using the CK.” *Id.*, [0057]. The CK “is unique per card” and therefore the DTC is limited in use to the specific user device. *Id.*, [0057], [0032] (explaining that the term “card” refers to “a smart card” or “other device adapted for use as a payment instrument”), [0021]; SAMSUNG-1003, ¶155.

Similarly the dynamic PAN is generated by the user device “based on the real PAN and an Institution Key Card Variant (IKCV) stored on the device.” SAMSUNG-1004, [0005]. In another example, the dynamic PAN is “computed by the device for each transaction by combining the digits from the card number with the ATC and with the unpredictable number sent by the RFID or NFC reader and then encrypting these digits with the IKCV.” *Id.*, [0057]. Both the DTC and dynamic PAN are “valid for a single transaction” and are therefore limited-use. *Id.*, [0033]. The dynamic pan or “Pseudo-PAN can be sent in place of the real PAN.” *Id.*, [0057], [0007], [0032]; SAMSUNG-1003, ¶156. In other examples, Royyuru describes “providing the DTC and dynamic PAN to a Point-of-Sale (POS) device”

and “from the POS device to a payment processor system” rather than the real PAN. SAMSUNG-1004, [0006]-[0010].

[1.j]

Royyuru describes “[t]he device can then provide the DTC 327 and the dynamic PAN 326 to the NFC module 325” and then “providing the dynamic PAN to a Point-of-Sale (POS) device” via the NFC interface. *Id.*, [0051]-[0052], [0034], [0047], [0054], [0057]; SAMSUNG-1003, ¶157.

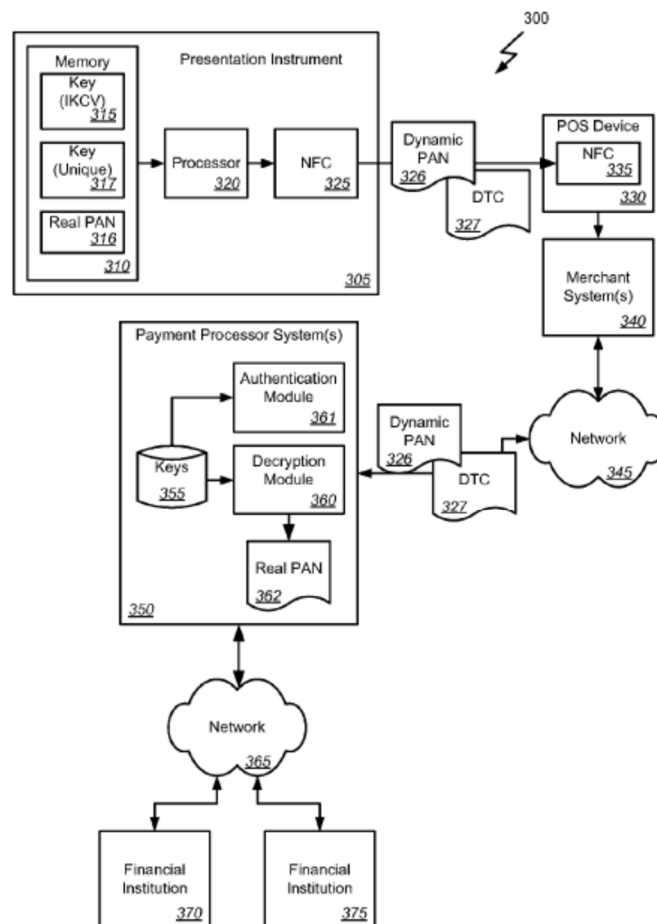


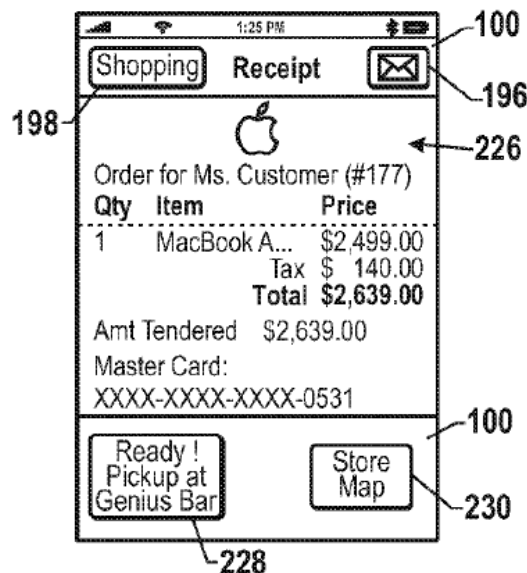
FIG. 3

SAMSUNG-1005, FIG. 3.

[1.k]

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

For example, the receipt may identify the amount tendered, the payment recipient, and the payment instrument used.” SAMSUNG-1006, 10:47-53, *see also* 10:20-29, 16:3-20; SAMSUNG-1003, ¶¶158-159.



SAMSUNG-1006, FIG. 8.

[2]

Royyuru describes that “[t]he DTC can be computed by the device by combining several fields including the **PAN**, **service code**, expiration date, **unpredictable number**, and **ATC** and encrypting them using the **CK**.” SAMSUNG-1004, [0057]. Similarly, in one example, the dynamic PAN is computed using “the **digits from the card number** with the **ATC** and with the **unpredictable number**

sent by the **RFID or NFC reader** and then encrypting these digits with the **IKCV.**” *Id.* The PAN/card number are payment information; the unpredictable number is transaction, device, merchant, NFC recipient, and payment reader information; the IKCV and CK are card issuer keys; the IKCV is a device account number; and the ATC is a device transaction sequence counter or device secret keys. SAMSUNG-1004, [0004], [0006], [0057], [0047] (“time of day”), [0051]; SAMSUNG-1003, ¶¶160-163.

[3]

The *Dynamic Transaction Cryptogram* (DTC) can be computed using “the **PAN**, **service code**, expiration date, **unpredictable number**, and **ATC** and encrypting them using the **CK.**” SAMSUNG-1004, [0005], [0057]; SAMSUNG-1003, ¶¶164-169. The ATC is an “Application Transaction Counter” which “increments for each transaction.” *Id.* The “Institution Key Card Variant (IKCV)” is a card-level key. *Id.*, [0005]-[0006], [0057] (referring to “card-level key” as “CK”). The IKCV is “generated when each card (device) is being customized” by the payment processor or financial institution using “an institution key for that issuer;” therefore it is (or is derived from) a payment issuer secret. SAMSUNG-1004, [0057], [0046]; SAMSUNG-1003, ¶165. The IKCV also is computed using a “Device Sequence number” and is therefore both a device account number and device

identifier. SAMSUNG-1004, [0091]-[0096], [0057]; SAMSUNG-1003, ¶165. The unpredictable number can be “a time of day.” SAMSUNG-1004, [0047].

The DTC is provided to a POS terminal then to a payment processor. SAMSUNG-1004, [0006]-[0010], [0051]-[0052], [0034], [0054], [0057].

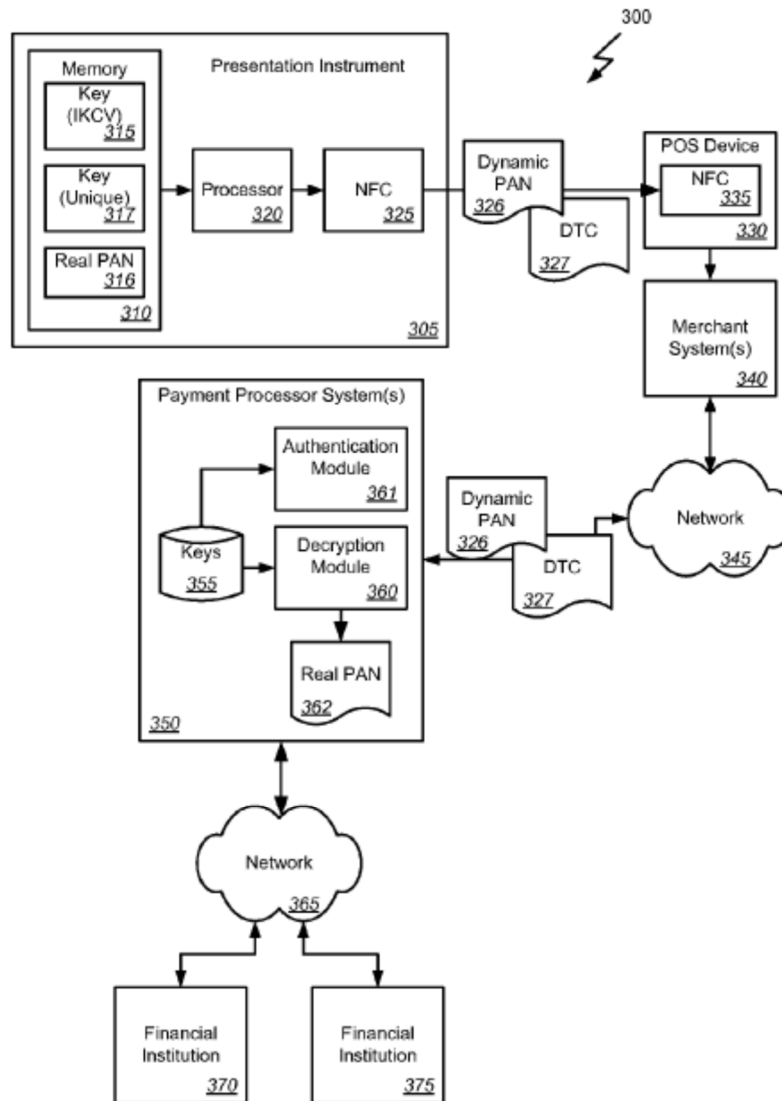


FIG. 3

SAMSUNG-1004, FIG. 3.

The “[p]ayment processor network can validate the DTC and decline the transaction if the DTC is incorrect” and is therefore utilized in the resulting Royyuru-Phillips-Casey system in place of a card validation value originated from the card issuer. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶167. The DTC is provided as “Track 1” “verification information” that is conveyed from the merchant system to the payment processor to validate the payment information. SAMSUNG-1004, [0049]. As would have been recognized by a POSITA, this Track 1 data differs from standard Track 1 data in that it does not include a CVC, CVC3, CVV, or similar card validation value. SAMSUNG-1003, ¶¶167, 280; *see, e.g.* SAMSUNG-1005, [0059]. Therefore, a POSITA would have recognized that the DTC is provided in place of a card validation value originated from the card issuer to validate the payment information. SAMSUNG-1003, ¶167.

Royyuru’s “set of dynamic cryptograms...are *valid for a single transaction*.” SAMSUNG-1004, [0005], [0033], [0053], Abstract. This is because the ATC, which “increments for each transaction,” is used in the DTC calculation. *Id.*, [0057], [0084]; SAMSUNG-1003, ¶168.

[4]

Royyuru’s IKCV is a device account number. SAMSUNG-1003, ¶¶170-176. The IKCV is “generated when each card (device) is being customized” and is generated by the payment processor *or issuer* based on the PAN and “institution key

of the issuer of the account.” SAMSUNG-1004, [0057], [0046], [0033], [0055] (“IKCV *of the device*”). SAMSUNG-1003, ¶171. Because the IKCV can be generated by the issuer, a POSITA would have recognized that it is provided, either directly or indirectly, to the device for use by the device in payment transactions. SAMSUNG-1003, ¶171; SAMSUNG-1004, [0046], [0033], [0055], [0057]. A POSITA would have therefore recognized the IKCV as a device account number because it is specific to the device and based on payment account information. SAMSUNG-1003, ¶171. Royyuru describes that the IKCV is a card-level key (CK). SAMSUNG-1004, [0006], [0057]. The DTC is generated using one of the card-level keys (such as the IKCV) and the dynamic PAN is generated using the IKCV and therefore each comprises the device account number. SAMSUNG-1004, [0057], [0005]-[0009].

The “expiration date” of the payment account is also used in generating the IKCV. SAMSUNG-1004, [0091]-[0096]. As would have been recognized by a POSITA, the IKCV has a limited time-duration of valid use because after the expiration date has expired, a new IKCV would need to be generated based on the new expiration date to match the valid account information having the new expiration date. SAMSUNG-1003, ¶172. Alternatively, it would have been obvious to a POSITA to make the IKCV of a limited time-duration of valid use tied to the payment account expiration date so that an IKCV generated using an expired PAN

could not be used for transactions. SAMSUNG-1003, ¶172. This would help ensure that the user's account is still valid. *Id.*

As yet another alternative, a POSITA would have recognized that the dynamic PAN itself is a device account number. SAMSUNG-1003, ¶173. The dynamic PAN is a dynamic "Primary *Account Number*." SAMSUNG-1004, [0005]-[0009]. The dynamic PAN is generated by the device for limited-use in a payment transaction performed by the device, making the dynamic PAN specific to the device, and therefore the dynamic PAN comprises a *device* account number. *Id.*, [0005]-[0010], [0032], [0057]. The dynamic PAN is generated at least in part on information provided by the issuer (including the real PAN). SAMSUNG-1004, [0057], [0005]. The dynamic PAN "is valid for a single transaction" and therefore has a limited time duration of valid use (the single transaction). SAMSUNG-1004, [0033]; SAMSUNG-1003, ¶173.

The DTC and dynamic PAN are both generated at the device (SAMSUNG-1004, [0005]-[0010]) and therefore both separately and together comprise device generated payment information. SAMSUNG-1003, ¶174. As described with respect to claim 1, *supra*, the DTC and dynamic PAN are transmitted together to the POS terminal, and then the payment processor, in place of card issuer information (e.g., the real PAN and validation code) to perform payment transactions. SAMSUNG-1004, [0032]-[0034], [0047], [0051]-[0052]; SAMSUNG-1003, ¶174. The

dynamic pan can be sent in place of the real PAN. *Id.*, [0057], [0032] (“This dynamic PAN can then be used in the transaction instead of the real PAN”).

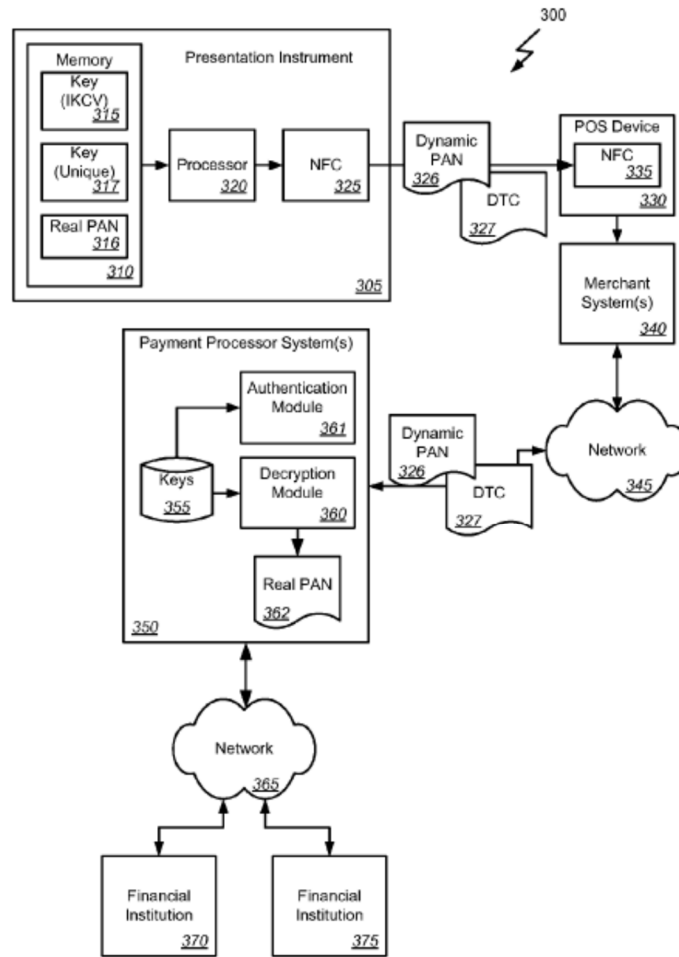


FIG. 3

SAMSUNG-1004, FIG. 3.

In the alternative where the IKCV is the device account number, the IKCV makes up part of the DTC and is therefore combined with the limited-use number (the dynamic PAN) (or vice versa) as part of the device generated payment information. SAMSUNG-1003, ¶175; SAMSUNG-1004, [0057], [0005]-[0009]. In the

alternative where the dynamic PAN is the device account number, it is combined/provided with the DTC (one example of a limited-use number in claim 1) as part of the device generated payment information. SAMSUNG-1003, ¶175; SAMSUNG-1004, [0032]-[0034], [0047], [0051]-[0052].

[6]

Royyuru discloses that “[t]he transaction can be authenticated at the payment processor system or at the financial institution **based on the DTC**. For example, **determining the real PAN** can comprise decrypting the dynamic **PAN using a key maintained by the payment processor system** and corresponding to one of the card-level keys of the device (e.g., the IKCV). SAMSUNG-1004, [0006], [0034], [0039], [0048]. Furthermore, “[a]uthenticating the transaction at the payment processor can **comprise validating the DTC using a key maintained at the DTC validation system** (e.g., the payment processor system or the financial institution), corresponding to the unique card level key on the payment device.” *Id.* “The real PAN can then be sent from the payment processor system to a financial institution to affect processing of the transaction.” *Id.*,

Therefore the keys are used to verify the limited-use number for use in processing the transaction. SAMSUNG-1003, ¶¶177-181. After the DTC is validated, “using the unique card level key,” the real PAN is sent to the financial institution

to process the transaction. SAMSUNG-1004, [0055], [0050]. The financial institution provides a response “to indicate approval and/or completion of the transaction.” *Id.*

A POSITA would have found obvious from the above disclosures that verification of the DTC and/or dynamic PAN by the payment processor are used in processing the transaction and therefore the limited-use number (DTC or dynamic PAN) is rejected if invalid number generation (e.g., invalid DTC or dynamic PAN) is detected. SAMSUNG-1003, ¶180. Furthermore, the DTC and dynamic PAN are valid for a single transaction, therefore they will be rejected by the payment processor if used after the single transaction (invalid use of an expired limited-duration number). SAMSUNG-1004, [0033], [0053], [0057]; SAMSUNG-1003, ¶180.

[7]

Royyuru describes priming through passing or tapping the user device on or near the POS terminal. SAMSUNG-1004, [0047]. A POSITA would have recognized that the device passing or tapping provides, or at least renders obvious, a device motion detection interface. SAMSUNG-1003, ¶¶182-185. Phillips further discloses that the device of the Royyuru-Phillips-Casey combination can be primed by entering a pin to initiate a financial transaction to increase security. SAMSUNG-1005, [0035], [0038]-[0039], [0066]. The resulting combination has “a touch screen capable of accepting user input” and therefore the user would enter the PIN

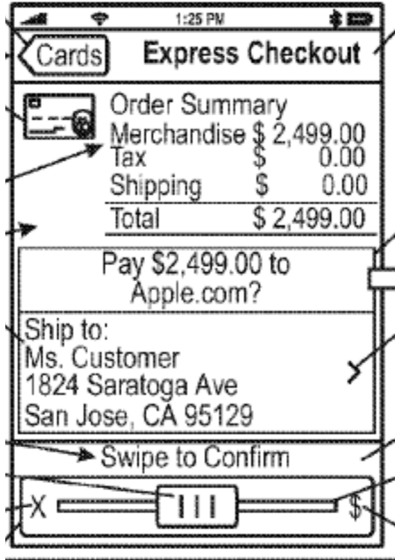
using the device touch-screen interface. SAMSUNG-1005, [0020]; SAMSUNG-1003, ¶¶183-184.

[8]

Royyuru teaches that the priming operation can be an electronic device tap. SAMSUNG-1004, [0047], [0044]. The priming operation can also be entering a PIN on a touchscreen (a touch-input sequence) or selecting a payment method as taught by Phillips. SAMSUNG-1005, [0036]-[0041], [0020]; SAMSUNG-1003, ¶¶186-188; *see also* SAMSUNG-1006, 9:4-28, 9:58-10:2, 12:46-65. Phillips and Casey disclose that in the resulting combination the electronic device is enabled for payment through user entry of a valid PIN or correct user swiping. SAMSUNG-1005, [0059], [0062], [0066], [0070]; SAMSUNG-1006, 9:9-36, 12:64-13:51, FIGs. 5-8.

[9.a]

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



SAMSUNG-1006, FIG. 5, *see also* FIGs. 6-8, 9:9-36, 13:24-51 (“...prompt the user to move a graphical element 180 to confirm the payment transaction”); SAMSUNG-1003, ¶¶189-191.

[9.b]

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

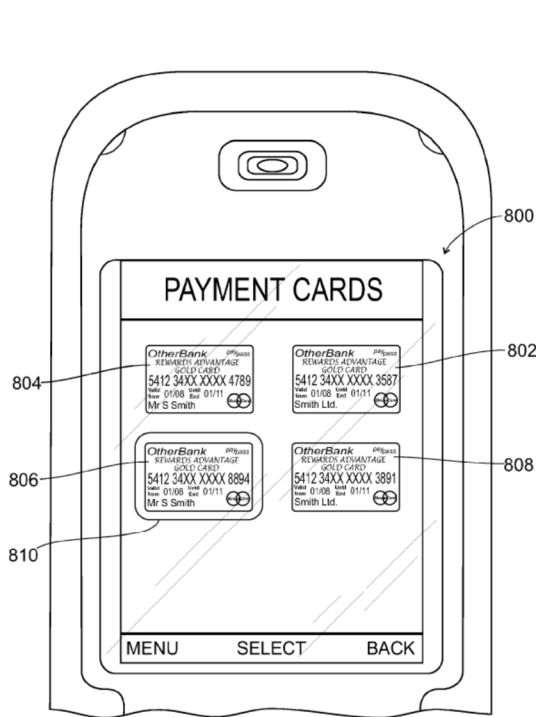


FIG. 8

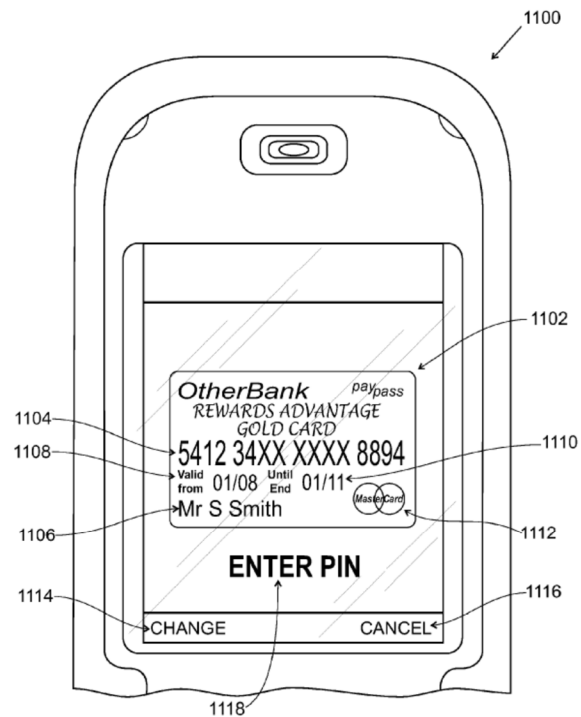


FIG. 11

SAMSUNG-1005, FIGs. 8, 11; [0036]-[0041]; *see also* SAMSUNG-1006, 8:52-9:28, 9:58-10:2, 12:46-65, 13:24-51, FIGs. 5-8; SAMSUNG-1003, ¶¶192-193.

[9.c]

Phillips discloses receiving payment method selection user input. SAMSUNG-1005, [0036]-[0041]. The user can provide approval of an automatically selected card by entering a PIN. *Id.*, [0059], [0066]. The user can also cancel (deny) the transaction or adjust the transaction payment (change payment type). *Id.*, [0068].

Casey similarly discloses approving and denying the transaction such as entering “a PIN to verify the payment instrument” or swiping in different directions

to confirm or deny the transaction. SAMSUNG-1006, FIGs. 5-8, 9:9-36, 13:24-51, 14:12-49; SAMSUNG-1003, ¶¶194-197.

[11]

Both Phillips and Casey disclose that in the Royyuru-Phillips-Casey combination, the transaction is completed upon receiving an authorization input on the electronic device from a valid user in response to presenting the user with at least one of selection of continuing with the default payment, selecting an alternate payment account, inputting an approval authorization, and adjustment of the transaction payment. SAMSUNG-1003, ¶¶198-203. Phillips discloses that after an exceptional condition, such as “transaction interval exceeding a pre-set time duration,” a security check (“card is locked”), or “a transaction in an amount above a certain limit,” the user can approve an “automatically selected card” by entering a PIN or select “a different choice of card account.” SAMSUNG-1005, [0043], [0059], [0066], [0061], [0068]; SAMSUNG-1003, ¶¶200-201. Casey similarly discloses that after a timeout period returning to a payment selection screen prior to approving and denying the transaction such as entering “a PIN to verify the payment instrument” or swiping in different directions to confirm or deny the transaction. SAMSUNG-1006, FIGs. 5-8, 9:9-36, 9:66-10:2, 13:24-51, 14:12-49; SAMSUNG-

1003, ¶202. The approval screen that includes the swipe control for approving/denying the transaction includes the transaction request information. *Id.*, see also, FIGs. 5-8.

[12]

As discussed with respect to Element [1.f], *supra*, the combination's "Payment Cards' sub-menu" allows "selection of the payment card account that corresponds to the payment card represented by the card-face image." SAMSUNG-1005, [0036]-[0041], FIG. 8; 9:58-10:2, 12:46-65; SAMSUNG-1003, ¶¶204-207. The displayed cards include expiration dates, card issuer icons, bank logos, card images, etc. SAMSUNG-1005, [0036]-[0041], FIG. 8. "[T]he user may be required to enter a PIN or code before selecting a payment card" and therefore the card selection menu is presented subsequent to the priming operation. SAMSUNG-1005, [0039]; SAMSUNG-1003, ¶205.

Phillips also discloses that the device will proceed with a default payment option ("automatically selected card") if the user does not select an alternative payment method. SAMSUNG-1005, [0005], [0059], [0066], [0017], [0029]; SAMSUNG-1003, ¶206. The default card is identified based on previously entered user criteria. *Id.*

[15.pre]

Supra, Preamble [1.pre].

[15.a]

Supra, Elements [1.d]-[1.e].

[15.b]

Supra, Elements [1.c], [1.f], [9.b].

[15.c]

Supra, Elements [1.f], [9a], [9c], [11]-[12].

[15.d]

Supra, Element [1.e].

[15.e]

Supra, Element [1.j].

[15.f]

Supra, Element [9.a]

[15.g]

Supra, Elements [1.g]-[1.h], [9.b]

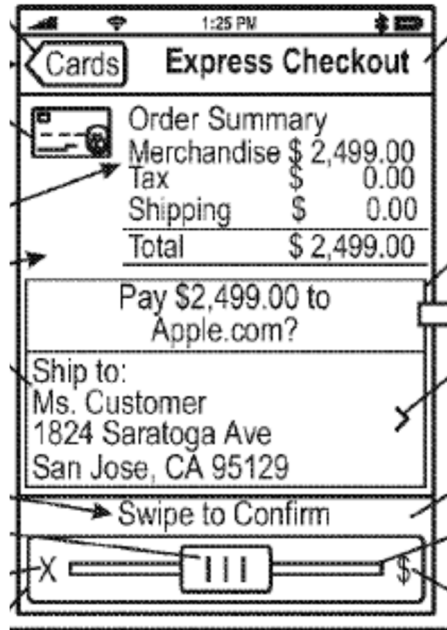
[15.h]

Supra, Elements [9.a], [9.c], [11].

[16]

The device of the Royyuru-Phillips-Casey combination has a touchscreen display. *Supra*, [1.c]; SAMSUNG-1004, [0021]; SAMSUNG-1011, [0006]; SAMSUNG-1005, [0018]; SAMSUNG-1006, 3:10-19. As described by Casey, the re-

sulting device presents a confirmation screen displaying “details about the sales order, such as the item price” and “a prompt asking a user to confirm the payment transaction.” SAMSUNG-1006, 13:24-51. The device “prompt[s] the user to move a graphical element 180 to confirm the payment transaction.” *Id.*



SAMSUNG-1006, FIG. 5; *see also* FIGs. 6-8; SAMSUNG-1003, ¶¶226-228.

[17]

Supra, Elements [1.f]-[1.h], [9.b]-[9.c], [11]-[12].

[18]

Supra, Elements [1.a], [8].

[19.pre]-[19.b]

The predictable combination provides “a mobile device” such as “a cellular telephone” having “a processor... and a memory communicatively coupled with

and readable by the processor.” SAMSUNG-1004, [0021], [0007], [0046], [0051]; SAMSUNG-1003, ¶¶237-240; *supra* [1.a]-[1.b].

[19.c]

Supra, Element [1.c].

[19.d]

The device of the Royyuru-Phillips-Casey combination includes “one or more input devices **210** (e.g., a scan device, a mouse, a keyboard, etc.)” including a touchscreen. SAMSUNG-1004, [0040], [0021]; SAMSUNG-1011, [0006]; SAMSUNG-1005, [0018]; SAMSUNG-1003, ¶¶242-243, *supra* [1.c].

[19.e]

Supra, Elements [1.e]-[1.f].

[19.f]

“The memory can also have stored therein a series of instructions which, when executed by the processor, cause the processor to” perform the described actions. SAMSUNG-1004, [0007], [0051]; SAMSUNG-1003, ¶245.

[19.g]

Supra, Elements [1.a], [7]-[8].

[19.h]

As Royyuru describes, in the resulting combination “a consumer can use the presentation instrument 305 to *initiate a transaction* at the POS device 330, for example by *scanning or tapping the presentation instrument 305 on or near the*

POS device 330 at the time of payment for a purchase.” SAMSUNG-1004, [0044]; *supra*, Elements [1.a], [8]. In another example, “[p]assing or tapping the presentation instrument near the POS device 330 can trigger” the device to generate the dynamic PAN and DTC and provide them “to the merchant system 340, e.g., via the NFC module 325 of the presentation instrument and corresponding NFC module 335 of the POS device 330” to facilitate the transaction. *Id.*, [0047]; SAMSUNG-1003, ¶¶247-248.

Phillips and Casey disclose that in some arrangements of the resulting combination the electronic device is enabled for payment by priming actions such as user entry of a valid PIN or correct user swiping. SAMSUNG-1005, [0035], [0059] (“a payment transaction...is not enabled unless the PIN had been recently entered into the phone”), [0062], [0066], [0070]; SAMSUNG-1006, 9:9-36, 12:64-13:51, FIGs. 5-8.

[19.i]

Supra, Elements [1.f]-[1.h].

[19.j]

Supra, Elements [1.f], [8], [9a], [9c], [11]-[12].

[19.k]

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

Supra, [1.i]; SAMSUNG-1003, ¶¶251-254. Royyuru further discloses that the generation of the dynamic PAN and DTC occurs in response to initiation of NFC communication with the POS device by the user “[p]assing or tapping the presentation instrument near the POS device.” SAMSUNG-1004, [0047], [0009] (describing generating the DTC and dynamic PAN responsive “to detect[ing] initiation of the transaction.”).

Phillips discloses that in the predictable Royyuru-Phillips-Casey combination, the verification cryptograms (DTC and dynamic PAN) are generated in response to receiving an NFC transaction payment request. SAMSUNG-1003, ¶252. Similar to Royyuru, Phillips discloses that the device interacts with the POS terminal via NFC. SAMSUNG-1005, [0023]. Phillips discloses that in the resulting combination the transaction is initiated when “the mobile device...receives 1302 a payment request.” SAMSUNG-1005, [0072]. The request can come in the form of “interrogation signals” received from a POS terminal via NFC. *Id.*, [0023], [0027], [0057]; *see also* SAMSUNG-1006 8:52-9:8 (“receiving information through...the NFC device...may include a request for payment”); FIGs. 5-8. “The interrogation signal stimulates the mobile telephone 100 to exchange wireless RF communications with the merchant proximity reader,” thus initiating the transaction. SAMSUNG-1005, [0057]; SAMSUNG-1003, ¶252.

Phillips discloses that, after receiving these interrogation signals and receiving a merchant identifier, the user device automatically selects a user payment card or allows the user to select a different payment method. SAMSUNG-1005, [0057]-[0058]. Phillips further discloses that the mobile device “cryptographically generate[s] a dynamic security code (CVC3) for the transaction and transmit[s] the dynamic security code to the reader.” *Id.*, [0059]. Because the transaction is initiated in response to a request from the POS device, a POSITA would have recognized that this cryptographic dynamic security code is generated in response to receiving the NFC transaction payment request. SAMSUNG-1003, ¶253.

Therefore, because Royyuru discloses that the DTC and dynamic PAN are dynamically generated responsive to the device “detect[ing] initiation of the transaction” (SAMSUNG-1004, [0047], [0009]), a POSITA would have recognized that in the resulting combination of Royyuru with Phillips and Casey, based on Phillips disclosure that the transaction is initiated responsive to receiving the payment request at the device (SAMSUNG-1005, [0072], [0023], [0027], [0057]-[0059]), the device generates the DTC and dynamic PAN responsive to receiving the NFC transaction payment request. SAMSUNG-1003, ¶254.

[19.]

Supra, Element [1.j]

[19.m]

Supra, Element [1.k]

[20]

Supra, Elements [1.a], [1.c], [7]-[8], [11]. A POSITA would have recognized that a touchscreen provides or at least renders obvious a touch sensor array and a touch key-pad and that a valid PIN entry, as described above with respect to Elements [1.a] and [9.c] and claims [7]-[8] and [11]-[12] provides a correct passcode entry sequence and a correct user response input from a security challenge (“an ‘Enter PIN’ prompt”) to verify that the user is a valid user. SAMSUNG-1003, ¶¶258-260; SAMSUNG-1005, [0035], [0038], [0058]-[0059] (describing PIN entry using a “numeric keypad” of the touchscreen).

[21]

Royyuru discloses that the “memory [is] communicatively coupled with and readable by the processor.” SAMSUNG-1004, [0007]. As discussed with respect to claims [3]-[4], *supra*, Royyuru discloses a static device-specific device account number of limited-use in the form of the IKCV stored on the device. SAMSUNG-1003, ¶¶261-266. The IKCV is “generated when *each card (device) is being customized*” and is generated by the payment processor *or issuer* based on the PAN and “institution key of the issuer of the account.” SAMSUNG-1004, [0057], [0046], [0032]-[0033], [0054]-[0055]. The IKCV is a device account number be-

cause it is specific to the device and based on payment account information. SAMSUNG-1003, ¶262. Because it can be generated by the issuer and provided to the device, it is static and originates from a card issuing authority. *Id.* The IKCV is of limited-use because it can only be used for transactions by the specific mobile device SAMSUNG-1003, ¶262; SAMSUNG-1004, [0057].

The IKCV has a limited time-duration based on the expiration date of the payment account or alternatively it would have been obvious to a POSITA to make the IKCV of a limited time-duration based on the expiration date of the payment account. *See, supra*, Claim [4]; SAMSUNG-1004, [0091]-[0096]; SAMSUNG-1003, ¶263.

The DTC is generated using one of the card-level keys (such as the IKCV) and the dynamic PAN is generated using the IKCV. SAMSUNG-1004, [0057], [0005]-[0009]. Both the DTC and the dynamic PAN are limited-use payment information. *Supra*, Element [1.i]. Furthermore, Royyuru discloses “generat[ing] a dynamic PAN 326 based on the real PAN 316, the **card-level key 315**, and one or more factors from the payment device or the POS reader such as **unpredictable numbers** or counters.” SAMSUNG-1004, [0051]. The undeterminable number can be any “*received by the presentation instrument 305*” which includes the expiration date, which, as described above, is the expiration date for both the real PAN and the IKCV generated using the expiration date. SAMSUNG-1004, [0051],

[0057], [0091]-[0096]; SAMSUNG-1003, ¶264. Therefore, the dynamic PAN is limited-use payment information generated in part based on combining the IKCV (static device-specific device account number) and the device account expiration date. *Id.*

Similarly, the DTC is generated using values including “expiration date” and a card-level key (which can be the IKCV). SAMSUNG-1004, [0057], [0005]-[0006]; SAMSUNG-1003, ¶265. Therefore, the DTC is another example of limited-use payment information generated in part based on combining the IKCV (static device-specific device account number) and the device account expiration date. SAMSUNG-1003, ¶265. Phillips discloses that the cryptogram is generated after selection of the payment method. SAMSUNG-1005, [0059], [0066]. Indeed, the DTC and dynamic PAN are generated based on information specific to the selected account. SAMSUNG-1004, [0051], [0057], [0005]-[0006].

[22]

As discussed with respect to claims [21] and [3]-[4], *supra*, the IKCV is a limited-use device account number stored in the memory accessible to the processor that is valid for a limited duration (expiration date) or alternatively it would have been obvious to a POSITA to make the IKCV of a limited time-duration of valid use. SAMSUNG-1004, [0007], [0057], [0046], [0032]-[0033], [0054]-[0057], [0091]-[0096]; SAMSUNG-1003, ¶¶267-271.

The IKCV is a key and Royyuru discloses that the device stores numerous other “unique card level key[s] *stored on the device*.” SAMSUNG-1004, [0005]-[0007], [0032] (describing “a unique encryption key per card or other device” and “a unique, card-level key” each stored on the device), [0051], [0057], FIG. 3.

The DTC is generated using one of the card-level keys (such as the IKCV) and the dynamic PAN is generated using the IKCV. SAMSUNG-1004, [0057], [0005]-[0009]. Both the DTC and the dynamic PAN are one-time limited-use cryptogram numbers. *Supra*, Claim [3], The IKCV makes up part of the dynamic PAN and is therefore combined with the limited-use cryptogram number (the DTC) (as part of the device generated payment information. SAMSUNG-1003, ¶270; SAMSUNG-1004, [0057], [0005]-[0009]. Alternatively, the IKCV makes up part of the DTC and is therefore combined with the limited-use cryptographic number (the dynamic PAN) as part of the device generated payment information. SAMSUNG-1003, ¶270; SAMSUNG-1004, [0057], [0005]-[0009].

[23]

Supra, Elements [1.j], [2]-[3].

B. [GROUND 1B] – Obviousness based on Royyuru-Phillips-Casey-Gomez (Claim 5)

1. Royyuru-Phillips-Casey-Gomez Combination

Gomez describes a mobile payment system to address “[t]he problems of fraud and identity theft” with credit card transactions. SAMSUNG-1007, 1:32-48.

Similar to Royyuru, Gomez describes a mobile payment device that generates an “authentication cryptogram” based on information unique to the device and other information related to the transaction. *Id.*, 7:17-48. Gomez further discloses displaying the authentication cryptogram on the payment device to beneficially “facilitat[e] an online transaction.” SAMSUNG-1007, 12:64-13:4, 13:22-33, 21:5-20.

A POSITA would have been prompted to apply the teachings of Gomez to the Royyuru-Phillips-Casey combination to provide a mobile payment system in which the cryptograms generated by the resulting device (e.g., the DTC and dynamic PAN of Royyuru) are displayed on the device to “beneficial[ly] facilitate[e] an online transaction.” SAMSUNG-1007, 12:64-13:4, 13:22-33, 21:5-20; SAMSUNG-1003, ¶¶276-277. Displaying the cryptograms on the device would allow the user to manually enter the DTC and/or dynamic PAN into a website of an online merchant to increase the utility of the resulting device and provide for more secure online transactions (in addition to more secure in-person transactions). SAMSUNG-1003, ¶277. Furthermore a POSITA would have recognized that application of Gomez’s teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. *Id.*

2. Application of Royyuru-Phillips-Casey-Gomez

Claim [5]

Royyuru's DTC is a "***Dynamic Transaction Cryptogram***" generated at the device using "the **PAN, service code, expiration date, unpredictable number, and ATC** and encrypting them using the **CK**." SAMSUNG-1004, [0005], [0057]. The DTC is limited in use to the specific user device "for a single transaction." *Id.*, [0057] (CK is "unique per card"), [0032]-[0033], [0005]. The ATC is a device transaction sequence counter. *Id.*, [0057]. The IKCV is a card-level key used to generate the DTC and is a device account number. *Supra*, Claim [4]; SAMSUNG-1004, [0005]-[0006]; SAMSUNG-1003, ¶¶278-282. The PAN is a payment card account number. SAMSUNG-1004, [0007]-[0008]. The unpredictable number provides "a time of day." *Id.*, [0047].

The "[p]ayment processor network can validate the DTC and decline the transaction if the DTC is incorrect" and is therefore utilized in the resulting Royyuru-Phillips-Casey system in place of a card issuer card security code. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶280. Specifically, Royyuru describes that the DTC is part of the "Track 1" "verification information" that is conveyed from the merchant system to the payment processor to validate the payment information. SAMSUNG-1004, [0049]. As would have been recognized by a POSITA, this Track 1 data differs from standard Track 1 data in that it does not include a

CVC, CVC3, CVV, or similar card validation value. SAMSUNG-1003, ¶280; *see, e.g.* SAMSUNG-1005, [0059]. Therefore, a POSITA would have recognized that the DTC is provided in place of a card issuer card security code to validate the payment information. SAMSUNG-1003, ¶280.

Gomez would have been beneficially applied to the Royyuru-Phillips-Casey combination to display the limited-use security number on the user-interface. SAMSUNG-1003, ¶¶277, 281. Gomez describes “a great variety of useful information may be displayed” on the display of the payment device, for example “the generated authentication cryptogram may be displayed, which may be beneficial in facilitating an online transaction.” SAMSUNG-1007, 12:64-13:4, 13:22-33, 21:5-20.

C. [GROUND 1C] – Obviousness based on Royyuru-Phillips-Casey-Deibert (Claims 10, 14)

1. Royyuru-Phillips-Casey-Deibert Combination

Deibert describes a mobile payment system with a disabling feature. SAMSUNG-1012, Abstract. The user can set “a predetermined timeout time such that the mobile payment application is disabled after the predetermined timeout time has elapsed” to “help prevent the accidental transmittal of [payment] information.” *Id.*, [0009], [0023]. Deibert discusses manual activation of a mobile payment application and multiple techniques for disabling the mobile application to prevent

unintentional transmittal of payment information, including completion of a transaction, manual disabling based on user input, and expiration of a predetermined timeout time. *Id.*, [0023]-[0025], [0058]-[0059].

A POSITA would have been prompted to apply the teachings of Deibert to the Royyuru-Phillips-Casey combination to include multiple mechanisms by which a payment priming operation is disabled (including through completion of a transaction, manual user input, and expiration of a timeout period) to “help prevent the accidental transmittal of information,” provide increased functionality of allowing the user to intentionally return the device to an idle state, and to “allow[] the phone to have full contactless card functionality, while removing limitations.” SAMSUNG-1012, [0023]-[0025], [0061]. SAMSUNG-1003, ¶¶284-285. This modification also “minimize[s]” user concern and hesitancy regarding mobile payment transactions, thus increasing user satisfaction. SAMSUNG-1012, [0061]; SAMSUNG-1003, ¶285. Such a modification would also save power by decreasing the amount of time that the NFC circuit is actively transmitting payment information and increase ease of use by providing mechanisms for disabling payment priming that don’t require user interaction. SAMSUNG-1003, ¶285. Furthermore, a POSITA would have recognized that application of Deibert’s teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have

had a reasonable expectation of success in making such a modification. SAMSUNG-1003, ¶¶284-285.

2. Application of Royyuru-Phillips-Casey-Deibert

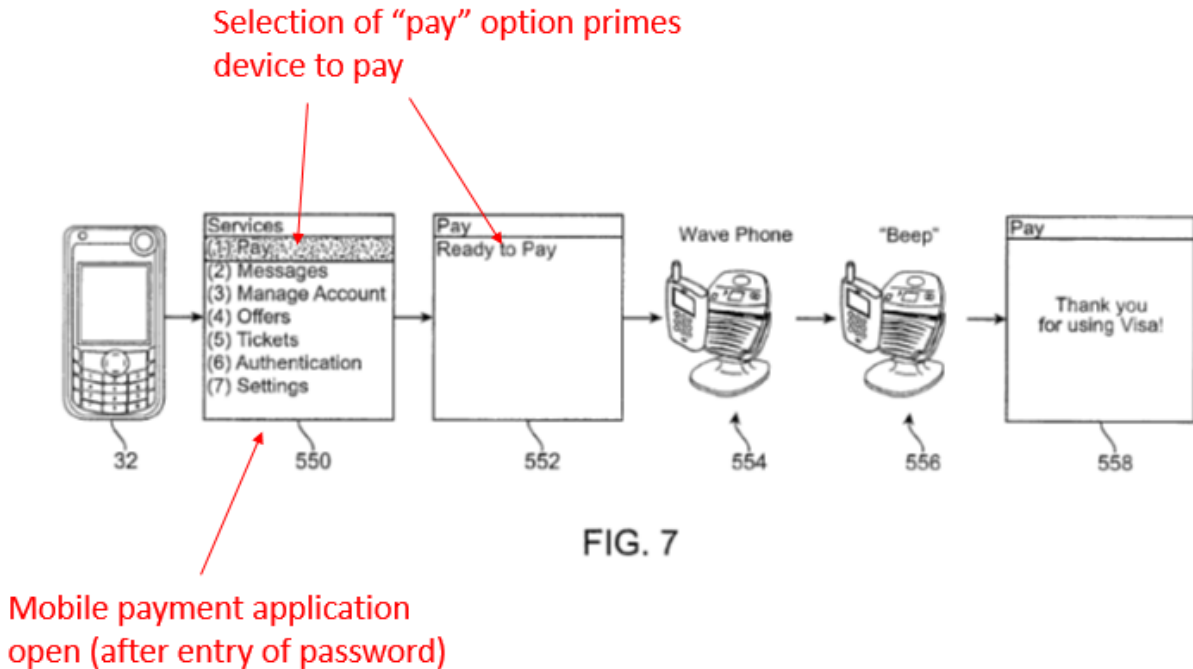
[10]

Like Royyuru, Deibert similarly discloses using NFC to facilitate communications between the user device and merchant terminal during mobile payment transactions. SAMSUNG-1012, [0019], [0040]; SAMSUNG-1004, [0022], [0044], [0047]. Deibert describes manually activating a mobile phone application (e.g., priming) and in response “the mobile phone will transmit payment information.” SAMSUNG-1012, [0023]. This communication is limited to “a predetermined timeout time” such that “[i]f no payment transaction occurs within the predetermined timeout time, then after the predetermined timeout time, the mobile payment application on the phone will automatically disable so that contactless payments cannot be made.” *Id.*, [0025]-[0026], [0058]. The manual activation can include “entering a password.” *Id.*, [0057]. A POSITA would have understood that terminating the mobile payment application provides, or at least renders obvious, terminating the NFC communication and aborting the transaction. SAMSUNG-1003, ¶¶286-288.

[14]

Both Phillips and Casey disclose requiring a PIN (a passcode) to access the payment application/functionality prior to selecting a specific payment method.

SAMSUNG-1005, [0035], [0038]-[0039], [0066]; SAMSUNG-1006, 9:9-36. A POSITA would have recognized that user selection of a payment method provides a priming operation after entry of the PIN/passcode. SAMSUNG-1003, ¶¶289-292. Deibert similarly describes requiring “entering a password into the mobile phone application, in order to authenticate the consumer 30 and prevent fraud.” SAMSUNG-1012, [0057], [0049] (“user is prompted to enter a password”). Deibert describes further priming operations after entry of the password, including manual activation of the payment application after expiration of a timeout period without requiring additional password entry “because the consumer has already been authenticated by entering the password the first time.” SAMSUNG-1012, [0058], [0023] (describing that the user “*manually* select[s] the mobile phone application *each time* before making a purchase). In another example, Deibert describes that after the payment application is opened (which can require entry of a password), the device requires a further priming operation of selecting the “pay functionality of the mobile payment application” to prime the device “to engage in a payment transaction.” SAMSUNG-1012, [0060], [0057].



SASMUNG-1012, FIG. 7, [0057], [0060].

Furthermore, a POSITA would have recognized that payment priming is a type of device priming. SAMSUNG-1003, ¶291. Deibert discloses disabling a device priming on further button pressing, stating “the consumer can manually disable the mobile phone application, thereby returning the mobile phone to the idle state.” SAMSUNG-1012, [0024]. Deibert further teaches that “[i]f no payment transaction occurs within the predetermined timeout time, then *after the predetermined timeout time, the mobile payment application on the phone will automatically disable* so that contactless payments cannot be made.” *Id.*, [0025]-[0026], [0058]. Additionally, [o]nce a transaction has occurred, the mobile phone can go back to the idle state.” *Id.*, [0024], [0059]-[0060].

D. [GROUND 1D] – Obviousness based on Royyuru-Phillips-Casey-Deibert-Power (Claim 13)

[13]

Phillips discloses priming (preparing the device to transmit payment information) through selection of a “card accounts” option from menu 700 followed by selection of a displayed payment option. SAMSUNG-1005, [0036]-[0037], FIGs. 7-8. These menu button selections would have been conducted via the “select button” disclosed by Phillips in at least some embodiments. SAMSUNG-1005, [0033]; SAMSUNG-1003, ¶296. This sequence of menu selections using a button falls within the disclosure of a button double press in the ’579 patent. SAMSUNG-1001, 9:64-10:3, 17:19-23.

Furthermore, a POSITA would have applied the teachings of Power to Royyuru-Phillips-Casey-Deibert to require biometric sensing of the device continuously remaining in contact of the valid user and disabling the priming operation when the device is not continuously in contact with the user. SAMSUNG-1003, ¶¶293-294, 297. Powers teaches that the device “detects a presence or an absence of a gating signal.” SAMSUNG-1016, 2:1-3. In some embodiments, presence of the gating signal (to allow use of a smart payment device) requires continued contact with “the customer’s body.” *Id.*, 4:37-43. The device includes a transducer to “monitor[] the one or more physical phenomena” and enables/disables the wire-

less-communication circuit in response to detection or absence of the physical phenomena. *Id.*, 2:52-60, 3:51-67. The transducer(s) can detect a temperature, resistance, capacitance, or pressure change “when the user is holding the payment card” such that the device “is only active (and able to communicate the financial information) when it is being used by customer.” *Id.*, 1:55-62, 3:65-4:19.

A POSITA would have applied these teachings of Power to Royyuru-Phillips-Casey-Deibert to “protect” transaction information from being inadvertently transmitted when the user does not intend to conduct a financial transaction, thereby preventing unintended or fraudulent charges to the user’s payment cards and “increase[ing] security.” SAMSUNG-1016, 2:47-3:5; SAMSUNG-1003, ¶294. Furthermore, such protections are not overly burdensome and provide “ease of use” because the user only needs to make physical contact with the card to maintain the priming state. *Id.*

Both Phillips and Casey require PIN (passcode) entry to re-validate a user, which a POSITA would have recognized as adding an extra layer of security when combined with Power’s physical contact detection requirement. SAMSUNG-1005, [0035], [0038]-[0039], [0066]; SAMSUNG-1006, 9:9-36; SAMSUNG-1003, ¶298.

Deibert discloses that the Royyuru-Phillips-Casey-Deibert-Power combination provides the last three elements of claim 13 for the reasons discussed in Ground 1C, *supra*. SAMSUNG-1003, ¶299.

E. [GROUND 1E] – Obviousness based on Royyuru-Phillips-Casey-Carlson (Claims 4, 21, 22)

1. Royyuru-Phillips-Casey-Carlson Combination

Similar to Royyuru, Carlson describes a mobile device for “conducting transactions using pseudo primary account identifiers.” SAMSUNG-1013, [0012], [0029]. The pseudo account identifier can be “similar in format to a consumer’s real account identifier” without revealing the true sequence of numbers or characters in the real account identifier. *Id.*, [0030]. The pseudo account identifier is generated by the payment processor and provided to the mobile device for use in place of the primary account identifier. *Id.*, [0035], [0017]-[0018]. “[T]he pseudo primary account number may be *set to expire* after a certain number of transactions or after a certain time period” to avoid “illicit use.” SAMSUNG-1013, [0036], [0044], [0086].

A POSITA would have been prompted to apply the teachings of Carlson to the Royyuru-Phillips-Casey combination such that the IKCV is “set to expire...after a certain time period” because “[d]oing so can help to ensure that if for some reason a pseudo primary account number is revealed to anyone other than an authorized user, the amount of damage that can be done is limited due to the limited lifetime of the pseudo primary account number.” SAMSUNG-1013, [0036]; SAMSUNG-1003, ¶¶302-304. Implementing the IKCV to “have a limited lifetime... provides a level of protection to the consumer’s account” because it would likely

“expire[] before any illicit use could be made.” SAMSUNG-1013, [0044]; SAMSUNG-1003, ¶303. Therefore, setting an expiration for the IKCV can prevent fraudulent use of the IKCV to generate DTCs and dynamic PANs by unauthorized devices. SAMSUNG-1003, ¶303. A POSITA would have found it beneficial to apply such an expiration date/time limitation to other account and device related information in the combination to achieve similar benefits. *Id.*

Furthermore a POSITA would have recognized that application of Carlson’s teachings to the Royyuru-Phillips-Casey system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. SAMSUNG-1003, ¶304.

2. Application of Royyuru-Phillips-Casey-Carlson

With respect to claims [4], [21], and [22], as discussed above, in the Royyuru-Phillips-Casey-Carlson system, the IKCV is “set to expire...after a certain time period” by the payment processor or issuer. SAMSUNG-1013, [0036], [0044], [0086]; SAMSUNG-1003, ¶¶303, 306. The IKCV therefore has an expiration date of limited duration of validity and is therefore of limited time-duration of valid use. SAMSUNG-1003, ¶306. Furthermore, the DTC and dynamic PAN can be generated using both the IKCV and any “unpredictable number” including any “number...*received by the presentation instrument*.” SAMSUNG-1004, [0051],

[0057], [0006]; SAMSUNG-1003, ¶306. Therefore the DTC and dynamic PAN are generated by combining the IKCV of limited duration (based on Carlson) and the expiration date for the IKCV, as disclosed by Royyuru (claim [21]). SAMSUNG-1003, ¶306; SAMSUNG-1004, [0006]-[0007], [0057].

All other elements of claims [4], [21], and [22] are disclosed by the Royyuru-Phillips-Casey-Carlson combination for the reasons discussed in Ground 1A, *supra*. SAMSUNG-1003, ¶¶307, 170-176, 261-271.

F. [GROUND 2A] – Obviousness based on Gomez-Amacker-Mullen-Smith (Claims 1-9, 11-12)

1. Gomez

Gomez describes a mobile payment system “utiliz[ing] a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card, and which expires within a short period of time thereafter.” SAMSUNG-1007, 1:58-63, 7:17-48. Because the authentication cryptogram is time-limited, “the information that can be gleaned from a payment card...is rendered useless for making an unauthorized subsequent transaction.” *Id.*, 5:7-11, FIG. 7.

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

The payment card transmits the static EPIC number and the dynamically-generated authentication cryptogram to the point-of-sale (POS) terminal, which is

then conveyed to an authentication server (e.g., EPIC) before the transaction request is sent to an issuer or bank for approval. *Id.*, 7:49-8:82.

2. Amacker

Amacker discloses a “mobile wallet server” stored on a user’s personal mobile device that allows a user to “control the distribution of personal/payment information...by selectively approving or rejecting requests.” SAMSUNG-1008, 2:13-57. “The person may respond to the request by interacting with the mobile wallet server...Upon a selection of ‘accept’ (or similar approval), the mobile wallet server may transmit the requested information (e.g., personal/payment information, etc.) to the retailer to complete a pending process.” *Id.*

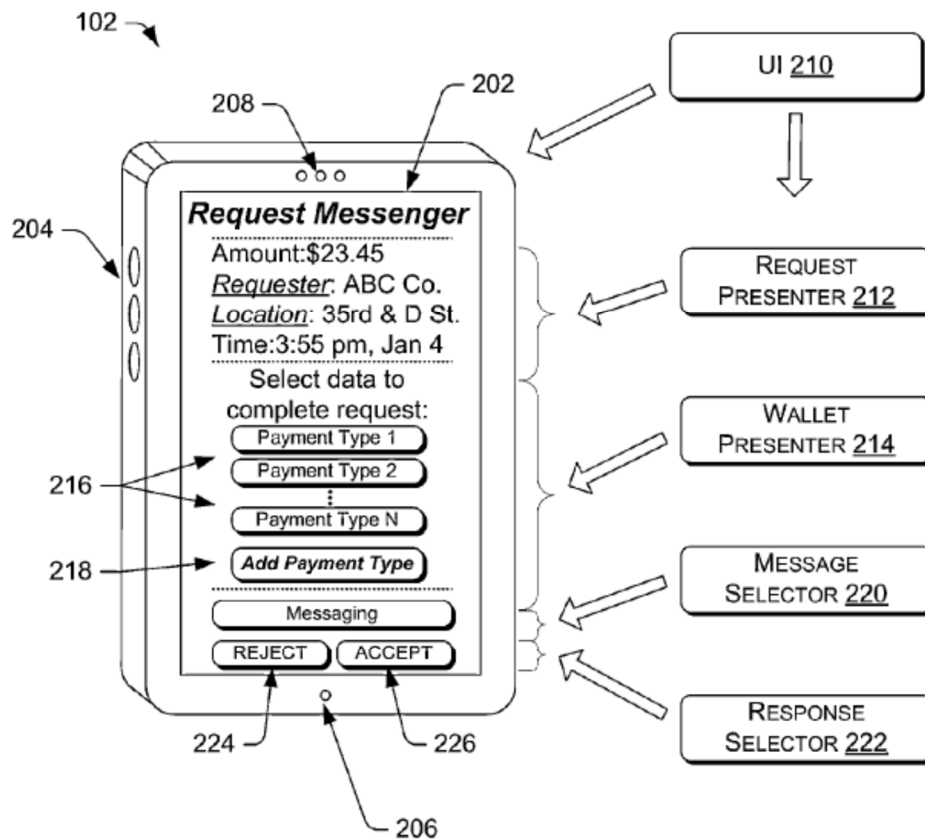
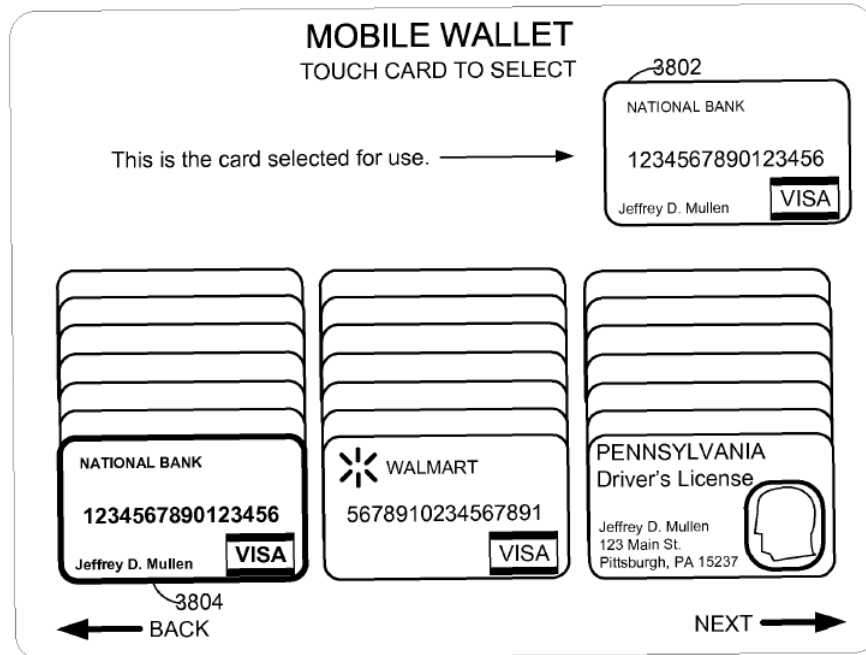


Fig. 2

3. Mullen

Mullen describes a mobile device that implements a mobile wallet containing a collection of virtual payment card(s). SAMSUNG-1009, [0326], [0328], [0353], FIG. 38. The device provides a user interface through which a user can select a particular virtual payment card for a transaction, like that shown in Figure 38 (reproduced below). *Id.*



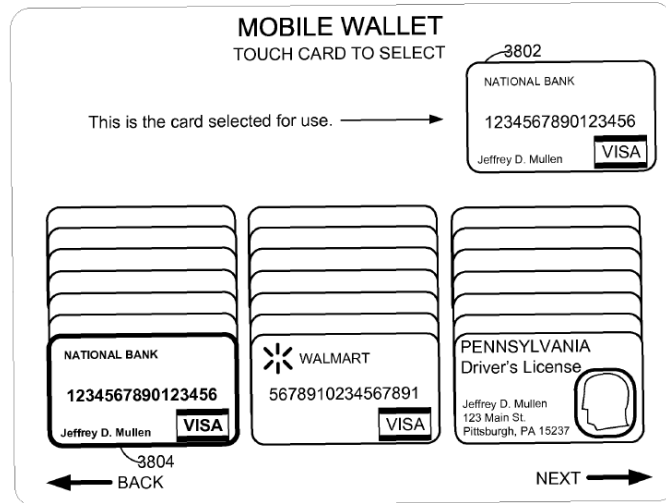
SAMSUNG-1009, FIG. 38. Upon completion of the transaction, a “payment receipt...[is] provided to mobile wallet” and can be displayed by the device. SAMSUNG-1009, [0287], [0339]-[0340], [0038], [0210].

4. Smith

Smith describes “processing a financial transaction using a mobile cloud account mapped to a payment account” using “a master key identifier, a mobile cloud account number (MCA), and a real card account number (RCA).” SAMSUNG-1010, Abstract. The service provider generates the MCA using the RCA and includes “at least the last four digits of the RCA” as the last four digits of the MCA. *Id.*, [0083]. The device displays “an image of a payment card with first twelve digits of the MCA obscured (e.g., replaced by asterisks) and the last four digits displayed.” *Id.*

5. Gomez-Amacker-Mullen-Smith Combination

A POSITA would have beneficially applied the teachings of Amacker, Mullen, and Smith to modify Gomez's mobile payment system to include multiple improvements. SAMSUNG-1003, ¶¶309-320. First, a POSITA would have modified Gomez such that the EPIC payment card of Gomez is modified to include a larger, touchscreen display and/or is integrated into a mobile device (such as a smartphone) having a touchscreen display, as taught by both Amacker and Mullen. SAMSUNG-1007, 5:48-57, 10:34-42; SAMSUNG-1008, 4:51-60, 2:13-25, 6:21-30; SAMSUNG-1009, [0041], [0151], [0326], [0458]; SAMSUNG-1003, ¶¶311-312, 60-63. A POSITA would have recognized that including a larger, touchscreen display would have allowed the resulting device to display additional information regarding payment cards, details of the transaction, and transaction status on the device while allowing for easier, intuitive user manipulation via the touchscreen, such as when selecting a payment card, thereby improving the user experience. SAMSUNG-1003, ¶¶311-312; SAMSUNG-1008, 5:1-17, FIG. 2; SAMSUNG-1007, [0326]-[0328], [0353], FIGs. 36-40.



SAMSUNG-1009, FIG. 38. Furthermore, a POSITA would have recognized that Gomez, Amacker, and Mullen 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 amount of devices that a user needs to carry while also improving the user experience due to the improved user interfaces and processing power of smartphone devices of the time. SAMSUNG-1007, 8:53-57, 7:49-54; SAMSUNG-1008, 3:27-34; SAMSUNG-1009, [0158]; SAMSUNG-1003, ¶¶310-312.

Second, a POSITA would have modified Gomez based on Amacker to receive and display a payment request at the resulting device. SAMSUNG-1008, 2:37-3:3, 3:42-57, 4:37-5:17; SAMSUNG-1003, ¶¶313-314. Gomez describes NFC communication with the merchant and Amacker beneficially discloses that such NFC communications can include a payment request. SAMSUNG-1007, 8:53-57, 7:49-54; SAMSUNG-1008, 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:

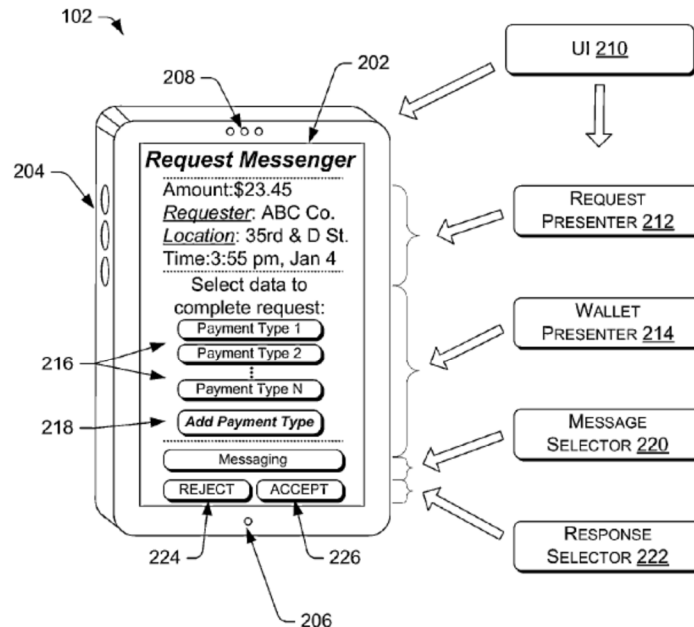


Fig. 2

SAMSUNG-1008, FIG. 2. This modification would have improved the resulting system by allowing the user to better ensure that they are approving a payment transaction and transmitting payment information to a correct merchant terminal, which can prevent fraudulent transmittal of payment information to an incorrect terminal. SAMSUNG-1003, ¶314. Such a modification would also allow the user to visually review transaction data before approving (or denying) the transaction. *Id.*; SAMSUNG-1008, 3:27-57, 2:37-3:3, 4:37-5:41, 6:2-15. Requiring the user to authorize the transaction (as taught by Amacker) would have allowed the user to review transaction information (e.g., price, purchase items) prior to completing the

transaction, allowed the user extra opportunity to change their mind regarding a transaction, and provide extra assurance that the user intends to initiate a payment transaction rather than having inadvertently opened a payment application. SAMSUNG-1003, ¶314.

Third, a POSITA would have modified Gomez based on Amacker and Mullen 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.” SAMSUNG-1007, 20:30-42, 21:5-20; SAMSUNG-1003, ¶¶315-316. Amacker and Mullen provide additional details on how a user can use a touchscreen display to view additional information about payment methods before selecting. SAMSUNG-1003, ¶¶315-316; SAMSUNG-1008, 5:18-41, Cl. 1, FIG. 2; SAMSUNG-1009, [0037], [0326], [0328], [0353], FIG. 38. 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. SAMSUNG-1003, ¶316.

Fourth, a POSITA would have modified Gomez based on Mullen and Smith to only display the last four digits of the payment card in the card selection menu. Mullen discloses that the payment numbers for the card may be “partially displayed.” SAMSUNG-1009, [0433]-[0434]; SAMSUNG-1003, ¶317. Additionally,

Smith discloses only displaying the last four digits of available payment options.

SAMSUNG-1010, [0083]. A POSITA would have recognized that only displaying the last four digits of the payment number for each card (a partial number) would have allowed the user to more readily recognize and identify a desired payment method from among the multiple payment methods stored on the resulting device while obscuring the entire payment number to prevent fraud due to nearby third-parties observing the displayed payment numbers, thereby increasing user utility while increasing security. SAMSUNG-1003, ¶317.

Fifth, a POSITA would have modified Gomez based on the teachings of Amacker to generate the authentication cryptogram in response to receiving the request to ensure that the limited-duration cryptogram is valid for the intended transaction. SAMSUNG-1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; SAMSUNG-1003, ¶318. Such a modification would have saved processing resources by only utilizing the processor to generate the authentication cryptogram when a valid payment request has been received. SAMSUNG-1003, ¶318.

Sixth, a POSITA would have modified Gomez based on Mullen to display information regarding the transaction status, such as transaction complete receipt information, on the user device. SAMSUNG-1009, [0287], [0339]-[0340], [0038], [0210]; SAMSUNG-1003, ¶319. Such a modification would have provided

additional assurance to the customer that the correct transaction occurred, or allowed for quick correction of an incorrect transaction, thus increasing user satisfaction and eventually increasing the customer base. SAMSUNG-1003, ¶319. Such a modification would have also allowed the user to more easily keep digital records of financial transactions. SAMSUNG-1003, ¶319.

Finally, a POSITA would have recognized that applying the teachings of Amacker, Mullen, and Smith 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. SAMSUNG-1003, ¶320.

[1.pre]

To the extent the preamble is treated as a limitation, Gomez describes “purchase transaction approval at a retail merchant.” SAMSUNG-1007, 3:65-67, 5:65-6:4, 2:45-54. SAMSUNG-1003, ¶¶321-323.

[1.a]

Gomez describes priming operations such as entry of “***a fingerprint or PIN number, into the payment card.***” SAMSUNG-1007, 2:59-64, 5:13-18, 7:9-16, 9:12-33, 13:40-44; SAMSUNG-1003, ¶324. Gomez discloses performing the described functions using an “EPIC payment card.” SAMSUNG-1007, 11:19-38, 2:55-3:3, FIG. 9. As discussed above, in the predictable combination, the payment

device can be implemented as a mobile device such as a smartphone. SAMSUNG-1008, 2:13-25; SAMSUNG-1009, [0041], [0458]; SAMSUNG-1003, ¶324.

[1.b]

The device of the Gomez-Amacker-Mullen-Smith combination “includes a processor.” SAMSUNG-1007, 10:34-38, 2:59-64; SAMSUNG-1003, ¶325.

[1.c]

Gomez discloses “a display” and “an activation input device.” SAMSUNG-1007, 12:49-61; 10:34-38. The display “may be a touch screen display.” SAMSUNG-1008, 4:51-60; SAMSUNG-1003, ¶326.

[1.d]

The Gomez-Amacker-Mullen-Smith device includes “NFC circuits for implementing a near-field communications transceiver.” SAMSUNG-1007, 8:53-57, 7:49-54, 2:40-3:3; SAMSUNG-1003, ¶327.

[1.e]

Amacker discloses that in the predictable combination the retailer can “transmit a request to the person's mobile device” including requests for “payment information” for completing “in person” transactions. SAMSUNG-1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; SAMSUNG-1003, ¶328. The communication occurs via the NFC interface. SAMSUNG-1007, 8:53-57, 7:49-54; SAMSUNG-1008, 3:27-34.

[1.f]

The Gomez-Amacker-Mullen-Smith 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.” SAMSUNG-1007, 20:30-59, 21:5-20, FIG. 9.

Amacker confirms that in the predictable combination “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.).” SAMSUNG-1008, 5:18-41, Cl. 1; SAMSUNG-1003, ¶¶329-332.

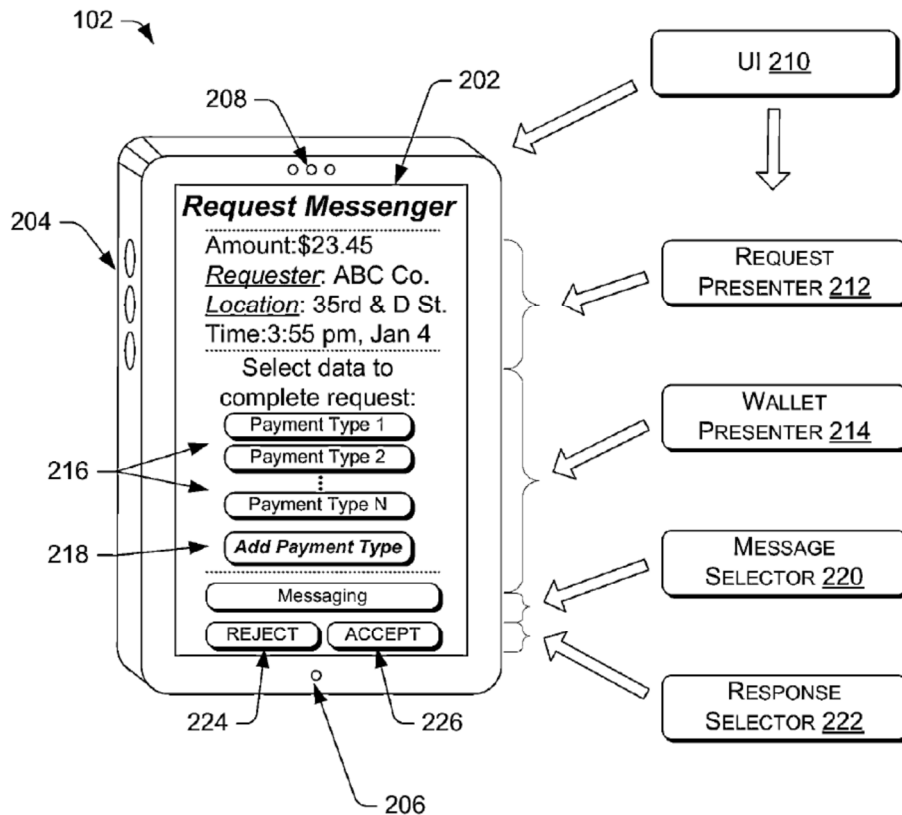
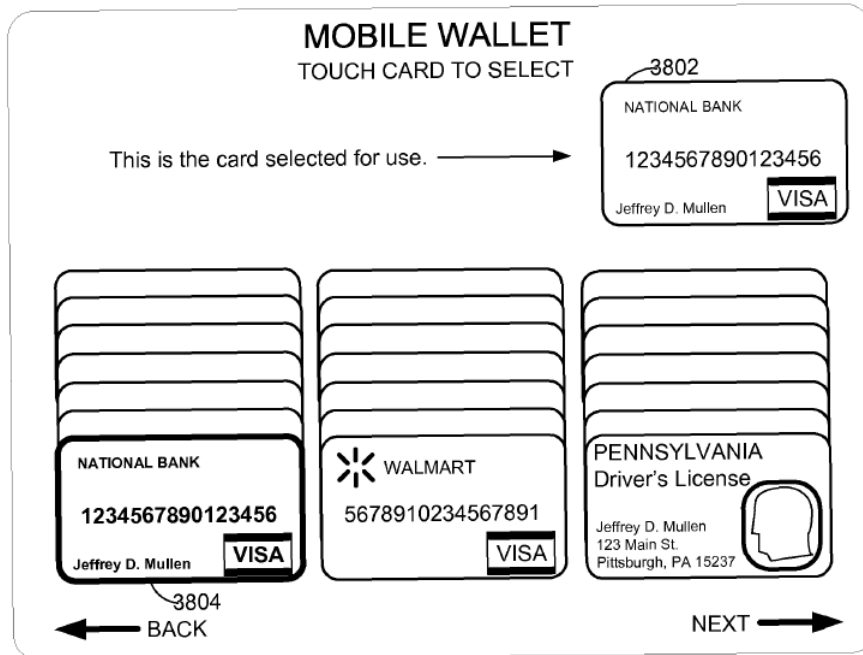


Fig. 2

SAMSUNG-1008, FIG. 2.

Mullen describes “a virtual manual interface” that allows a user to “select (e.g., touch) in order to select a method of payment” displaying “account number and merchant affiliation” for the cards. SAMSUNG-1007, [0353], [0326]-[0328], [0037], FIGs. 36-40.

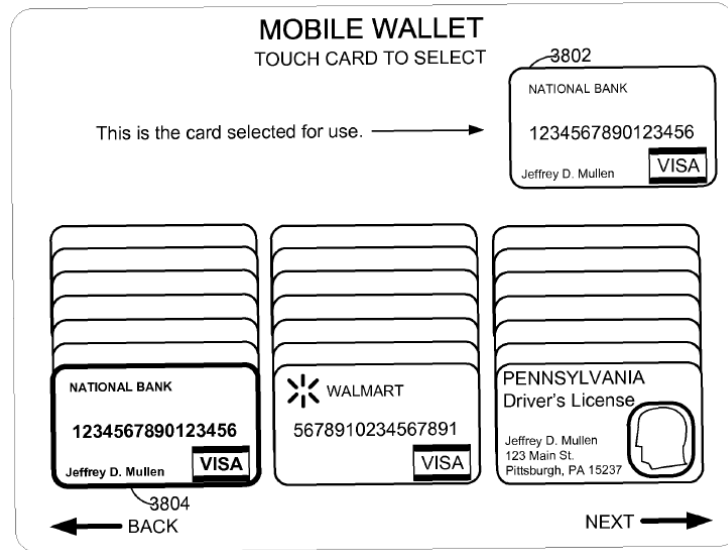


SAMSUNG-1009, FIG. 38.

Payment numbers for the cards “may be entirely, *or partially*, displayed.” SAMSUNG-1009, [0433]-[0434]. Smith discloses displaying only “the last four digits” of available cards to help the user in selecting the desired card while obscuring payment card numbers that could be viewed by nefarious onlookers. SAMSUNG-1010, [0083]; SAMSUNG-1003, ¶332.

[1.g]

Gomez discloses displaying a “*card logo*” for each card. SAMSUNG-1007, 20:43-59; *see also* SAMSUNG-1008, 5:18-41. As Mullen discloses, the device of the predictable combination displays “graphical information, such as logos and barcodes” as part of the card selection menu. SAMSUNG-1009, [0434]; SAMSUNG-1003, ¶¶333-334.



SAMSUNG-1009, FIG. 38.

[1.h]

As disclosed by Gomez and Mullen, the device of the predictable combination displays additional iconography of the payment card such as “name (or nickname)” and “graphical information, such as logos and barcodes.” SAMSUNG-1007, 20:43-59; SAMSUNG-1009, [0434]; FIGs. 36-40; SAMSUNG-1003, ¶¶335-336.

[1.i]

Gomez describes “a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card” based on a seed value and temporal value “which expires within a short period of time thereafter.” SAMSUNG-1007, 1:58-2:4. The device generates an “authentication cryptogram for

each attempted transaction only after the cardholder successfully presents a credential.” *Id.*, 5:13-18; *see also* 7:26-8:9; SAMSUNG-1003, ¶¶337-338.

As would have been recognized by a POSITA, the authentication cryptogram (the limited-use payment information) is used in place of the card issuer supplied payment information (the “actual credit card account number” disclosed by Gomez) in that the authentication cryptogram is combined with the static EPIC account number to form limited-use payment information and provided to the merchant rather than the issuer supplied payment information. SAMSUNG-1007, 1:55-2:39, 5:19-24, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3; SAMSUNG-1003, ¶338.

[1.j]

Gomez discloses “communicating a payment card identifying number to a payment processing system, and communicating *the authentication cryptogram* in a payment card account name field to the payment processing system” “using near field communication (NFC).” SAMSUNG-1007, 2:50-54, 7:49-54, 8:16-23. As discussed above, in some embodiments, the “payment card identifying number” is “an EPIC account which is not itself a live payment card account, but to which are linked one or more live payment card accounts” and therefore is not an issuer supplied payment information. SAMSUNG-1007, 5:19-24, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3; 1:55-2:39; SAMSUNG-1003, ¶339.

[1.k]

Gomez describes that “a great variety of useful information may be displayed, including...secure messages, alarms, and other notifications.” SAMSUNG-1007, 12:58-67, 10:18-26, 11:53-62. Gomez teaches that a transaction status is provided “back to the merchant 406 to indicate either approval or denial of the transaction.” *Id.*, 6:56-64. As discussed above, Mullen discloses that in the predictable combination, the transaction status is further provided to the user device for display to the user. SAMSUNG-1009, [0287], [0339]-[0340], [0038], [0210]; SAMSUNG-1003, ¶¶340-342. For example, the “mobile device may provide receipt delivery options to a user” including “in a graphical format.” SAMSUNG-1009, [0012], [0210].

[2]

Gomez’s “**authentication cryptogram**” is generated using a seed value and a temporal signal value such as “the date/time of the transaction” or “the sequence value (or sequential number) of the attempted use.” SAMSUNG-1007, 1:58-2:4, 5:25-32, 6:27-33, 7:17-48, 10:66-11:6. The “seed value is unique for each payment card, [] corresponds to the payment card identifying number,” and “may include certain non-random customer specific information, such as a **unique customer key**.” *Id.*, 7:17-48; SAMSUNG-1003, ¶¶343-345.

[3]

Claim [3] does not require that the cryptogram number be distinct from the limited-use payment information of claim 1. Gomez's "authentication cryptogram" is dynamically generated on the device by combining "a seed value" and "a temporal signal" such as "the sequence value (or sequential number) of the attempted use." SAMSUNG-1007, 1:58-2:4, 7:41-43, 21:37-48, 7:17-26, 8:36-41, 10:58-11:6, FIG. 7; SAMSUNG-1003, ¶¶346-350. The "seed value is *unique for each payment card*" and can include "*unique customer key*" and therefore provides the claimed device account number, device identifier, device secrets, device key, and payment issuer key. *Id.*, 7:17-48, 12:30-34, 16:31-34, 16:64-17:13; SAMSUNG-1003, ¶347. Alternatively, Gomez discloses that the temporal value can be a sequence counter or time and it would have been obvious to a POSITA to use *both* a sequence counter and time when generating the cryptogram to increase the security of the resulting cryptogram by incorporating multiple temporal values. SAMSUNG-1007, 5:25-32, 6:27-33, 7:17-48, 10:66-11:6; SAMSUNG-1003, ¶347.

The authentication cryptogram is provided in place of "the 3-digit security code" provided by the issuer to validate the transaction. SAMSUNG-1007, 9:65-10:17, 2:4-12, 14:37-63, 6:23-38; SAMSUNG-1003, ¶348. The cryptogram "is *generated uniquely for each attempted use of the payment card*" and good for a single transaction. SAMSUNG-1007, 1:58-2:1, 21:37-48; 5:15-16, 8:36-39, 14:3-4;

SAMSUNG-1008, 4:26-30, 8:28-33, 11:38-51; SAMSUNG-1003, ¶349. The sequential counter used to generate the cryptogram is “increment[ed] for each attempted use” such that each cryptogram is unique for each attempted use. SAMSUNG-1007, 8:36-39.

[4]

Gomez’s seed value, which is used to generate the authentication cryptogram, “is *unique for each payment card*, and *corresponds to the payment card identifying number*” and is therefore a device account number. SAMSUNG-1007, 7:17-48, 12:30-34, 16:31-34, 16:64-17:13; SAMSUNG-1003, ¶¶351-354. The seed value “corresponds to the payment card identifying number,” and therefore the expiration date for the payment card number is the expiration date for the seed value, giving the seed value a limited time-duration of valid use. SAMSUNG-1007, 3:67-4:4, 5:50-57, 11:23-27, 7:17-48; SAMSUNG-1003, ¶352. Alternatively, it would have been obvious to a POSITA to make the seed value of a limited time-duration of valid use tied to the payment account expiration date so that a seed value generated using an expired account number could not be used for transactions. SAMSUNG-1003, ¶352.

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

mitted to the payment processing system to perform a payment transaction. SAMSUNG-1007, 2:50-3:3, 5:48-60, 6:23-38. The payment card identifying number can be “an EPIC account number” “which is not itself a live payment card account, but to which are linked one or more live payment card accounts.” SAMSUNG-1007, 6:7-22, 5:19-24. Therefore the combined payment information is conveyed in place of card issuer information during a payment transaction. SAMSUNG-1003, ¶353.

[5]

Gomez describes cryptographically combining the seed value and temporal value to generate the authentication cryptogram and therefore combines at least one of a device transaction sequence counter, a device account number, device identifiers, device secrets, device keys, issuer secrets, a payment card account number, a time, and an expiration date. *See supra*, Claims [2]-[4]; SAMSUNG-1007, 5:25-32, 6:27-33, 7:17-48, 8:36-41, 10:58-11:6; 10:64-11:6, 12:30-34, 16:31-34, 16:64-17:13, 1:58-63, FIG. 7; SAMSUNG-1003, ¶¶355-358. The authentication cryptogram is provided in place of the card issuer card security code. *See supra*, Claims [3]-[4]; SAMSUNG-1007, 9:65-10:17, 2:4-12, 14:37-63; SAMSUNG-1003, ¶¶348, 356. “[T]he generated authentication cryptogram may be displayed.” SAMSUNG-1007, 12:64-13:4, 13:22-33, 21:5-20.

[6]

An account authentication request including “the EPIC account number, the date and time of the transaction, and the authentication cryptogram” is sent to an authentication server. SAMSUNG-1007, 6:12-38, 14:21-27, 17:40-62. The authentication server “independently generat[es] a ‘reference’ authentication cryptogram based upon the seed value corresponding to the EPIC account number, and based upon the *date/time of the transaction* (or other temporal signal value, as described below).” *Id.* As discussed above (*supra*, Claims [2]-[4]), the “other temporal signal values” include a transaction sequence counter and the seed value provides at least a device account number, user account information, issuer secrets, issuer keys, and issuer-provided device keys. SAMSUNG-1007, 7:17-48, 8:36-41, 10:58-11:6, 12:30-34, 16:31-34, 16:64-17:13; SAMSUNG-1003, ¶¶359-362. The authentication cryptogram is provided in place of the card issuer card security code. *See supra*, Claims [3]-[4]; SAMSUNG-1007, 9:65-10:17, 2:4-12, 14:37-63; SAMSUNG-1003, ¶¶348, 360.

The payment processor/authentication server authorizes the transaction “[i]f the server-calculated reference authentication cryptogram matches the received authentication cryptogram.” SAMSUNG-1007, 6:23-64, 17:23-28, 18:20-25. The transaction is rejected if a previously used authentication cryptogram is reused or has expired. SAMSUNG-1007, 5:34-47, 21:37-48; SAMSUNG-1003, ¶361.

[7]

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

[8]

Gomez describes priming: “the cardholder successfully presents a credential, such as a fingerprint or PIN number, into the payment card.” SAMSUNG-1007, 5:13-18, 13:40-44; SAMSUNG-1003, ¶¶366-368.

[9]

The predictable combination provides a touchscreen display of “**a requester's identity/location**, a time of the request, **an amount (if applicable)** and/or **other relevant information**.” SAMSUNG-1008, 5:1-17; SAMSUNG-1003, ¶¶369-372.

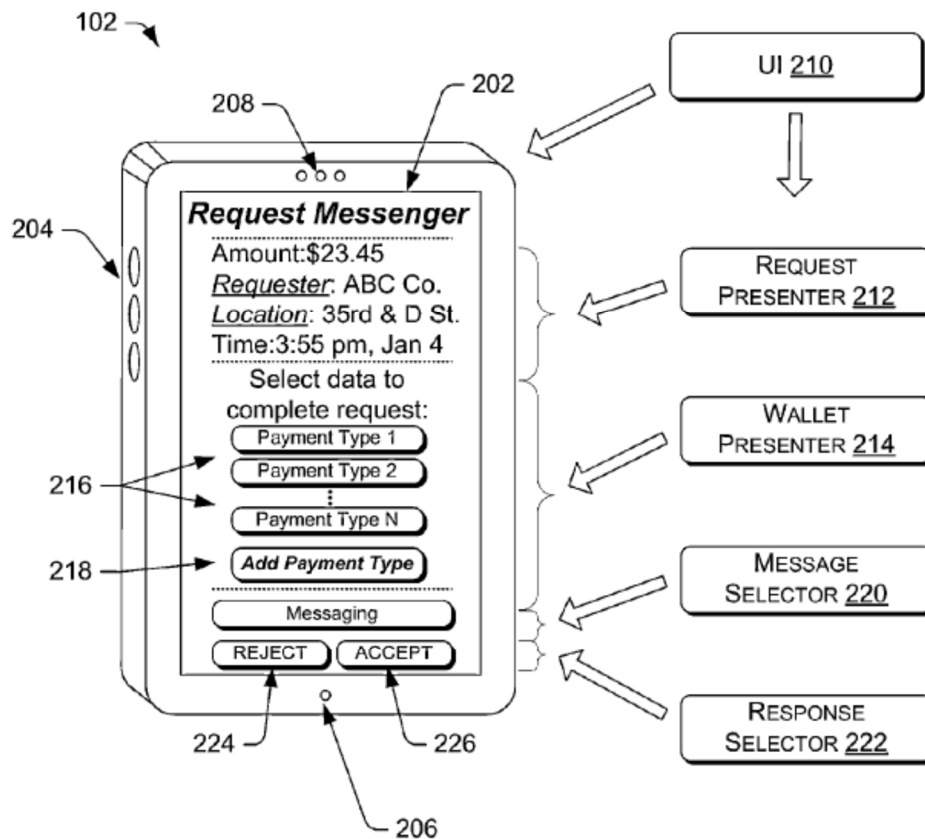


Fig. 2

SAMSUNG-1008, FIG. 2. As shown in FIG. 2, the display includes “a reject option 224 and an accept option 226” and a plurality of selectable payment options. *Id.*, 6:2-15, 5:18-41; 4:40-46; SAMSUNG-1009, [0037], [0326], [0328], [0353], FIGs. 36-40 (various indicia); SAMSUNG-1007, 20:30-21:20; SAMSUNG-1003, ¶¶373-374; *Supra*, Element [1.f].

[11]

The device of the resulting combination allows “selectively approving or rejecting requests for personal information using the mobile wallet server” after a

transaction timeout period or an exceeded transaction amount. SAMSUNG-1008,
2:32-49, 6:2-15, 12:34-13:6, FIG. 2; SAMSUNG-1003, ¶¶375-377.

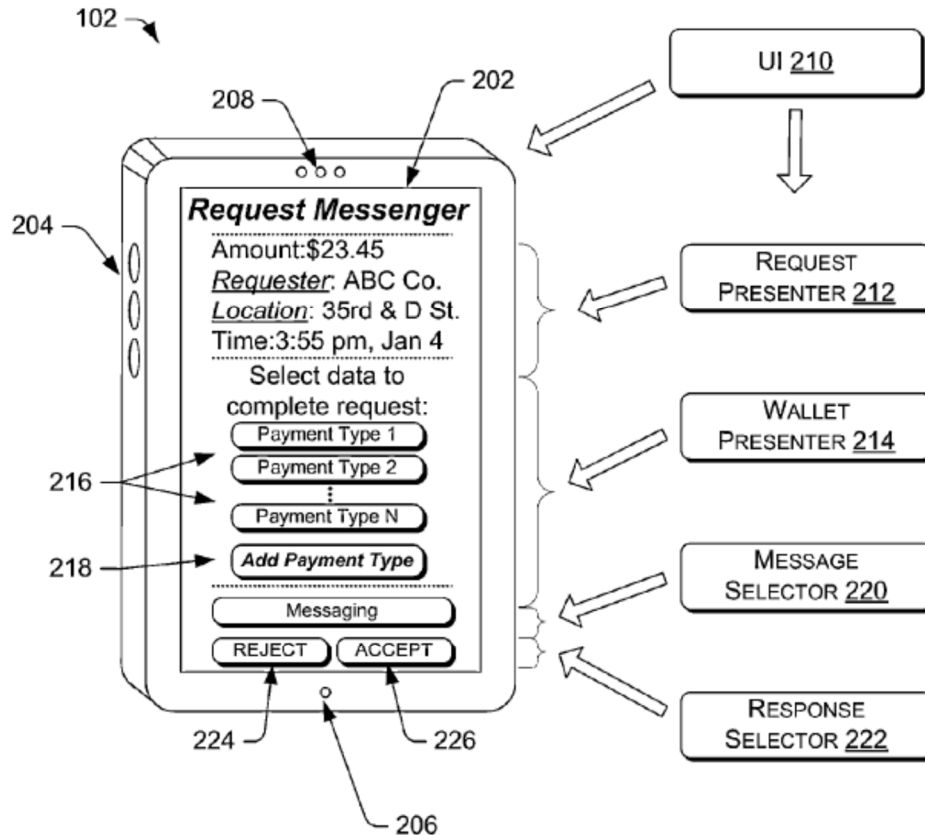


Fig. 2

SAMSUNG-1008, FIG. 2.

[12]

Gomez discloses “*after entering a customer-established PIN authorization code*, a customer may then view all credit cards in their EPIC account by their description name (or nickname) and *card logo*, and *select the card* they wish to use.”

SAMSUNG-1007, 20:43-21:20, 20:12-23. If the user does not select a payment

option, “the EPIC card defaults to the pre-established credit card account selection order.” *Id.*; SAMSUNG-1003, ¶¶378-380; *see also* SAMSUNG-1009, [0037], [0326], [0328], [0353], FIGs. 36-40.

G. [GROUND 2B] – Obviousness based on Gomez-Amacker-Mullen-Smith-Deibert (Claims 10, 14)

A POSITA would have applied the teachings of Deibert to the Gomez-Amacker-Mullen-Smith combination in the same manner, for the same reasons, and to achieve the same benefits discussed in Ground 1C, *supra*, and would have had a reasonable expectation of success. SAMSUNG-1003, ¶¶381-382.

[10]

The Gomez-Amacker-Mullen-Smith-Deibert combination renders obvious Claim [10] based on Deibert’s disclosure for the same reasons discussed in Ground 1C, *supra*. SAMSUNG-1003, ¶¶383-385, 286-288; *see also supra* Ground 2A, Elements [1.d]-[1.e] (transactions conducted using NFC).

[14]

Gomez discloses requiring a PIN (a passcode) to access the payment application/functionality prior to selecting a specific payment method. *Supra* Ground 2A, Claim [12]; SAMSUNG-1007, 20:43-21:20, 20:12-23. A POSITA would have recognized that user selection of a payment method provides a priming operation after entry of the PIN/passcode. SAMSUNG-1003, ¶387. Deibert’s disclosure

renders obvious the additional recitations of Claim [14] for the same reasons discussed in Ground 1C, *supra*. SAMSUNG-1003, ¶¶386-389, 289-292.

H. [GROUND 2C] – Obviousness based on Gomez-Amacker-Mullen-Smith-Deibert-Power (Claim 13)

[13]

A POSITA would have applied the teachings of Power to Gomez-Amacker-Mullen-Smith-Deibert in the same manner and for the same reasons as discussed with respect to the Royyuru-Phillips-Casey-Deibert-Power combination. *Supra*, Ground 1D; SAMSUNG-1003, ¶¶390-393, 294.

Mullen discloses that the resulting device can be primed to perform a payment transaction (“activated for use”) when the user touches a displayed virtual card button twice. SAMSUNG-1009, [0327], [0360], [0370]; SAMSUNG-1003, ¶¶392-397; SAMSUNG-1001, 9:64-10:3, 17:19-23. Furthermore, Gomez discloses requiring PIN (passcode) entry to re-validate a user. SAMSUNG-1007, 20:43-21:20, 20:12-23; SAMSUNG-1003, ¶394.

Disclosure from Deibert and Power renders obvious all remaining elements of claim 13 for the reasons discussed in Grounds 1C-1D, 2B, *supra*. SAMSUNG-1003, ¶¶395-397, 296-299.

I. [GROUND 2D] – Obviousness based on Gomez-Amacker-Mullen (Claims 15-20, 22-23)

A POSITA would have applied the teachings of Amacker and Mullen to Gomez in the same manner, for the same reasons, and to achieve the same benefits discussed in Ground 2A, *supra*. SAMSUNG-1003, ¶¶398-399.

[15.pre]

Supra, Preamble [1.pre].

[15.a]

Supra, Element [1.e].

[15.b]

Supra, Elements [1.c], [1.f], [9].

[15.c]

Supra, Elements [1.f], [9], [11]-[12].

[15.d]

Supra, Element [1.e].

[15.e]

Supra, Element [1.j].

[15.f]

Supra, Claim [9]

[15.g]

Supra, Elements [1.g]-[1.h], [9]

[15.h]

Supra, Claims [9], [11].

[16]

The device of the Gomez-Amacker-Mullen combination has a touchscreen.

Supra, Ground 2A, [1.c]; SAMSUNG-1008, 4:51-60; SAMSUNG-1009, [0151], [0326]. The confirmation screen includes a requester identity, amount, and accept/reject options. SAMSUNG-1008, 5:1-17, 6:2-15.

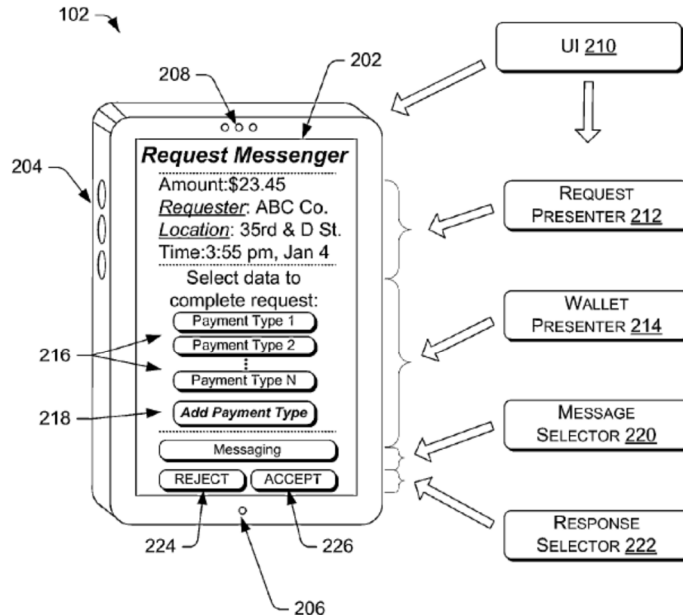


Fig. 2

[17]

Supra, Elements [1.f]-[1.h], [9], [11]-[12].

[18]

Supra, Elements [1.a], [8].

[19.pre]-[19.b]

The resulting device includes a processor coupled to memory and can be implemented as a mobile device/phone. SAMSUNG-1007, 10:34-38, 11:19-38, 2:55-3:3, FIG. 9; SAMSUNG-1008, 2:13-25; SAMSUNG-1009, [0041], [0458]; SAMSUNG-1003, ¶¶429-431.

[19.c]

Supra, Element [1.c].

[19.d]

Gomez discloses “an activation input device” including “a fingerprint reader.” SAMSUNG-1007, 10:34-38, 11:14-31, 2:55-59; SAMSUNG-1008, 4:51-60, 5:42-49, 8:49-53; SAMSUNG-1007, 13:22-33; SAMSUNG-1009, [0151], [0326]; SAMSUNG-1003, ¶¶433-434.

[19.e]

Supra, Elements [1.e]-[1.f].

[19.f]

The resulting combination includes a processor that executes instructions to perform the described functions. SAMSUNG-1007, 2:59-64; SAMSUNG-1008, 6:21-30; SAMSUNG-1003, ¶436.

[19.g]

Supra, Ground 2A, Elements [1.a], [7]-[8].

[19.h]

Gomez's device generates the cryptogram "upon verification of a valid credential" (priming). SAMSUNG-1007, 2:59-64, 5:13-18, 7:17-20; SAMSUNG-1003, ¶438. At this point, "the card is considered ready to communicate with the payment processing system." SAMSUNG-1007, 8:11-15, 9:30-41, 11:53-62; SAMSUNG-1008, 2:32-57, 6:2-15.

[19.i]

Supra, Ground 2A, Elements [1.f]-[1.h].

[19.j]

Supra, Ground 2A, Elements [1.f], [8]-[9], [11]-[12].

[19.k]

Gomez discloses that the predictable combination generates a limited-use payment information for use in place of card issuer payment information in the form of the authentication cryptogram. *Supra*, Element [1.i]; SAMSUNG-1007, 1:58-2:4, 5:13-24, 7:26-8:9, 1:55-2:39, 5:48-6:51, 17:40-62, 18:4-13, 18:50-19:3; SAMSUNG-1003, ¶441.

Amacker discloses that, in the predictable combination, the authentication cryptogram is generated in response to receiving the NFC transaction payment request. SAMSUNG-1003, ¶442; SAMSUNG-1008, 2:37-3:3, 3:42-57, 4:37-50, 6:37-61; *Supra*, [1.e]. The device "generate[s] the limited use number following

the ‘yes’ route” of the user accepting the request. *Id.*, 12:9-17, 10:66-11:64; SAMSUNG-1003, ¶442. In another example, the limited use number is generated and provided to the merchant “[u]pon a selection of ‘accept’” in response to the payment request. SAMSUNG-1008, 2:46-49.

[19.l]

Supra, Element [1.j]

[19.m]

Supra, Element [1.k]

[20]

Supra, Elements [1.a], [1.c], [8], [12]. A valid PIN entry provides a correct passcode entry sequence and a correct user response input from a security challenge. SAMSUNG-1003, ¶¶446-448; SAMSUNG-1007, 2:59-64, 5:13-18, 7:9-16, 20:43-21:20, 20:12-23, 11: 15-38 (“fingerprint reader”)

[22]

Gomez discloses a memory coupled to the processor. SAMSUNG-1007, 10:34-38. As discussed with respect to Claim [4], *supra* Ground 2A, Gomez’s seed value (stored on the device), used to generate the authentication cryptogram, “is *unique for each payment card*, and *corresponds to the payment card identifying number*” and therefore provides a device account number of limited-use (i.e., limited in use to the specific card). SAMSUNG-1007, 7:17-48, *see also id.*, 12:30-34, 16:31-34, 16:64-17:13, 5:25-28; SAMSUNG-1003, ¶¶449-452. The seed value

includes “a unique customer key.” SAMSUNG-1007, 7:31-41, 14:30-36, 9:23-29.

The limited use number in the resulting combination can be provided by the issuer. SAMSUNG-1008, 11:58-12:8; SAMSUNG-1003, ¶450. Having the issuer provide the seed value would beneficially improve the system by ensuring that the seed value is known to the issuer (and payment processor) for purposes of verifying the authentication cryptogram. SAMSUNG-1003, ¶450.

As discussed with respect to Claim [4], *supra* Ground 2A, a POSITA would have recognized that, because the seed value “corresponds to the payment card identifying number,” the expiration date for the payment card number is also the expiration date for the seed value. SAMSUNG-1007, 3:67-4:4, 5:50-57, 11:23-27, 7:17-48; SAMSUNG-1003, ¶451. Alternatively, it would have been obvious to a POSITA to make the seed value of a limited time-duration of valid use tied to the payment account expiration date so that a seed value generated using an expired account number could not be used for transactions. SAMSUNG-1003, ¶451.

[23]

Supra, Ground 2A, Elements [1.j], [2]-[3].

J. [GROUND 2E] – Obviousness based on Gomez-Amacker, Mullen-Smith-Carlson (Claim 4)

A POSITA would have been prompted to apply the teachings of Carlson to the Gomez-Amacker-Mullen-Smith combination such that Gomez’s seed value is “set to expire...after a certain time period” to provide “protection to the consumer's

account” by limiting the amount of possible damage should the seed value be stolen. SAMSUNG-1013, [0036], [0044]; SAMSUNG-1003, ¶¶456-459.

Furthermore a POSITA would have recognized that application of Carlson’s teachings to the Gomez-Amacker-Mullen-Smith system is merely the application of known techniques to a known system ready for improvement to yield predictable results and would have had a reasonable expectation of success in making such a modification. SAMSUNG-1003, ¶459.

Turning to claim [4], in the Gomez-Amacker-Mullen-Smith-Carlson system, the seed value is “set to expire...after a certain time period” by the payment processor or issuer. SAMSUNG-1013, [0036], [0044], [0086]; SAMSUNG-1003, ¶¶460-462. The seed value therefore has an expiration date of limited duration of validity and is therefore of limited time-duration of valid use. SAMSUNG-1003, ¶461. All other elements of claim [4] are disclosed by the Gomez-Amacker-Mullen-Smith-Carlson combination for the reasons discussed in Ground 2A, *supra*. SAMSUNG-1003, ¶¶461, 351-354.

K. [GROUND 2F] – Obviousness based on Gomez-Amacker-Mullen-Carlson (Claim 22)

A POSITA would have applied the teachings of Carlson to the Gomez-Amacker-Mullen combination to set the seed value to expire after a certain time

period in the same manner and for the same reasons discussed in Ground 2E, *supra*. SAMSUNG-1003, ¶¶463-467, 458. All other elements of claim [22] are disclosed by the Gomez-Amacker-Mullen-Carlson combination for the reasons discussed in Ground 2D, *supra*. SAMSUNG-1003, ¶¶466, 449-452.

L. [GROUND 2G] – Obviousness based on Gomez-Amacker-Mullen-Carlson-Royyuru (Claim 21)

A POSITA would have been prompted to apply the teachings of Royyuru to Gomez-Amacker-Mullen-Carlson to use additional values when generating the authentication cryptogram including one or more unpredictable/undeterminable and one or more expiration dates. SAMSUNG-1004, [0057], [0051]; SAMSUNG-1003, ¶¶468-470. A POSITA would have recognized that using these additional values when generating Gomez’s authentication cryptogram would have increased security because the cryptogram would be based on additional values that would be difficult for third parties to determine or intercept. SAMSUNG-1003, ¶469; SAMSUNG-1004, [0004].

It would have been beneficial to combine the seed value with the expiration date for the seed value when generating the authentication cryptogram in the predictable combination to increase the difficulty for third parties to replicate it. SAMSUNG-1003, ¶470. Carlson teaches that in the resulting combination the seed value is “set to expire...after a certain time period.” SAMSUNG-1013, [0036],

[0044], [0086]; SAMSUNG-1003, ¶470; *Supra* Grounds 2E-2F. Royyuru discloses that values similar to the seed value (Royyuru's IKCV) can be combined with their respective expiration dates or other unpredictable/undeterminable numbers known to the device (which would include the expiration for the seed value) to increase security. SAMSUNG-1004, [0057], [0051]. For example, Royyuru's DTC, which is highly similar to Gomez's authentication cryptogram, is generated using values including "expiration date" and the IKCV. SAMSUNG-1004, [0057], [0005]-[0006]; SAMSUNG-1003, ¶265. A POSITA therefore would have similarly combined the seed value and its respective expiration date when generating the authentication cryptogram in the resulting combination. The Gomez-Amacker-Mullen-Carlson-Royyuru combination provides the remaining elements of Claim [21] for the reasons discussed with respect to Claim [4] (Grounds 2A, 2E) and Claim [22] (Grounds 2E-2F), *supra*. SAMSUNG-1003, ¶¶351-354, 449-452, 461, 466.

IV. DISCRETIONARY CONSIDERATIONS

None of the relied upon references were cited during prosecution. The facts associated with this Petition strongly favor institution, even under the *Fintiv* framework, as clarified by interim guidelines dated June 22, 2022. SAMSUNG-1016, 2.

Factor 1 (Stay)—Neither party has requested a stay.

Factor 2 (Trial Date)—Patent Owner's complaint was filed on May 11,

2022 in the Eastern District of Texas (E.D. Tex.). SAMSUNG-1100. Based on a median time from filing to trial in E.D. Tex. of 24.5 months, the likely disposition date is May, 2024. SAMSUNG-1103, 35. A final written decision (“FWD”) is anticipated in May, 2024. The Board should not deny institution due to the close proximity of the FWD and disposition date. SAMSUNG-1101, 3. Additionally, with a gap of just over three and a half months between the expected FWD and start of trial (*see* SAMSUNG-1104), the “efficiency and system integrity concerns that animate the *Fintiv* analysis are not as strong all other things being equal.” *Google LLC v. Parus Holdings, Inc.*, IPR2020-00846, Paper 9 at 14 (PTAB Oct. 21, 2020).

Factor 3 (Investment)—The bulk of investment in the Related Litigation by the parties and court has yet to occur. Significantly, no part of claim construction and no document production has yet occurred. SAMSUNG-1104. By the time of institution in this proceeding, the Related Litigation will be at a similar posture where “much of the district court’s investment relates to ancillary matters untethered to the validity issue itself.” *Sand Revolution*, IPR2019-01393, Paper 24 at 10-11.

Factor 4 (Overlap)—Should IPR be instituted based on this Petition, Petitioner stipulates that it will not pursue in the Related Litigation any invalidity grounds against the Challenged Claims of the ’579 patent that are the same as

those raised in this Petition.⁴ Thus, if IPR is instituted, there will be no overlap or concerns of duplicative efforts. *See Sand Revolution*, Paper 24 at 11-12. Factor 4 thus weighs against discretionary denial. *Id.*; *Coolit Systems, Inc. v. Asetek Danmark A/S*, IPR2021-01995, Paper 10 at 12-13 (PTAB Dec. 28, 2021).

Factor 6 (Merits and Other Circumstances)—The strength of the merits alone is enough to justify institution in the public interest, and outweighs any inefficiencies born of parallel litigation. *See Fintiv* at 15; SAMSUNG-1101, 1. Petitioner has been diligent in filing this Petition just over two months after service of Patent Owner’s preliminary infringement contentions and identification of asserted claims on September 12, 2022.

V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Samsung”) are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

⁴ Petitioner reserves all rights to pursue these invalidity grounds in the Related Litigation if IPR based on this Petition is not instituted.

The '579 Patent is the subject of a civil action, *CardWare Inc. v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.*, 2:22-cv-00141, E.D. Tex., filed May 11, 2022 (SAMSUNG-1100). Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the '579 Patent.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR39843-0145IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Patrick J. Bisenius, Reg. No. 63,893 Nicholas Stephens, Reg. No. 74,320 Kiersten Batzli, Reg. No. 75,476 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR39843-0145IP1@fr.com

(referencing No. 39843-0145IP1 and cc'ing PTABInbound@fr.com, [\[ptab@fr.com\]\(mailto:ptab@fr.com\), \[jjm@fr.com\]\(mailto:jjm@fr.com\), \[bisenius@fr.com\]\(mailto:bisenius@fr.com\), \[nstephens@fr.com\]\(mailto:nstephens@fr.com\) and](mailto:axf-</p></div><div data-bbox=)

batzli@fr.com).

Respectfully submitted,

Dated November 21, 2022

/Patrick J. Bisenius/
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Patrick J. Bisenius, Reg. No. 63,893
Nicholas Stephens, Reg. No. 74,320
Kiersten Batzli, Reg. No. 75,476
Fish & Richardson P.C.
3200 RBC Plaza, 60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2023-00196)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,981 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated November 21, 2022

/Patrick J. Bisenius/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Patrick J. Bisenius, Reg. No. 63,893
Nicholas Stephens, Reg. No. 74,320
Kiersten Batzli, Reg. No. 75,476
Fish & Richardson P.C.
3200 RBC Plaza, 60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on November 21, 2022, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided via Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

David Wyatt
c/o Murabito, Hao & Barnes
111 North Market Street, Suite 700
San Jose, CA 95113

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667