IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	David Wyatt	
U.S. Patent No.:	11,176,538	Attorney Docket No.: 39843-0146IP1
Issue Date:	November 16, 2021	
Appl. Serial No.:	17/075,637	
Filing Date:	October 20, 2020	
Title:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	

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. 11,176,538 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

EXHIBITS

SAMSUNG-1001 U.S. Patent No. 11,176,538 to Wyatt ("the '538 Patent")

SAMSUNG-1002 Excerpts from the Prosecution History of the '538 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-1007-1010 [RESERVED]

SAMSUNG-1011 U.S. Patent Publication No. 2008/0017704 A1 to VanDeburg et al. ("VanDeburg")

SAMSUNG-1012 RESERVED

SAMSUNG-1013 U.S. Patent Publication No. 2008/0319905 to Carlson ("Carlson")

SAMSUNG-1014 U.S. Patent Publication No. 2007/0278291 to Rans et al. ("Rans")

SAMSUNG-1015 U.S. Patent Publication No. 2012/0150750 to Law et al. ("Law")

SAMSUNG-1016-1021 [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 payment transaction, the method comprising:
[1.a]	receiving an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user; and,
[1.b]	wherein the authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface, a gesture sensor, a motion sensor, and a biometric sensor; and,
[1.c]	receiving a request for a transaction payment at said electronic device via an NFC interface of the device; and,
[1.d]	displaying, on a display of the device, a transaction payment request and at least a portion of an original static issuer-supplied payment account information associated with a payment method, for a user selection in paying the payment request; and,
[1.e]	retrieving from a memory attached to a processor of the device, a device-specific static limited-use payment information, associated with said selected payment method; and,
[1.f]	dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method; and,
[1.g]	using said limited-use payment information in place of at least a portion of said selected original issuer-supplied payment information for the transaction; and,
[1.h]	combining of said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information; and,

Claim Element	Claim Language
[1.i]	transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction; and,
[1.j]	receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the transmitted complete device payment information by a payment processor authority and a payment issuer authority; and,
[1.k]	visually conveying the transaction payment authorization status via a user-interface displayed on said display.
[2]	The method of claim 1, further comprising receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.
[3]	The method of claim 1, further comprising receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device.
[4]	The method of claim 3, wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment transactions performed by said device, in place of said selected issuer-payment information; and, wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.
[5.a]	The method of claim 3, wherein the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information; and,

Claim Element	Claim Language
[5.b]	wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction; and,
[5.c]	wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device; and,
[5.d]	a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number; and,
[5.e]	an adjusting of said transaction sequence counter count on a per transaction basis; and,
[5.f]	an authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching.
[6.a]	The method of claim 3, wherein the generating the limited-use payment information further utilizes a secure combination of said information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information; and,
[6.b]	a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority; and,
[6.c]	a payment processing authority comparing said device generated payment information, and said payment processing authority generated

Claim Element	Claim Language
	payment information, for a verifying of a limited-use payment as valid; and,
[6.d]	a conveying of said validation result as a declining or accepting of said transaction payment; and,
[6.e]	upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction.
[7]	The method of claim 3, wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including: a confirmation result of payment authority authenticating said device-transmitted limited-use payment information, a confirmation result of payment authority authenticating said device-transmitted complete device payment information, an NFC transaction status, a transaction payment amount, a payment facility wherein the transaction was performed, a merchant information, an original issuer payment account information, an original payment issuer information, a request for an authorized-user approval of the transaction, a payment processing status, an issuer payment approval status, and a payment completion status.
[8.a]	The method of claim 1, wherein the generating the limited-use payment information is comprising: a device-specific account number; and,
[8.b]	a device-internal transaction sequence counter count; and,
[8.c]	an information unique to the user and device which does not pass in the transaction; and,
[8.d]	at least one payment authority-supplied information which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements, and

Claim Element	Claim Language
[8.e]	wherein said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information.
[9]	The method of claim 8, wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number, capable of passing in at least a portion of the device transaction payment information.
[10]	The method of claim 9, wherein the generating the limited-use payment information further utilizes a secure combination with a device key, and a payment issuer secret.
[11]	The method of claim 1, wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of: a device payment transaction sequence counter count, and at least one of a set comprising: a device-specific internal information associated with said device and also known to a payment processing authority; and, at least one payment processing authority-specific information provided by a payment processing authority; and, a payment issuer specific information provided by a payment issuer.
[12]	The method of claim 1, wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information.
[13]	The method of claim 1, wherein the generating the limited-use payment information utilizes a merchant identifying information.
[14]	The method of claim 1, wherein the generating the limited-use payment information utilizes a transaction facility information.

Claim Element	Claim Language
[15]	The method of claim 1, wherein the generating the limited-use payment information utilizes a payment amount.
[16]	The method of claim 1, wherein the generating the limited-use payment information utilizes a payment facility type.
[17]	The method of claim 1, wherein the generating the limited-use payment information utilizes an online transaction information.
[18.a]	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 payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number; and
[18.b]	wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number, via the incrementing of said transaction sequence counter count on a per-transaction basis, and using said updated transaction sequence counter count in said generation of said cryptogram; and,
[18.c]	wherein said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device.
[19.pre]	A method of performing an online payment transaction, the method comprising:
[19.a]	receiving an input signal at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface of the electronic device;
[19.b]	a displaying of the payment request notification at a touch-screen display user-interface of the electronic device; and,

Claim Element	Claim Language
[19.c]	upon an authorizing of a valid device user, displaying at least one user-selectable payment account option, and requesting a user approval of payment, via the touch-screen display user-interface;
[19.d]	receiving, from a valid device user, a payment selection and authorization approval input on the electronic device;
[19.e]	generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and
[19.f]	combining said at least one limited-use numbers, with said selected account information, to form a complete payment information; and,
[19.g]	wherein the receiving of a user payment approval authorization through the user-interface of the electronic device, is comprising a displaying on said display at least a portion of information comprising: the payment request, the merchant, the amount, and the transaction information; and,
[19.h]	receiving a user input providing for at least one transaction authorization actions, from a set of actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method; and,
[19.i]	on receiving said user payment approval authorization input, a transmitting by the wireless interface of the approved complete payment information for the online transaction.
[20.a]	The method of claim 19, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuing authority, and wherein dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count, a user information, a payment account number, information and secrets known to a payment processing authority; and

Claim Element	Claim Language
[20.b]	wherein further, said dynamically generating said card validation value number results in a one-time limited-use payment information, on incrementing the device transaction sequence counter count on each transaction payment, and said device combining said current transaction sequence count at the instant of generating said cryptogram number.
[21.a]	The method of claim 19, wherein at least a portion of said limited-use number comprises a static device account number,
[21.b]	and wherein the static device account number is of a limited scope of valid use to a specific device,
[21.c]	and wherein further a payment processing authority provides said device account number unique for the specific electronic device, in place of payment issuer information, in performing payment transactions by the electronic device, and further comprising:
[21.d]	performing a payment transaction by the electronic device including the dynamically generated limited-use number;
[21.e]	combining the dynamically-generated number and the static device account number within a device-generated complete payment information; and
[21.f]	conveying said device-generated complete payment information, in place of a selected payment issuer information, when the device is performing payment transactions; and
[21.g]	wherein a using of said static device account number without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage.
[23.a]	The method of claim 19, wherein a payment processing authority verifying and authorizing a transmitted limited-use number based on a time of use, and cryptographically combining a transaction sequence count information; a device account number; a user account information; a

Claim Element	Claim Language
	payment issuer information; a payment processing authority secrets; a transaction information; and,
[23.b]	further comprising: receiving an authorization of said transaction, responsive to verifying a valid limited-use number appearing in a transaction information in place of the payment issuer information; and
[23.c]	a rejecting by the payment processing authority, on a detecting as invalid at least one verification test, from a set of tests comprising: a mis-matching of the transacted limited-use number, and the authority cryptographically-combined number; a transactional use of a device account number outside of its limited scope of valid payment reader facility use; a transactional use outside of a valid time window; a transactional re-use of a number limited to a one-time use; and, a transactional use of an expired number outside of a limited time-of-use.
[24]	The method of claim 19, wherein the user selecting of a payment method at an electronic device comprises receiving a user touch input selection, via the user interface, of a displayed payment method option, on the device touch-screen display interface.
[25.pre]	A non-transitory, computer-readable medium storing computer executable instructions that when executed by one or more processors, cause the one or more processors to:
[25.a]	accept a priming action of the electronic device by an identified valid device user, identified from the device inputs;
[25.b]	enable the electronic device for imminent performance of a payment operation responsive to the priming action of said valid user;
[25.c]	display a summary of online purchase information including the merchant information and the purchase amount; and,
[25.d]	display at least one selectable issuer payment account methods on a display; and,

Claim Element	Claim Language
[25.e]	receive a payment selection and approval authorization from said valid device user via a human input sensing at the device; and
[25.f]	responsive to receiving a valid user transaction payment approval, generate a device-specific limited-use payment information for use in place of at least a portion of said selected issuer payment account information on the device,
[25.g]	form a complete combined device payment information from a dynamically generated portion and a statically generated portions stored in a memory of the device,
[25.h]	wherein the communication interface is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction; and
[25.i]	wherein further the processor is operable to receive an approval and a denial confirmation from an online payment facility of the complete device payment information, and cause the display to visually convey a status of the online purchase transaction.
[26.a]	The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more processors to: receive the priming action of a user via the device human input sensors;
[26.b]	identify an authorized valid device user through a human to device inputs, selected from at least one security challenge, of a set of human to device input challenges comprising: a correct passcode touch entry sequence, a correct touch gesture, a touch input of a known device user, a biometric recognition of a valid user, a biometric sensing of a valid user's skin touch, a touch input sensor recognition of a unique customer identifier, a security question which a valid user could answer correctly, and receiving a correct user response input, from a security challenge presented on the device display; and

Claim Element	Claim Language
[26.c]	responsive to receiving an incorrect user response input, offer a reduced number of additional challenge attempts before failing the user authorization at the device, and denying the payment authorization.
[27.a]	The non-transitory, computer-readable medium of claim 25, wherein the one or more processors include a cryptographic processor, and wherein the executable instructions further cause the one or more processors to:
[27.b]	cryptographically compute a dynamically generated one-time-use cryptogram number,
[27.c]	and combine said dynamically generated portion with a static device-specific account number known to a payment processing authority and limited in use to the device use in place of an issuer payment method; and,
[27.d]	wherein further said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count, a payment account information, a user information, and information stored in the device and specific to the device and which is not communicated in the transaction; and,
[27.e]	wherein said transaction sequence counter, said information and said secrets are known to both said device, and to said payment processing authority; and,
[27.f]	wherein further said static device-specific device account number is known to a payment issuer, and has a device-specific expiration date of limited duration of validity; and,
[27.g]	wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram,

Claim Element	Claim Language
[27.h]	and transmitting said complete device payment information when said issuer payment account method is selected.
[28.a]	The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further causes the one or more processors to perform: a combining of a static device-specific payment account information, a device generated information, and other user and account information stored on the device which is uniquely identifying the specific user, specific selected account, and the specific device; and,
[28.b]	a generating of a limited-use payment information by the one or more device processors cryptographically generating at least one one-time limited-use cryptogram numbers; and,
[28.c]	wherein the one or more device processors are further operable to combine said limited-use static device account information and said one-time use cryptogram number(s) to produce the complete combined device payment information; and,
[28.d]	wherein the one or more device processors are further operable to transmit said complete payment information in place of said user-selected payment account information in a device payment transaction; and,
[28.e]	wherein the one or more device processors are further operable to display at least a portion of said user-specific selected account information associated with said complete device payment information used during said transaction, via a user interface disposed of the device.
[29.a]	The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more processors to dynamically generate a one-time limited-use cryptogram number, via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority, and selected from a set of information known and stored at both said payment authorities, and on said device, including: a transaction sequence counter, a device account number, a device account expiration date, a device secret, a

Claim Element	Claim Language
	payment processing authority secret, a user information, a payment account information, a payment issuer information, a payment amount, transactional information; and,
[29.b]	wherein said one or more processors uses said one-time limited-use cryptogram number in place of at least a portion of an issuer's static payment information, in a payment transaction using said payment account; and,
[29.c]	wherein said payment authorities are operable to recognize from the transactional payment information, the correct set of user, device and account specific information to be cryptographically combined into an authority computed cryptogram, for comparing with device transmitted limited-use payment information; and,
[29.d]	wherein said payment processing authorities are operable to deny as invalid a transaction including a cryptogram not matching an authority computed cryptogram; and,
[29.e]	wherein said payment authorities are operable to approve as valid a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,
[29.f]	wherein said device is operable to receive an approval and a denial status of said transaction, from said payment authorities, and visually convey said transaction status in the user-interface on the display disposed of the device.
[30.a]	The electronic device of claim 25, further comprising a processor and a non-transitory, computer-readable medium storing computer executable instructions that when executed by the one or more processors, cause the one or more device processors to dynamically generate a one-time limited-use cryptogram number by a cryptographic combination, of at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic device, and selected from a set of information including: a transaction sequence counter; a user payment account number; a device

Claim Element	Claim Language
	payment account number; a device secret; device keys; a payment issuer original account information; a payment issuer device account information; a payment processing authority secret; a transaction information; and a user private information; and,
[30.b]	wherein said cryptogram is operable to be used in place of at least a portion of an issuer's static payment information, in a payment transaction for said selected payment account; and,
[30.c]	wherein said payment processing authority is operable to deny as invalid, a transaction including a cryptogram not matching a payment processing authority computed cryptogram; and,
[30.d]	wherein said payment processing authority is operable to approve as valid, a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,
[30.e]	wherein said user device is operable to receive an approval and a denial status of said transaction information validation, and visually convey said transaction status in the user-interface on the display disposed of the device; and,
[30.f]	wherein said user device is operable to emulate the behavior of an issuer account payment transaction, when said complete device payment information is used in electronic payment facilities.

Samsung Electronics Co., Ltd. ("Petitioner" or "Samsung") petitions for *Inter Partes* Review ("IPR") of claims 1-21, 23-30 ("the Challenged Claims") of U.S. Patent No. 11,176,538 ("the '538 Patent").

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the '538 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	**1-18**	Royyuru-Phillips-Casey
1B	**5-6, 8-11, 13-17**	Royyuru-Phillips-Casey-Rans
2A	**19-21, 23-25, 28-30**	Phillips-Royyuru-Casey
2B	**23, 28-30**	Phillips-Royyuru-Casey-Rans
2C	**27**	Phillips-Royyuru-Casey-Rans-Carlson
2D	**26**	Phillips-Royyuru-Casey-Law

The '538 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
Rans	12/22/2006	12/06/2007
Carlson	06/24/2008	12/25/2008
Law	12/13/2011	06/14/2012

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

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 '538 PATENT

A. Brief Description

The '538 patent describes an electronic payment card that generates a "limited-duration number" for use in a payment transaction. SAMSUNG-1001, 2:20-29, 2:49-62, 10:22-12:15, FIG. 7; SAMSUNG-1003, ¶¶28-31. Figure 7 shows the process:

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

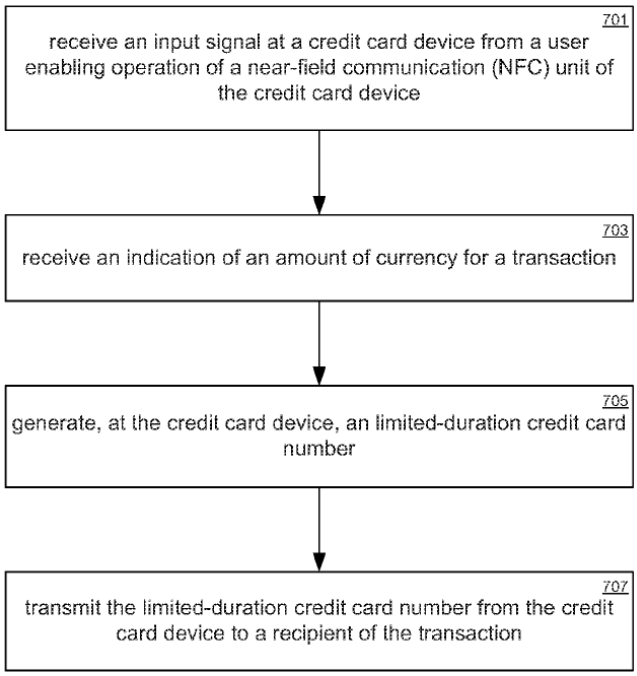


FIG. 7

SAMSUNG-1001, FIG. 7.

The limited duration number is generated "according to the user's private information, a bank information, information regarding the facility performing the transaction, and the time of day." *Id.*, 10:33-39. Further, the "limited-duration credit card number is able to be limited to only one transaction, a finite number of transactions." *Id.*, 10:39-44.

B. Level of Ordinary Skill in the Art

A person of ordinary skill as of the Critical Date ("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. SAMSUNG-1003, ¶¶45-51. Additional education could substitute for professional experience, or vice versa. *Id*.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1A] – Obviousness based on Royyuru-Phillips-Casey (Claims 1-18)

1. Royyuru[3]

Royyuru describes a system for conducting contactless financial transactions between a smartphone or other device, and a Point-of-Sale (POS) device. SAMSUNG-1004, [0034]-[0035], [0047]; SAMSUNG-1003, ¶¶80-85. The user device generates "a set of dynamic cryptograms that are valid for a single transaction" including a "Dynamic Transaction Cryptogram (DTC)" and a "dynamic PAN" using various information stored on or received by the device. SAMSUNG-1004, [0005]-[0010], [0032]-[0034], [0047]-[0048], [0051], [0057]. A Payment processor or issuer authenticates the transaction "based on the DTC" and determines the real PAN to process the transaction. *Id.* FIG. 3 shows the communication flow of the system:

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

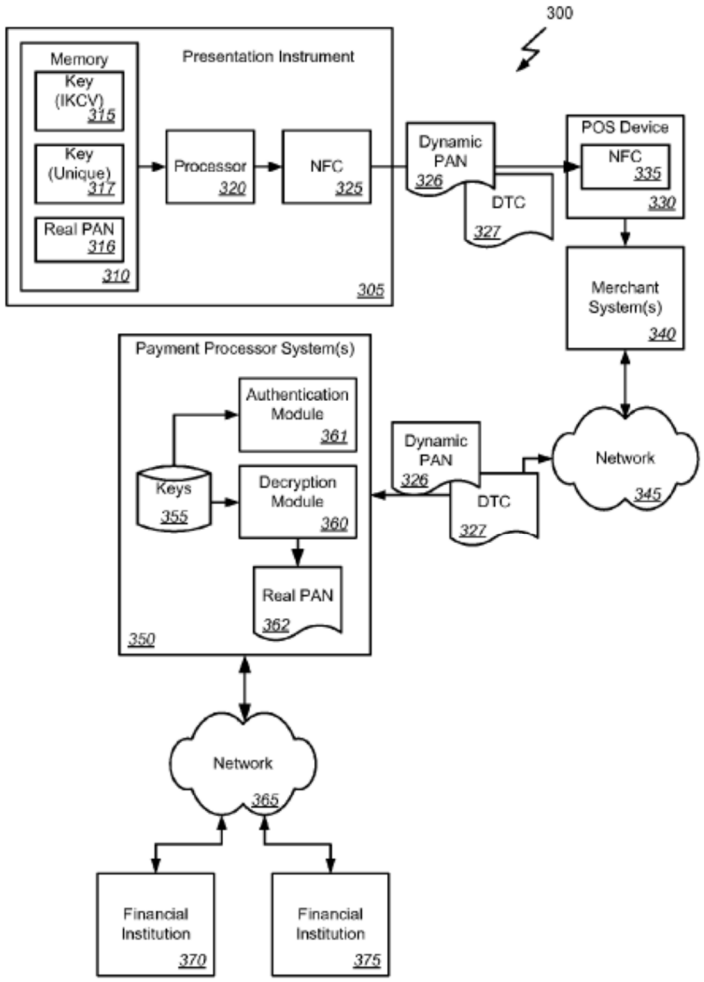


FIG. 3

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]; SAMSUNG-1003, ¶¶86-90.

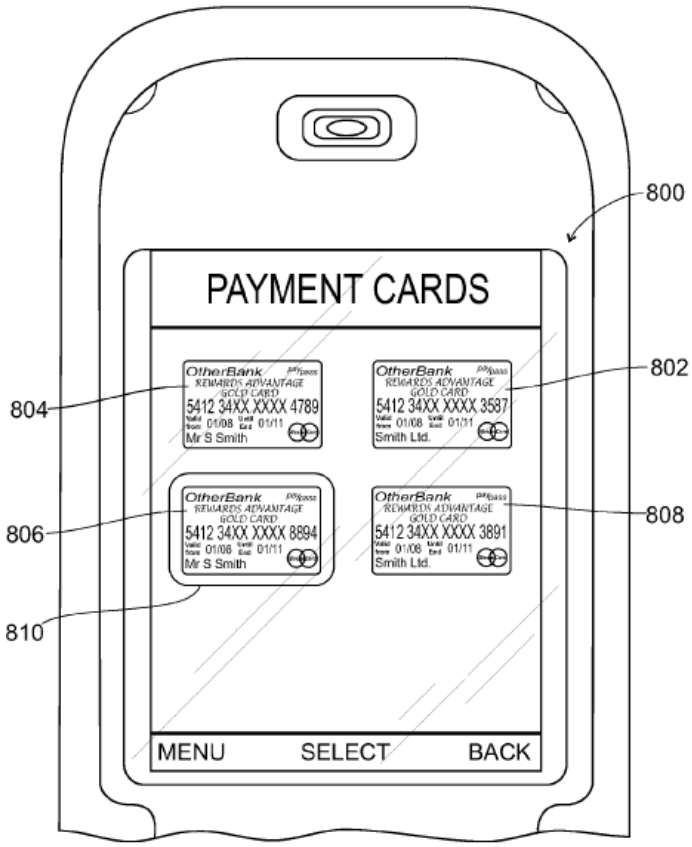


FIG. 8

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)," such as through "interrogation signals," to initiate the

card selection and payment transaction functions. SAMSUNG-1005, [0072], [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." SAMSUNG-1006, Abstract; SAMSUNG-1003, ¶¶91-95. 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:

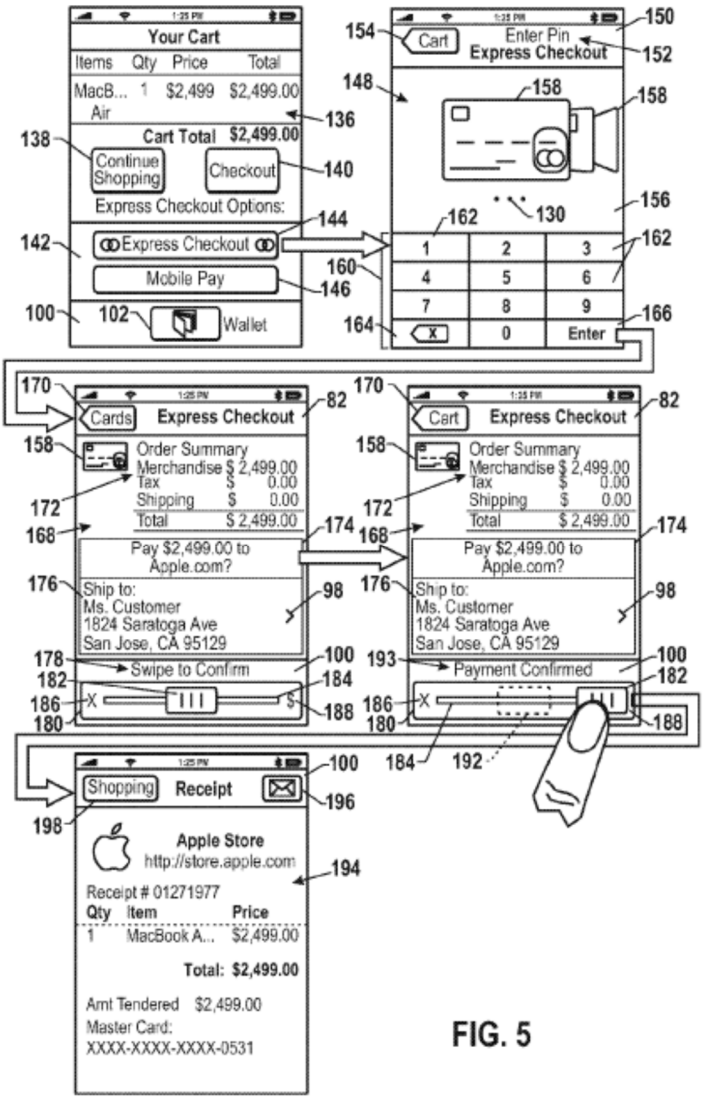


FIG. 5

After confirmation of the payment information by the payment processor, "the device 10 may receive and display (block 78) a receipt for the payment transaction." SAMSUNG-1006, 10:47-53, 10:20-29, 16:3-20.

4. Royyuru-Phillips-Casey Combination

A POSITA would have beneficially applied 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, ¶¶108-115.

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, ¶¶110-111. 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:

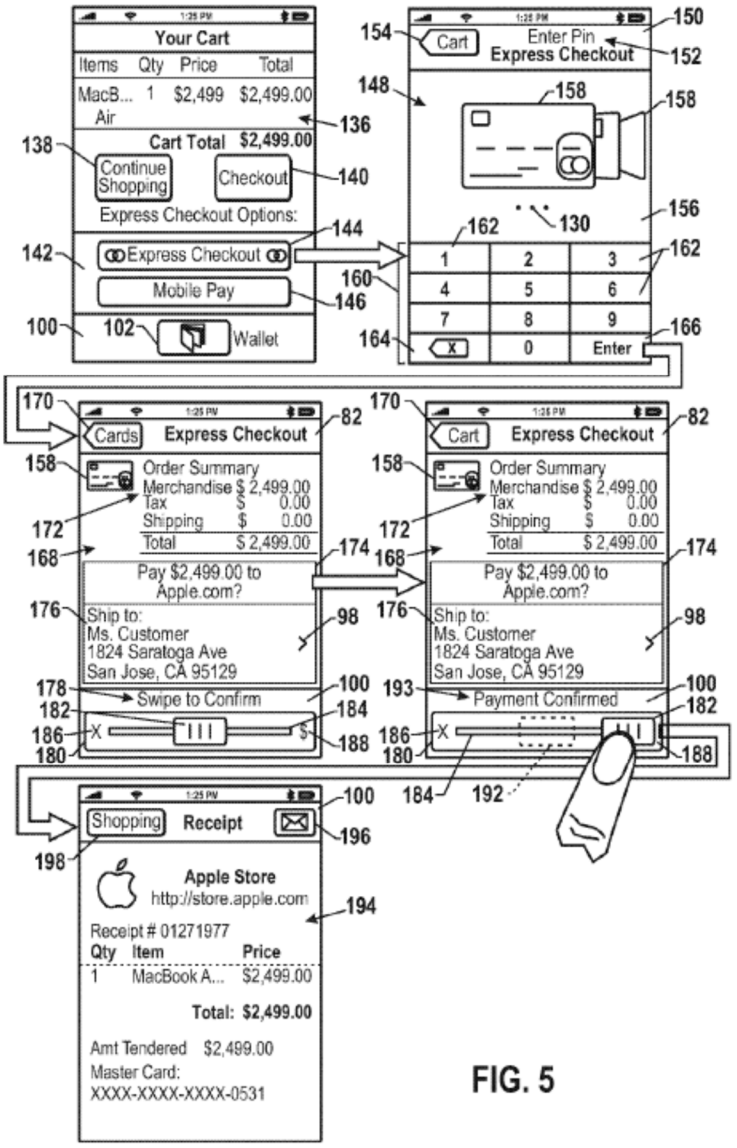


FIG. 5

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, ¶111. Such a modifica-

tion 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. *Id*. Such a modification would also allow the user to visually review transaction data before approving the transaction. SAMSUNG-1003, ¶111; 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, ¶111.

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, ¶112; 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, ¶112. 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); and
- avoiding unintended activation of a payment application and/or transmission of payment information.

SAMSUNG-1003, ¶112; 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:

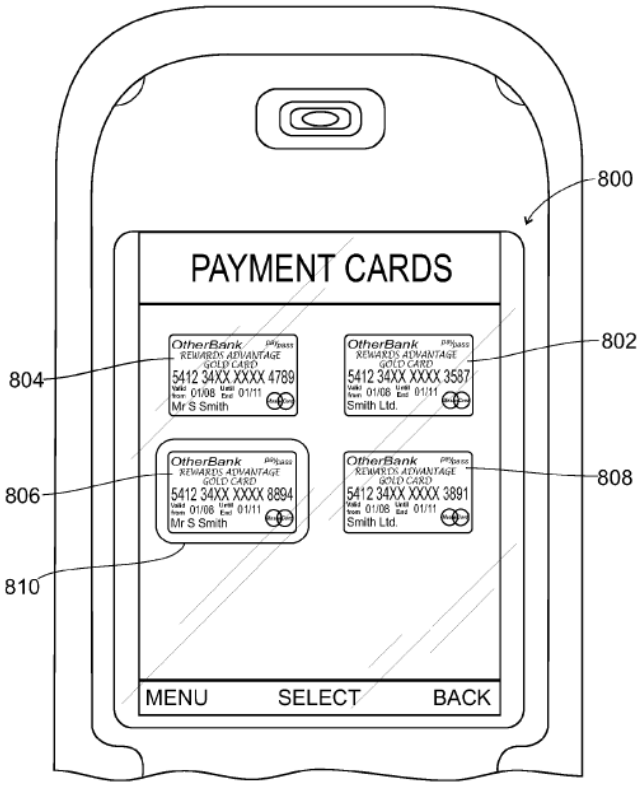


FIG. 8

SAMSUNG-1003, ¶113; 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 options with respect to how the user spent their money while allowing for the most appropriate selection for a given scenario (e.g., due to budgeting or credit card rewards considerations), and reducing or eliminating the need for the user to carry additional physical payment options. SAMSUNG-1003, ¶113. 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 while providing assurances of correct card

selection. SAMSUNG-1003, ¶113. 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 card information. *Id.*

Fourth, 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, ¶114. 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. *Id*. 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, ¶114.

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, ¶¶115, 109; *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, ¶¶115, 109. A POSITA would have furthermore had a reasonable expectation of success in modifying Royyuru's system 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, ¶116.

[1.a]

Royyuru describes tapping the user device near the POS terminal to prime/initiate the device for a transaction. SAMSUNG-1004, [0047], [0005], [0044], [0050], [0053]; SAMSUNG-1003, ¶¶117-118. 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 authorized. SAMSUNG-1003, ¶118; SAMSUNG-1005, [0035], [0038].

[1.b]

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, ¶¶119-120, 62-65. Phillips discloses that the user "enter[s] his/her personal identification number (PIN)" using the touchscreen to authorize the user. SAMSUNG-1005, [0020], [0035]; *see also* SAMSUNG-1006, 9:37-52.

[1.c]

The resulting device uses an "NFC module" for "close proximity…short range communications between [the] mobile device and [the] POS device." SAMSUNG-1004, [0051], [0022], [0044], [0046]-[0047], [0002]; SAMSUNG-1005, [0023], [0009]. Phillips discloses that the resulting device receives "a payment request" such as through NFC "interrogation signals" from a POS terminal. SAMSUNG-1005, [0072], [0023], [0027], [0057]; SAMSUNG-1006 8:52-9:8; FIGs. 5-8; SAMSUNG-1003, ¶¶121, 57-61.

[1.d]

Casey discloses that the resulting device displays the request, including "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. This information

is received through the "NFC device" as "a ***request*** for payment." SAMSUNG-1006 8:52-9:8; SAMSUNG-1003, ¶¶122-124. FIG. 8 shows an example display of request information on the device:

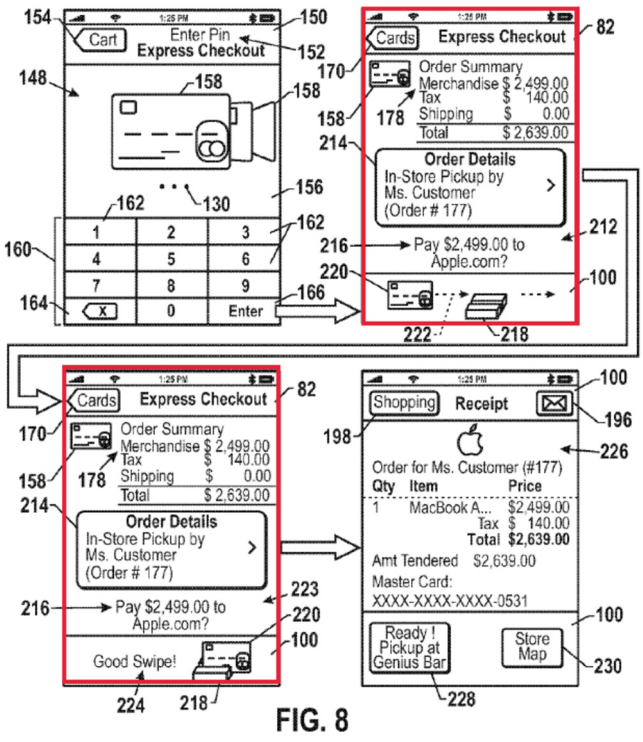


FIG. 8

SAMSUNG-1006, FIG. 8; *see also* FIGs. 5-7; SAMSUNG-1003, ¶122.

Additionally, Philips describes that the resulting device includes 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], [0057]; SAMSUNG-1003, ¶¶123-124.

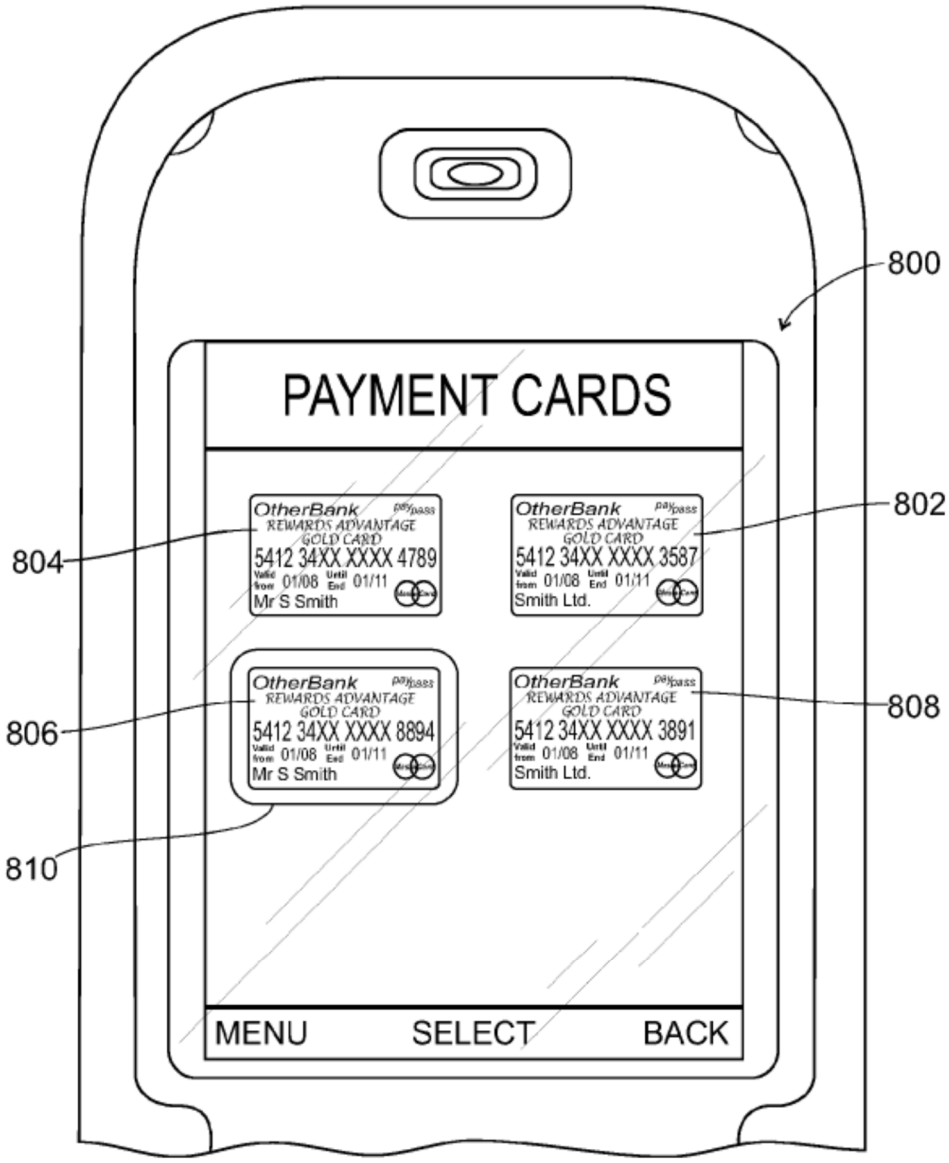


FIG. 8

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 infor-

mation such as the payment card account number [and] issuer bank name." SAMSUNG-1005, [0039], [0036]. As shown in FIG. 8, each displayed card includes at least a portion of an original static issuer-supplied payment account information. *Id.*, FIGs. 8, 11; *see also*, SAMSUNG-1004, [0032]; SAMSUNG-1003, ¶¶123-124.

[1.e]

The device of the predictable combination includes "a processor…and a memory communicatively coupled with and readable by the processor." SAMSUNG-1004, [0007], [0046], [0051]. Royyuru discloses the device-specific static limited-use payment information in the form of the "Institution Key Card Variant (IKCV) ***stored on the device***." SAMSUNG-1004, [0005]; SAMSUNG-1003, ¶¶125, 66-71. The IKCV is retrieved from memory for use in generating both the "Dynamic Transaction Cryptogram (DTC)" and dynamic PAN taught by Royyuru. SAMSUNG-1004, [0005]-[0010], [0057]. The "IKCV ***of the device***" is static and device specific in that it 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" and is therefore associated with a selected payment information. SAMSUNG-1004, [0055]-[0057], [0046], [0033]. The IKCV is limited in use to payments conducted with the device and with the associated card. *Id.*; SAMSUNG-1003, ¶125.

[1.f]

Royyuru provides at least two examples of the claimed "device-specific limited-use payment information": the "Dynamic Transaction Cryptogram (DTC)" and the "dynamic PAN." SAMSUNG-1004, [0005]-[0010], [0032]-[0033], [0047]; SAMSUNG-1003, ¶¶126-127, 55-56. The DTC "can be ***generated at the device***, using a unique card level key stored on the device." SAMSUNG-1004, [0005]. The IKCV provides an example of a "card-level key[] of the device." *Id.*, [0006]. 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 (card-level key) "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, ¶126. Because the PAN and expiration date are used to generate the DTC, it is payment information for the selected payment method. SAMSUNG-1003, ¶126; SAMSUNG-1004, [0057].

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].

[1.g]

The dynamic pan or "Pseudo-PAN can be sent in place of the real PAN." SAMSUNG-1004, [0057], [0007] (describing the issuer supplied "Primary Account Number (PAN)"), [0032] ("This dynamic PAN can then be used in the transaction instead of the real PAN"); SAMSUNG-1003, ¶¶128-129. 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], [0034]. As discussed above (Element [1.f]), the DTC and dynamic PAN are generated using the IKCV and/or CK.

[1.h]

As described above (Element [1.f]), the IKCV (static limited-use payment information) makes up part of the DTC. SAMSUNG-1004, [0057], [0005]-[0009]. Furthermore, the DTC and dynamic PAN (dynamic payment information) are provided together, along with additional information such as the ATC and cardholder

name, to the POS device and payment processor, which a POSITA would have recognized as combining the DTC and dynamic PAN (and additional information) to generate a complete device payment information. SAMSUNG-1004, [0006]-[0010], [0034], [0050], [0057]; SAMSUNG-1003, ¶¶130-131. Furthermore, because the IKCV makes up part of the DTC, a POSITA would have recognized that the IKCV is combined with the dynamic PAN as part of forming Royyuru's complete device payment information. SAMSUNG-1003, ¶130.

Alternatively, the dynamic PAN is also generated using the IKCV. *Supra*, [1.f]; SAMSUNG-1004, [0005], [0057]. In this alternative example, the DTC represents the dynamic information and, because the IKCV makes up part of the dynamic PAN, a POSITA would have recognized that the IKCV is combined with the DTC as part of forming Royyuru's complete device payment information. SAMSUNG-1003, ¶131.

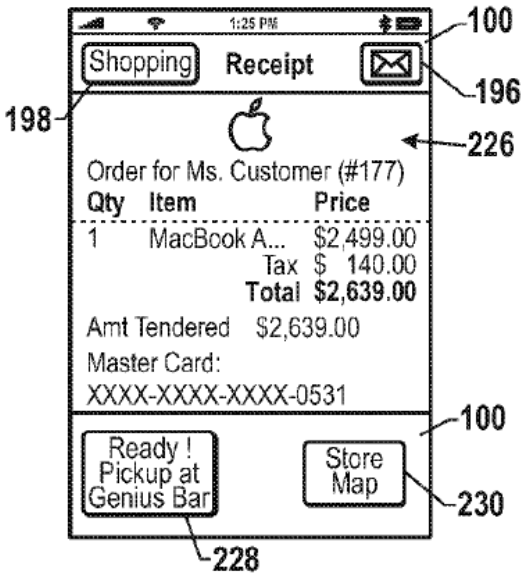
[1.i]

Royyuru describes "providing the DTC and dynamic PAN to a Point-of-Sale (POS) device" for "use in the transaction." SAMSUNG-1004, [0006]. This is conducted "via the NFC module 325 of the presentation instrument and corresponding NFC module 335 of the POS device 330." *Id.*, [0047], [0022], [0051], [0002], [0044]; SAMSUNG-1003, ¶132. The DTC and dynamic PAN are then "submitted

to the payment processor system…for approval and/or processing of the transaction." SAMSUNG-1004, [0047].

[1.j]-[1.k]

As described by Casey, in the Royyuru-Phillips-Casey combination, "***[a]fter the payment transaction has been confirmed***, the device 10 may ***receive and display*** (block 78) ***a receipt for the payment transaction***" including a payment amount. SAMSUNG-1006, 10:47-53, *see also* 10:20-29, 16:3-20; SAMSUNG-1003, ¶¶133-136. FIG. 8 shows the receipt screen showing the completed status of the transaction:



SAMSUNG-1006, FIG. 8.

Royyuru discloses that in the predictable combination, the transaction is completed dependent on validation of complete device payment information (DTC

and dynamic PAN) by a payment processor authority and a payment issuer authority and therefore the transaction status conveyed in the receipt is dependent on this validation. SAMSUNG-1004, [0006], [0034], [0047]-[0048], [0052], [0010], [0044], [0050], [0055]; SAMSUNG-1003, ¶¶133-134.

Royyuru describes "[t]he transaction can be authenticated at the payment processor system or at the financial institution based on the DTC." SAMSUNG-1004, [0006]. Specifically the dynamic PAN and DTC are "***submitted to the payment processor system 350 and/or financial institution***…for approval and/or processing of the transaction." SAMSUNG-1004, [0047]. In another example, DTC validation occurs at "the payment processor system or the financial institution" and the dynamic PAN is decrypted at the payment processor. SAMSUNG-1004, [0006]. A POSITA would have recognized that deciphering the real PAN at the payment processor and authenticating the DTC at the financial institution provides, or at least renders obvious, validation of the transmitted complete device payment information by a payment processor authority and a payment issuer authority. SAMSUNG-1003, ¶134.

In another example, "[t]he ***payment processor*** system can be adapted to ***authenticate the transaction based on determining the real PAN*** of the financial account based on the dynamic PAN and validating the DTC," upon which the pay-

ment processor "submit[s] the real PAN to a financial institution to affect processing of the transaction." SAMSUNG-1004, [0010]. "***[T]he payment processor system*** 350 can request approval of the transaction ***via one or more of the financial institutions***" using the DTC and dynamic PAN. SAMSUNG-1004, [0044], [0050]. As discussed above, after authorization, the payment authorization status is conveyed in the form of a receipt displayed on the user device, as disclosed by Casey. SAMSUNG-1006, 10:47-53, 10:20-29, 16:3-20, FIGs. 5, 8; SAMSUNG-1003, ¶135.

[2]

The resulting device communicates with the POS device using NFC. SAMSUNG-1004, [0002], [0051], [0022]; SAMSUNG-1006, 5:57-62, 6:58-59, 17:31-42. "After the payment transaction ***has been confirmed*** the device 10 may receive and display (block 78) a receipt for the payment transaction." SAMSUNG-1006, 10:47-53. Because "[t]he NFC interface" of the device of the resulting combination is "used to receive information," including information from the POS terminal, a POSITA would have recognized that the Royyuru-Phillips-Casey combination provides that the confirmation receipt is received via NFC from the payment reader facility. SAMSUNG-1004, [0002]; SAMSUNG-1006, 6:58-59, 5:57-62; SAMSUNG-1003, ¶¶137-140. A POSITA would have recognized that confirmation of the transaction provides that the payment processor and issuer authority validated

the complete device payment information (*supra*, Element [1.j]). SAMSUNG-1003, ¶139.

[3]

Supra, Element [1.c], [1.j], Claim [2]; SAMSUNG-1003, ¶¶141-143.

[4]

Royyuru's DTC and dynamic PAN each individually provide this element. SAMSUNG-1003, ¶¶144-147. In the predictable combination, both the DTC and dynamic PAN are "computed by the device" using the real PAN of the selected payment method and therefore both are limited-in-use to the selected issuer payment method. SAMSUNG-1004, [0057], [0005]-[0009]; SAMSUNG-1003, ¶145. The DTC and dynamic PAN are generated by the device using CKs/IKCV that are specific to the device and therefore limited-in-use to payment transactions performed by the device. *Supra*, [1.e]; SAMSUNG-1004, [0005]-[0010], [0055]-[0057]; SAMSUNG-1003, ¶¶145, 125. The DTC and dynamic PAN are "sent in place of the real PAN" in transactions. *Supra*, [1.g]; SAMSUNG-1004, [0057], [0032]-[0034], [0006]-[0010]; SAMSUNG-1003, ¶¶145, 128-129.

The payment processor or issuer uses the DTC to validate the transaction and the dynamic PAN is used to determine the real PAN for processing the transaction. SAMSUNG-1004, [0006], [0034], [0039], [0048], [0055], [0050]. The payment processor will "decline the transaction if the DTC is incorrect." *Id.*, [0057].

In some examples, the real PAN is determined from the dynamic PAN and the real PAN is then used to validate the DTC. *Id.*, [0039], [0055]. A POSITA would therefore have recognized that if either of the DTC or dynamic PAN is invalid, the received combined payment information is rejected as invalid by the payment processor or issuer. SAMSUNG-1003, ¶146.

[5.a]

"The 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]. The PAN and expiration date provide payment processing authority recognizable information. SAMSUNG-1003, ¶¶148-150. The ATC is an "Application Transaction Counter" which "increments for each transaction" and therefore provides the claimed device transaction sequence counter. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶¶149, 72-75. The CK is "unique per card" and therefore provides device-unique information. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶149. The "Institution Key Card Variant (IKCV)" can serve as the card-level key or "CK." SAMSUNG-1004, [0005]-[0006]. The IKCV is "generated when each card (device) is being customized" using a "Device Sequence number" and is therefore both a device account number and device unique information. SAMSUNG-1004

[0057], [0046], [0091]-[0096]; SAMSUNG-1003, ¶149. The unpredictable number can be any number generated "or ***received by the presentation instrument*** 305" and therefore provides any device-unique information calculated or received by the device such as a PIN. SAMSUNG-1004, [0051]; SAMSUNG-1003, ¶149.

The dynamic PAN can be similarly generated using the real PAN, ATC, unpredictable number, and IKCV. SAMSUNG-1004, [0057], [0005]-[0009]. As discussed above, the unpredictable number can be almost any information available to the device and therefore the dynamic PAN also provides this element. SAMSUNG-1004, [0051]; SAMSUNG-1003, ¶150.

[5.b]

Royyuru's "dynamic cryptograms…are ***valid for a single transaction***." SAMSUNG-1004, [0005], [0033], [0047], [0053], [0057], Abstract. This is because the ATC, which "increments for each transaction," is used to generate the DTC and dynamic PAN. *Id.*, [0057], [0084]; SAMSUNG-1003, ¶151. As previously discussed, the DTC and dynamic PAN are used to authorize/validate the transaction in place of the real PAN. *Supra*, [1.g], [1.j]; SAMSUNG-1004, [0047], [0044], [0057], [0032]-[0034], [0006]-[0010].

[5.c]

The transaction is authenticated "based on the DTC" by payment processor or issuer "validating the DTC." SAMSUNG-1004, [0006], [0034], [0048]; *supra* Element [1.j]. A POSITA would have recognized that it would have been obvious for the payment processor to validate the DTC by generating a comparison DTC value and then comparing the comparison DTC value to the received DTC. SAMSUNG-1003, ¶152. The ATC and other information, such as the PAN and expiration date that are used to generate the DTC, are known to the payment processor and therefore a POSITA would have found it obvious to use these values to recreate the DTC to authenticate the received DTC. SAMSUNG-1004, [0057], [0046], [0090]-[0096]; SAMSUNG-1003, ¶152.

[5.d]

The "most recent ATC" is received and stored "by the payment processor." SAMSUNG-1004, [0057]. The payment processor generates the IKCV based on the PAN and expiration date so these values are known to the payment processor. SAMSUNG-1004, [0057], [0046], [0091]-[0096], [0033], [0055]. The Card-Key (CK) is "system-generated by payment processor" and therefore is also known to the payment processor. SAMSUNG-1004, [0057]. These values provide the claimed values used to generate the DTC. *Supra*, Element [5.a]; SAMSUNG-1003, ¶¶153, 149-150. A POSITA would have found it obvious to use these values to

recreate the DTC to authenticate the received DTC. *Supra*, Element [5.c]; SAMSUNG-1003, ¶153.

[5.e]

The ATC is "a counter which increments for each transaction (message) generated by the card (device)." SAMSUNG-1004, [0057].

[5.f]

Supra, Elements [1.g], [1.j], [5.b]-[5.c]; SAMSUNG-1003, ¶¶155-156.

[6.a]

Supra, Element [5.a]. Furthermore, in at least some examples, the IKCV and other CKs are generated by the payment processor and therefore provide the claimed payment processing authority specific information. SAMSUNG-1004, [0057], [0046], [0091]-[0096]; SAMSUNG-1003, ¶¶157-158. The unpredictable number can also be any number specific to the payment processor known to the device, including the member number. SAMSUNG-1004, [0057], [0051], [0091]-[0096]; SAMSUNG-1003, ¶158.

[6.b]-[6.c]

Supra, Elements [5.c]-[5.d], [5.f], [1.g], [1.j].

[6.d]-[6.e]

The transaction is authorized or denied by the payment processor and/or issuer based on the DTC and dynamic PAN. *Supra*, [1.j]; SAMSUNG-1004, [0006],

[0047], [0044], [0050]; SAMSUNG-1003, ¶¶160-161. The payment processor validates the transaction using the DTC and dynamic PAN and then "submit[s] the real PAN to a financial institution to affect processing of the transaction." SAMSUNG-1004, [0010]. The payment processor "return[s] an approval or denial response" to the POS. SAMSUNG-1004, [0044]. As previously discussed, Casey discloses that in the predictable combination the approval or denial is returned to the user device from the POS terminal for display. SAMSUNG-1006, 10:20-53, 16:3-20, FIGs. 5-8; SAMSUNG-1003, ¶160.

[7]

Supra, Element [1.k]; SAMSUNG-1006, 10:20-53, 16:3-20, FIGs. 5, 8 (showing at least a confirmation result, payment amount, merchant information, and payment completion status); SAMSUNG-1003, ¶¶162-164.

[8.a]

The "IKCV ***of the device***" is a device-specific account number that is "generated when each card (device) is being customized." *Supra*, Element [1.e]; SAMSUNG-1004, [0055]-[0057], [0046], [0033], [0091]-[0096] (the IKCV is generated based on a "Device Sequence number"); SAMSUNG-1003, ¶¶165-166. The IKCV is a CK and is used in generating both the DTC and dynamic PAN. *Supra*, Elements [1.j], [5.a]; SAMSUNG-1004, [0057], [0005]-[0006].

[8.b]

The DTC and dynamic PAN are generated using the ATC, which is a device-internal transaction sequence counter count. *Supra*, [5.a]; SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶167.

[8.c]

The IKCV is generated when customizing the device and is therefore specific to the device. SAMSUNG-1004, [0055]-[0057], [0046]; SAMSUNG-1003, ¶168. The IKCV is generated using a member number and is therefore unique to the user. SAMSUNG-1004, [0091]-[0096]; SAMSUNG-1003, ¶168. Royyuru describes generating the dynamic PAN and DTC using the IKCV and transmitting the dynamic PAN, DTC, and ATC to the POS terminal, but not the IKCV. SAMSUNG-1004, [0006], [0047], [0022], [0051]-[0057]. The UN (undeterminable number), PIN, and/or customer name are all unique to the user and the device because the device is unique to the user. SAMSUNG-1003, ¶168; SAMSUNG-1004, [0047], [0051], [0053]. Royyuru discloses to a POSITA that any information known to (generated or received by) the device can be used in generating the dynamic PAN and DTC and therefore the PIN, user name, and/or UN can be used in generating these cryptograms, but are not passed to the POS terminal. SAMSUNG-1004, [0051], [0057]; SAMSUNG-1003, ¶168.

[8.d]

The IKCV (used in generating both the DTC and dynamic PAN) is supplied by the payment processor system. SAMSUNG-1004, [0046], [0057], [0091]-[0096]. The real PAN is also information supplied by the payment processor used in generating the DTC and dynamic PAN that is not passed in the transaction. SAMSUNG-1004, [0057], [0007], [0051]; SAMSUNG-1003, ¶¶169-170.

Both the DTC and dynamic PAN are "sent in place of the real PAN" and are needed to authorize and process the transaction. Therefore a POSITA would have recognized that the complete device payment information is only valid for use in place of an issuer payment method in authorized payments that comprise all valid device generated limited-use information elements. *Supra*, [1.g]-[1.j], [4]; SAMSUNG-1004, [0006], [0047], [0010], [0044], [0050], [0057]; SAMSUNG-1003, ¶¶169-170,

[8.e]

The DTC and dynamic PAN for the selected payment method are unique-per-device because they are generated using the ATC, card-level keys, and "IKCV of the device" that are all unique to the device. SAMSUNG-1004, [0055]-[0057], [0006]; SAMSUNG-1003, ¶¶171-172. Furthermore, these "dynamic cryptograms…are ***valid for a single transaction***." SAMSUNG-1004, [0005], [0033], [0047], [0053], [0057], Abstract. As described with respect to Elements [5.a],

[6.a], and [8.a]-[8.d], *supra*, each of the listed information elements is combined to generate both the dynamic PAN and the DTC. SAMSUNG-1003, ¶171.

[9]

Both the DTC and dynamic PAN are singular "dynamic cryptogram[]" numbers generated by combining the above described information. *Supra*, [1.f], [4], [5.a], [8.a]-[8.c]; SAMSUNG-1004, [0005], [0053], [0047], [0051]-[0057]; SAMSUNG-1003, ¶¶173-175. Each of the DTC and dynamic PAN makes up a part of the transmitted device transaction information. SAMSUNG-1004, [0006], [0047], [0022], [0051], [0044]; SAMSUNG-1003, ¶174. These functions are performed by a processor of the device. SAMSUNG-1004, [0007].

[10]

The IKCV and other CKs are specific to the device and provided by the payment processor/issuer and therefore are device keys and payment issuer secrets while the real PAN and UN are also payment issuer secrets. SAMSUNG-1004, [0055]-[0057], [0006], [0046], [0091]-[0096], [0057], [0004] (***securely*** handling a financial transaction); SAMSUNG-1003, ¶¶176-178. The IKCV, CKs, real PAN, and UNs are used in generating the DTC and dynamic PAN. SAMSUNG-1004, [0057], [0051], [0006]-[0009].

[11]

Supra, Elements [5.a], [5.d], [6.a]. The ATC is a device sequence counter used in generating the DTC and dynamic PAN. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶¶179-181. The IKCV and CKs are generated by the payment processor and are therefore payment processing authority-specific information. SAMSUNG-1004, [0055]-[0057], [0006], [0046], [0091]-[0096], [0057]; SAMSUNG-1003, ¶180. The real PAN is issuer specific information. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶180.

[12]

"The dynamic PAN can also be based on an undeterminable number generated or received by the device." SAMSUNG-1004, [0005], [0057], [0051], [0032] (dynamic PAN is generated using "one or more ***factors from the payment device or the POS reader***."), [0047], [0022] (NFC used to communicate with POS device). The DTC is also calculated using a UN received from the POS device via NFC. SAMSUNG-1004, [0057], [0051]. Royyuru identifies the terms "unpredictable number" and "undeterminable number" as interchangeable. *Id.*; SAMSUNG-1003, ¶¶182-184.

[13]

"The device can use the UN in both dynamic PAN and DTC calculations." SAMSUNG-1004, [0057], [0051]; SAMSUNG-1003, ¶¶185-190. The UN can be

any information received from the POS device. *Id.* In another example, the dynamic PAN is generated using "one or more ***factors from the payment device or the POS reader***." *Id.*, [0032], [0047].

As shown in Casey FIGs. 6-8, UNs/information received by the resulting device from the POS includes "recipient identifier" or "merchant information" which, as taught by Royyuru, would be used in generating the dynamic PAN and DTC in some embodiments. SAMSUNG-1006, 3:26-37, 10:20-35, *see also* SAMSUNG-1005, [0072] (receiving "merchant ID"), [0027], [0048]-[0050], [0057], [0064]. ; SAMSUNG-1003, ¶188.

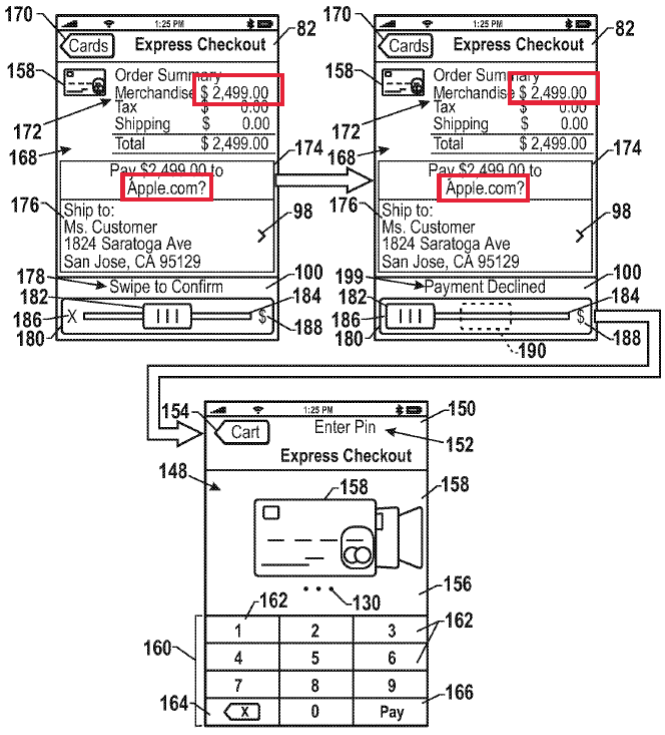


FIG. 6

SAMSUNG-1006, FIG. 6.

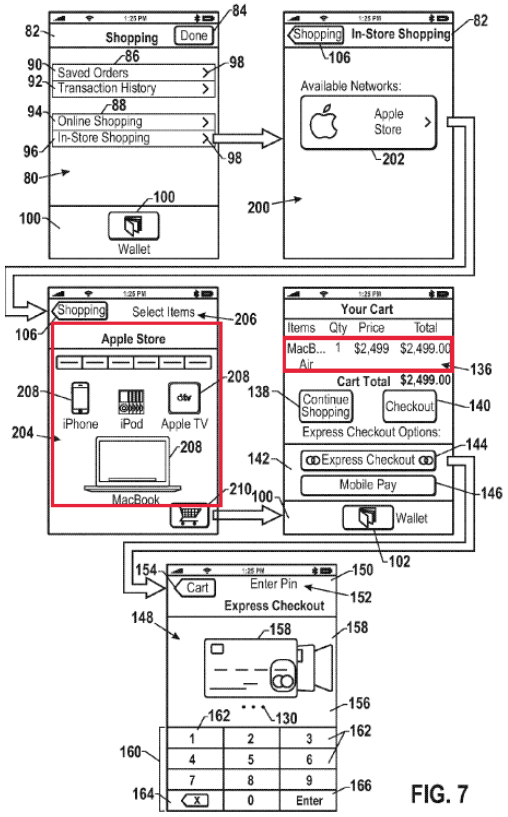


FIG. 7

SAMSUNG-1006, FIG. 7.

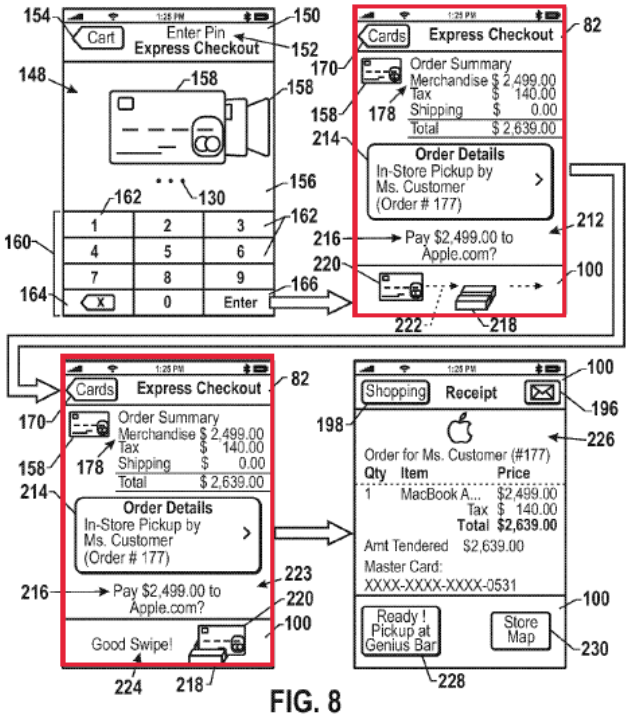


FIG. 8

SAMSUNG-1006, FIG. 8.

[14]

See Supra, Claims [12]-[13]. Furthermore, the merchant/recipient identifiers and "data identifying the merchant store" described by Casey and Phillips provide the claimed transaction facility information used as "one or more factors" in generating the DTC and dynamic PAN. SAMSUNG-1004, [0051], [0032]; SAMSUNG-1006, 3:26-37, 10:20-35; SAMSUNG-1005, [0072], [0027], [0048] ("wireless signal that identifies the location or store"), [0057], [0064]; SAMSUNG-1003, ¶¶191-193.

[15]

"The device can use the UN" or "one or more factors from the…POS reader" "in both dynamic PAN and DTC calculations." SAMSUNG-1004, [0057], [0051], [0032], [0047]; SAMSUNG-1003, ¶¶194-198; *supra,* Claims [12]-[13].

In the predictable combination such numbers/factors include a "payment amount." SAMSUNG-1006, 3:26-37, 10:20-35, 12:19-22, 13:36-39, FIGs. 5-8; SAMSUNG-1005, [0045]; SAMSUNG-1003, ¶197.

[16]

"The device can use the UN" or "one or more factors from the…POS reader" "in both dynamic PAN and DTC calculations." SAMSUNG-1004, [0057], [0051], [0032], [0047]; SAMSUNG-1003, ¶¶199-205; *supra,* Claims [12]-[13].

In the predictable combination these "factors" include a payment facility type. SAMSUNG-1003, ¶¶202-204. For example, "[t]he mobile telephone may 'recognize' that it is in a 'Sears™' retail store." SAMSUNG-1005, [0048]. Phillips also describes the device recognizing facility types "such as 'Candy Store', 'Supermarket', 'Convenience Store', 'Deli', and the like." *Id.*, [0046], [0049]-[0050].

[17]

"The device can use the UN" or "one or more factors from the…POS reader" "in both dynamic PAN and DTC calculations." SAMSUNG-1004, [0057], [0051], [0032], [0047]; SAMSUNG-1003, ¶¶206-210; *supra,* Claims [12]-[13].

In the predictable combination, in the context of on-line transactions, these "factors" include "an ***on-line*** merchant identifier or the like." SAMSUNG-1005, [0049], *see also* [0071], [0073], [0082]; SAMSUNG-1006, 3:14-19, 8:23-31, 11:50-60; SAMSUNG-1003, ¶¶207-209. Any of the information discussed above (claims [12]-[16]), provides online transaction information in the context of online transactions (as taught by Phillips). SAMSUNG-1003, ¶209.

[18.a]

Supra Elements [5.a], [6.a], [8], [10]. Additionally, a POSITA would have recognized that both the dynamic PAN and DTC are used to validate the payment

transaction and are therefore utilized in place of a card validation value. *Supra*, Elements [1.g], [1.j], [4], [5.c]; SAMSUNG-1003, ¶¶211-212. To the extent that the term "in place of a card validation value" is interpreted narrowly, Royyuru describes that 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. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶212. Specifically, Royyuru describes that the DTC is part of the "Track 1" "verification information" that is conveyed 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, ¶212; *see, e.g.,* SAMSUNG-1005, [0059] (cryptogram provided in place of conventional payment issuer security code (CVC3)).

[18.b]

Both the DTC and dynamic PAN are generated using the ATC, which is an "Application Transaction Counter" which "increments for each transaction." SAMSUNG-1004, [0057], [0005], [0051]. Royyuru's "dynamic cryptograms…are ***valid for a single transaction***." SAMSUNG-1004, [0005], [0033], [0047], [0053],

[0057], Abstract. This is because the ATC, which "increments for each transaction," is used in generating the cryptograms. *Id.*, [0057], [0084]; SAMSUNG-1003, ¶213.

[18.c]

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. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶¶214-215. The DTC is provided as part of "Track 1" "verification information" in place of traditional card validation values (CVC). *Supra*, [18.a]; SAMSUNG-1004, [0049]; SAMSUNG-1005, [0059]; SAMSUNG-1003, ¶214.

B. [GROUND 1B] – Obviousness based on Royyuru-Phillips-Casey-Rans (Claims 5-6, 8-11, 13-17)

1. Rans

Rans describes processes for "generating authentication data" in a mobile payment system. SAMSUNG-1014, [0006]; SAMSUNG-1003, ¶¶102-104. The described techniques "allow[] for additional security in contactless chip device transactions" including "over the internet [or] at a merchant's location." SAMSUNG-1014, [0020], [0024]. The mobile device transmits "authentication data" including a "dynamic" value to an "authentication agent, or other entity involved in the transaction." *Id.* The authentication agent generates "second authentication

data…based on data held by the card issuer, authentication agent or other entity involved in the transaction" which is compared to the "authentication data" received from the mobile device to authenticate the user and process the transaction. *Id.*, [0022], [0037]-[0040]. "The issuer, authentication agent, or entity involved in the transaction can maintain data such as the PIN, the challenge, the unpredictable number, a synchronized transaction counter, or ***any other data that may be used to generate the second authentication data***." *Id.*, [0023].

2. Royyuru-Phillips-Casey-Rans Combination

A POSITA would have applied Rans to Royyuru such that the payment processor generates a comparison version of Royyuru's DTC to compare to the user device generated DTC to authenticate the transaction. SAMSUNG-1003, ¶¶216-218. Royyuru describes that the transaction is authenticated by the payment processor and/or issuer "***based on the DTC***." SAMSUNG-1004, [0006], [0047]. Rans provides additional details for authenticating such transaction information that readily complements Royyuru's disclosure. SAMSUNG-1003, ¶218. Rans describes generating a "dynamic value" using a "cryptographic key," similar to Royyuru's DTC, that is combined with other information to form complete "authentication data" which is then provided to a payment processor for authentication. *Id.*, [0039], [0042], [0020]-[0023]. Rans provides additional details missing from Royyuru regarding generating comparison authentication information at the

payment processor, which is then compared to the received authentication data. SAMSUNG-1014, [0020]-[0023], [0037]-[0039]. Therefore, a POSITA would have applied Rans to the Royyuru-Phillips-Casey combination to generate comparison versions of the DTC and/or dynamic PAN at the payment processor or issuer to process the transaction. SAMSUNG-1003, ¶218. Application of Rans to Royyuru-Phillips-Casey would have reduced "the possibility of fraud" and prevented hacking in the resulting system. SAMSUNG-1014, [0002], [0072]; SAMSUNG-1003, ¶218. A POSITA would have recognized that application of Rans to Royyuru-Phillips-Casey 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. Here, all of the references describe similar mobile payment transaction systems using payment information stored on or generated by a mobile device and Rans describes improvements that would have been beneficially applied to the resulting system. SAMSUNG-1003, ¶218.

3. Application of Royyuru-Phillips-Casey-Rans

[5]

As discussed in Ground 1A, *supra* Element [5.a], Royyuru discloses that both the DTC and dynamic PAN are generated using a device transaction sequence counter count (ATC), a device account number (IKCV), device-unique information

(CK, IKCV, UN, and payment processing authority recognizable information (real PAN, expiration date, IKCV, UN). SAMSUNG-1003, ¶¶219-222.

In the resulting combination, the transaction is authenticated "based on the DTC." SAMSUNG-1004, [0006], [0034], [0048]. With respect to elements [5.c], [5.d], and [5.f], as discussed above, a POSITA would have applied Rans to the Royyuru-Phillips-Casey combination to generate comparison versions of the DTC and/or dynamic PAN at the payment processor or issuer to compare to the received DTC and/or dynamic PAN generated by the user device. SAMSUNG-1003, ¶221. Rans describes generating "a second authentication data" at the "authentication agent or other entity involved in the transaction," which a POSITA would have recognized as being equivalent to the payment processor and issuer described by Royyuru. SAMSUNG-1014, [0022], [0037], SAMSUNG-1003, ¶221. "The second authentication data is then compared 270 with the first authentication data" to determine whether the generated and received authentication data "are equal" to "validate that the first authentication data was calculated or generated by an authorized card holder" and provide a positive or negative response. SAMSUNG-1014, [0037]-[0038]. Therefore, in the Royyuru-Phillips-Casey-Rans combination, the comparison includes determining if the DTC and/or dynamic PAN received from the user device match the DTC and/or dynamic PAN generated at the pay-

ment processor or issuer. SAMSUNG-1003, ¶221. Rans discloses that "[t]he issuer, authentication agent, or entity involved in the transaction can maintain data such as the PIN, the challenge, the unpredictable number, a synchronized transaction counter, ***or any other data that may be used to generate the second authentication data***" and use such data to generate the comparison authentication data (the DTC and/or dynamic PAN in the predictable combination. SAMSUNG-1014, [0022]-[0023], [0037]-[0039] ("any other piece of data" used to generate dynamic cryptogram), [0042]-[0043]. Therefore in the Royyuru-Phillips-Casey-Rans combination, all of the data disclosed by Royyuru as being used to generate the DTC and/or dynamic PAN is stored at the payment processor and/or issuer and used to generate the respective comparison cryptogram. SAMSUNG-1003, ¶221. All other elements of claim [5] are provided by the Royyuru-Phillips-Casey-Rans combination for the reasons discussed in Ground 1A, *supra*. SAMSUNG-1003, ¶221.

[6]

For the reasons discussed with respect to claim [5], *supra*, the Royyuru-Phillips-Casey-Rans combination performs the same secure combination of the same information as retained at the payment processing authority and compares the payment processor generated value to the received cryptogram to verify the received DTC and/or dynamic PAN such that "a positive 280 or negative 290 response can be provided there from." SAMSUNG-1003, ¶¶223-225; SAMSUNG-1014, [0020]-

[0024]; [0037]-[0039]. All other elements of claim [6] are provided by the Royyuru-Phillips-Casey-Rans combination for the reasons discussed in Ground 1A, *supra*. SAMSUNG-1003, ¶224.

Claims [8]-[11], [13]-[17]

To the extent that any of claims [8]-[11] and [13]-[17] are interpreted narrowly or Royyuru's disclosure of the unpredictable/undeterminable number or "one or more factors from the payment device or the POS reader" used to generate the DTC and dynamic pan are interpreted narrowly, Rans demonstrates that the Royyuru-Phillips-Casey-Rans combination provides claims [8]-[11] and [13]-[17]. As discussed in Ground 1A, *supra*, the Royyuru-Phillips-Casey combination provides that information stored/received at the user device includes merchant identifying information (Casey's "merchant information," name, website, and price; Phillips' "merchant ID" and "data identifying the merchant store"), transaction facility information (merchant/recipient identifiers and "data identifying the merchant store" described by Casey and Phillips), payment amount (disclosed by Casey), a payment facility type (Phillips disclosure of identifying store as retail, candy, supermarket, convenience, deli, etc.), and on-line transaction information (all of the above described information in Casey and Phillips' on-line implementa-

tions). SAMSUNG-1006, 3:14-37, 10:20-35, 8:23-31, 11:50-60, FIGs. 6-8; SAMSUNG-1005, [0072], [0027], [0048]-[0050], [0057], [0064], [0071], [0073], [0082]; SAMSUNG-1003, ¶¶226-227.

Rans discloses that the dynamic authentication data (applicable to Royyuru's DTC and dynamic PAN) can be generated using an undeterminable number or "secret value" generated from a "cryptographic key," "***a number or any other piece of data***." SAMSUNG-1014, [0039]; SAMSUNG-1003, ¶227. In another example, "the PIN, the challenge, the unpredictable number, a synchronized transaction counter, or ***any other data that may be used to generate the authentication data***" is used to verify the authentication data. SAMSUNG-10147, [0023]. This includes values "from a merchant, website, card issuer, or any other participant in the transaction." *Id.*, [0024]. Therefore, a POSITA would have beneficially applied Rans to Royyuru-Phillips-Casey to use any or all of the above described information received/stored at the user device to generate the DTC and/or dynamic PAN. SAMSUNG-1003, ¶227. Such a modification would have increased the overall security of the resulting system by expanding the set of data that can be used in generating Royyuru's dynamic cryptograms thereby further protecting against brute force attacks or guessing attempts. SAMSUNG-1003, ¶227. Furthermore, a POSITA would have had a reasonable expectation of success in applying Rans to Royyuru-Phillips-Casey. SAMSUNG-1003, ¶227.

C. [GROUND 2A] – Obviousness based on Phillips-Royyuru-Casey (Claims 19-21, 23-25, 28-30)

1. Phillips-Royyuru-Casey Combination

A POSITA would have beneficially applied Royyuru to Phillips to generate the dynamic cryptograms described by Royyuru on the resulting device, generate and receive the information used to generate Royyuru's dynamic cryptograms (including values generated and/or provided by the payment processors, issuers, and merchants described by Royyuru), and to process a transaction for approval/denial by a payment processor and/or issuer as described by Royyuru to achieve known benefits. SAMSUNG-1003, ¶¶228-233. Such a modification would have increased the security of the resulting system while allowing for easy authentication of the transaction "based on the DTC at the payment processor system or at the financial institution." SAMSUNG-1003, ¶230; SAMSUNG-1004, [0005]-[0010], [0032]-[0034], [0047]-[0048], [0051], [0057]. Such a modification provides for "securely handling a financial transaction." SAMSUNG-1004, [0004]. Royyuru's authentication cryptograms are "valid for a single transaction," thus increasing security of the resulting system due to intercepted cryptograms being useless for conducting future, fraudulent transactions. SAMSUNG-1004, [0005]; SAMSUNG-1003, ¶230. Furthermore, a POSITA would have recognized that generating the cryptograms described by Royyuru using the various data described by Royyuru for generating the cryptograms would have helped to ensure that the cryptograms were strong and

could only be used by the intended device (e.g., the device associated with the IKCV). SAMSUNG-1003, ¶230. Furthermore, a POSITA would have applied Royyuru's dynamic cryptogram generating techniques to Phillips to fill in missing details regarding "cryptographically generat[ing] a dynamic security code (CVC3) for the transaction" in a secure manner. SAMSUNG-1005, [0059], [0066], [0073]; SAMSUNG-1003, ¶230.

A POSITA would have turned to Royyuru's teachings for processing the DTC and dynamic PAN (and other information such as the ATC) at the payment processor and/or issuer to approve/deny the transaction because Phillips contemplates "wirelessly transmitting" payment information for a selected payment method to the merchant, including a dynamically generated cryptogram, to process the transaction, and Royyuru describes approving/denying a transaction based on such information. SAMSUNG-1005, [0059]-[0060]; SAMSUNG-1004, [0006], [0010], [0034], [0044], [0047]-[0050]. SAMSUNG-1003, ¶231. Such secure processing of the transaction using the described cryptograms would have improved the overall security of the resulting system. SAMSUNG-1003, ¶231.

A POSITA also would have modified the device resulting from application of Royyuru to Phillips based on Casey for the reasons discussed in Ground 1A, *supra*, to display request information including merchant information, transaction in-

formation, price, etc., to require user authorization through manipulation of a displayed control, and to display transaction status / payment receipt information. SAMSUNG-1003, ¶232

Finally, application of Royyuru and Casey to Phillips would have been merely the application of known techniques to a known system ready for improvement to yield predictable results. SAMSUNG-1003, ¶233. Here, all three references describe aspects of conducting wireless payment transactions using payment information stored on or generated by a mobile device and Royyuru and Casey describe improvements that would have been beneficially applied to Phillips' system. *Id*. A POSITA would have furthermore had a reasonable expectation of success in modifying Phillips' mobile payment system based on Royyuru and Casey as they all are directed toward similar mobile payment systems. *Id*.

2. Application of Phillips-Royyuru-Casey

[19.pre]

Phillips discloses methods for "making on-line purchases." SAMSUNG-1005, [0049], [0071], [0073], [0082]; SAMSUNG-1006, 3:14-19, 8:23-31, 11:50-60; SAMSUNG-1003, ¶234.

[19.a]

Phillips describes that after selecting "on-line items" for an on-line transaction, the device receives "***a payment request.***" SAMSUNG-1005, [0072], FIG. 13. Phillips discloses using wireless communication during online transactions and

therefore a POSITA would have recognized that Phillips provides, or at least renders obvious, receiving the request via a wireless interface. SAMSUNG-1005, [0073], [0066]; SAMSUNG-1003, ¶235. For example, the device can receive the request as NFC "interrogation signals." *Id.*, [0023], [0027], [0057]. Casey confirms that in the resulting system the request is received via a wireless interface. SAMSUNG-1006, 6:62-7:12, 8:52-9:8, 5:49-50; SAMSUNG-1003, ¶235. A POSITA would have recognized that wireless communications (e.g., via WiFi, cellular networks, etc.) for facilitating on-line interactions (including on-line transactions) were in common use during the relevant timeframe and therefore a POSITA would have implemented the resulting system to utilize wireless communications for online transactions (as disclosed by Casey) to allow for on-line transactions over wireless networks. SAMSUNG-1003, ¶235.

[19.b]

"[T]he display component 110 may be a touch screen." SAMSUNG-1005, [0018]; SAMSUNG-1006, 3:10-19. "[T]he mobile device…receives 1302 a payment request that includes a merchant identifier (merchant ID)." SAMSUNG-1005, [0072]. Casey discloses that in the resulting combination, the payment request notification is displayed on the touchscreen. SAMSUNG-1003, ¶236. Casey discloses receiving "a request for payment" and displaying relevant request information "such as the item price, tax, and shipping costs" or "additional details about

the order." SAMSUNG-1006, 8:52-9:8, 13:24-35, 12:19-29. FIG. 5 of Casey shows the request information for the online transaction is displayed on the touchscreen to allow for user confirmation or cancellation:

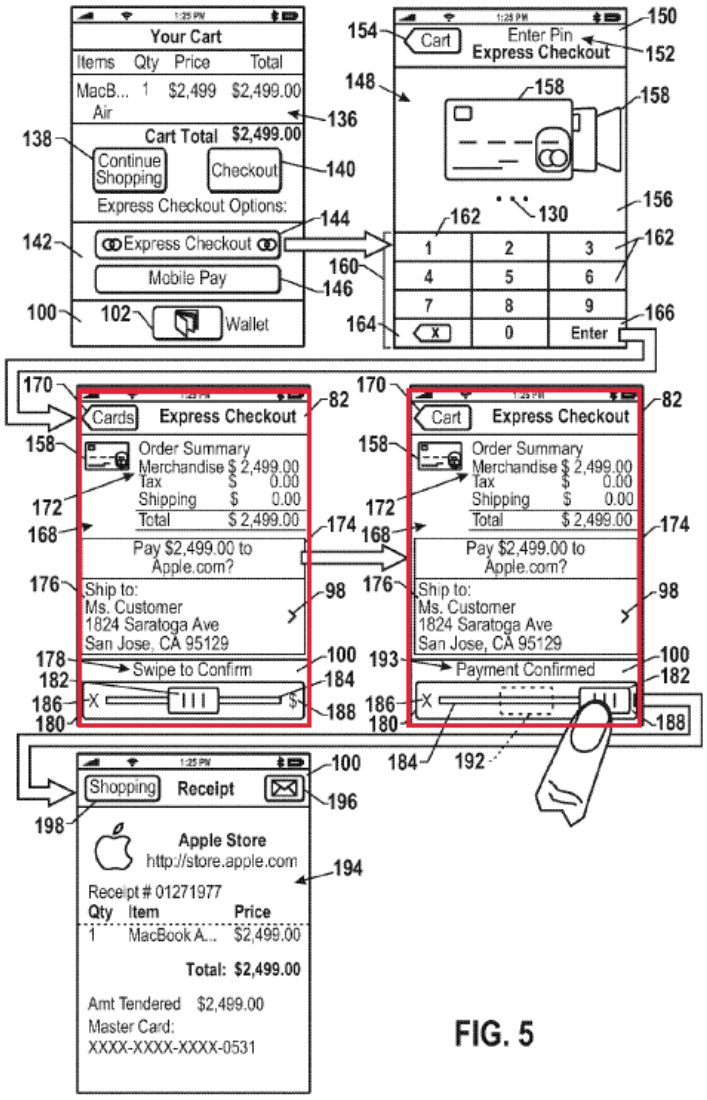


FIG. 5

SAMSUNG-1006, FIG. 5, *see also* FIGs. 6-8; SAMSUNG-1003, ¶236.

Elements [19.c]-[19.d]

Phillips discloses that responsive to receiving a payment request, the device displays an automatically selected card if it matches pre-specified criteria, or allows the user to select a different payment card account by selecting a "'Change' command icon 1114." SAMSUNG-1005, [0035]-[0036], [0072]-[0076].

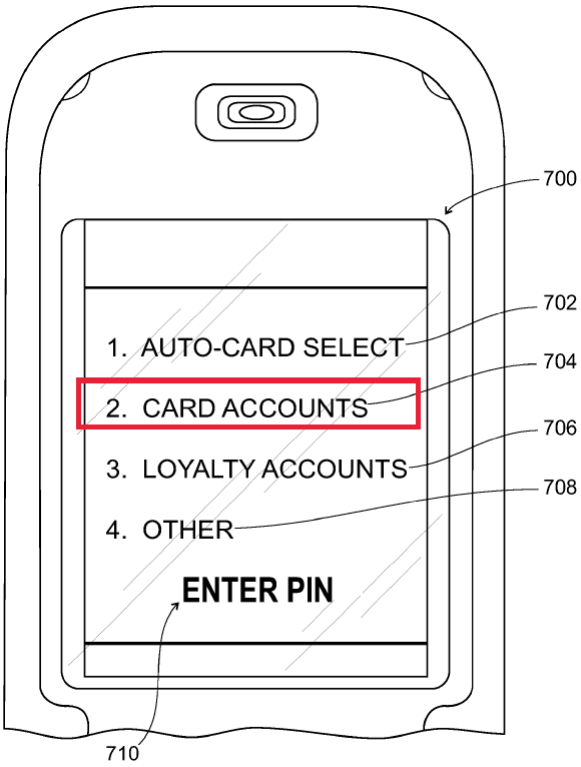


FIG. 7

SAMSUNG-1005, FIG. 7. Phillips discloses that upon selection of the "card accounts" option a plurality of selectable payment options are displayed. SAMSUNG-1005, [0036]-[0037], [0074]-[0075] (selection of "change" icon provides selectable payment options). In some embodiments, the user is "required" to enter "her PIN before being permitted to select any of the options 702 to 708" and there-

fore the user-selectable payment account options are only displayed upon authorizing the valid device user (via the PIN). SAMSUNG-1005, [0035], [0038]-[0039] ("Once the user PIN is entered, then the process 500 advances to block 516 wherein a card selection sub-menu of card account choices is displayed. The requirement for the user to enter a PIN guards against the possibility that the user of the mobile device is not the owner of a selected payment card account."), *see also* FIG. 11; SAMSUNG-1003, ¶¶237-240. Requiring such PIN entry prior to card selection would have provided additional security in both on-line and in-store implementations of the predictable combination. SAMSUNG-1003, ¶238. Casey confirms that the payment selection options are displayed responsive to receiving the request and the user entering a PIN. SAMSUNG-1006, 8:59-9:22; FIGs. 3, 5, 8.

Phillips' FIG. 8 shows various options for "selection of the payment card account" for a transaction. SAMSUNG-1005, [0039]-[0041]; SAMSUNG-1003, ¶¶239-240.

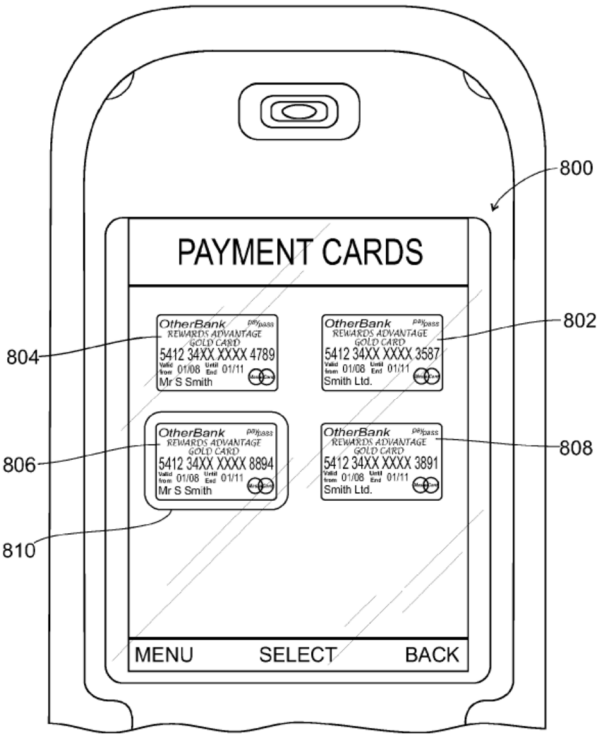


FIG. 8

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, 8:32-44, 9:4-36, 9:58-10:2, 12:46-65. A POSITA would have recognized that requiring selection of a payment type provides requesting a user approval of payment via the touch-screen display. SAMSUNG-1003, ¶240.

Alternatively, Casey discloses that in the resulting combination, after entry of a PIN and "***selection of a payment instrument***, the electronic device may display one or more ***graphical elements for confirming the payment transaction***" and "[u]pon confirmation, the electronic device may transmit transaction and ac-

count information." SAMSUNG-1006, 3:20-37, 8:32-44, 9:9-36, FIG. 3; SAMSUNG-1003, ¶241. Furthermore, "the device 10 may ***request***...***a PIN to verify the payment instrument***." SAMSUNG-1006, 9:9-43 ("confirm the payment transaction"), 15:23-37.

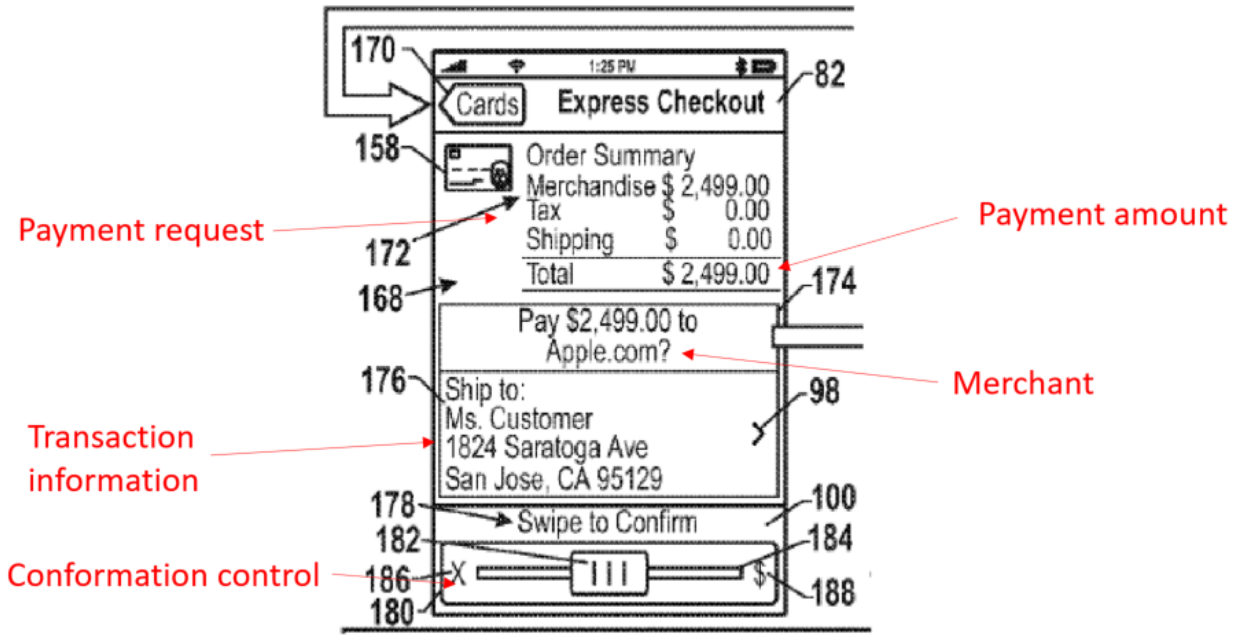
[19.e]-[19.f]

The Phillips-Royyuru-Casey combination provides Elements [19.e]-[19.f]. *Supra*, Elements [1.f]-[1.h]; SAMSUNG-1003, ¶242.

[19.g]

FIG. 5 of Casey demonstrates that the Phillips-Royyuru-Casey combination provides user interface screens for "confirmation of an online shopping payment through a touch screen" that include a "prompt" for "the user to move a graphical element 180 to confirm the payment transaction" and information comprising the payment request, the merchant, the amount and other transaction information.[4] SAMSUNG-1006, 2:33-35, 13:36-51; SAMSUNG-1003, ¶243.

[4] The term "transaction information" does not previously appear in claim 19.



SAMSUNG-1006, FIG. 5 (annotated), *see also* FIG. 6; 13:16-35.

[19.h]

Phillips discloses receiving user input approving the transaction: "the requirement that she enter her PIN to enable the transaction adds a second (knowledge) factor to the first (possession)." SAMSUNG-1005, [0062]; SAMSUNG-1003, ¶¶244-245. Phillips further describes "selection of the payment card account" by user input and "the user may be required to enter a PIN or code before selecting a payment card." SAMSUNG-1005, [0038]-[0039]. In another example, "[t]he user acknowledges 1012 in FIG. 10 that the automatically selected card is correct by entering 1014 her personal identification number (PIN)." *Id.*, [0059], [0057], [0066]. Phillips also receiving a "'Cancel' command" input. *Id.*, [0061]-[0062].

Casey confirms that in the resulting combination the user may "select a payment instrument by tapping a corresponding graphical element" and entering "a PIN to verify the payment instrument." SAMSUNG-1006, 9:9-36. The display further includes a control element to allow the user to confirm or deny the transaction. SAMSUNG-1006, 13:36-51, 14:12-49, 15:23-37, FIGs. 5-6.

[19.i]

Phillips discloses that after user selection of the desired payment option and confirmation of the transaction (e.g., entering of a PIN), payment information for the selected payment method is transmitted to the merchant. SAMSUNG-1005, [0073]. A POSITA would have recognized that in the Phillips-Royyuru-Casey combination, this payment information comprises the DTC and dynamic PAN described by Royyuru. SAMSUNG-1003, ¶¶246-247; SAMSUNG-1004, [0006] ("The DTC and the dynamic PAN can be provided by the device for use in the transaction"), [0047]. Casey confirms that in the resulting combination, after the user moves the graphical control "to the conformation position…the device 10 may transmit payment information to confirm the payment transaction." SAMSUNG-1006, 14:11-24.

[20.a]

Royyuru discloses that in the predictable combination, the DTC is a cryptogram generated using **the PAN**, **expiration date, unpredictable number, ATC**,

CK (IKCV). SAMSUNG-1004, [0057], [0005]-[0007]; *see also Supra*, Elements [5.a], [6.a], [8], [10], [18.a]; SAMSUNG-1005, [0059] ("cryptographically generate a dynamic security code"). The dynamic PAN is calculated using the real PAN, ATC, UN, and IKCV. SAMSUNG-1004, [0057], [0005]. The ATC is an "Application Transaction Counter" which "increments for each transaction." SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶¶248-250. The PAN ("digits from the card number") is a payment account number and information known to the processing authority. SAMSUNG-1004, [0007], [0057]. The UN is any number generated or "***received by the presentation instrument***" and therefore provides any device-unique information calculated or received by the device such as "information known by the owner…e.g., a PIN or other identifying information," thus providing the claimed user information. SAMSUNG-1004, [0051]; SAMSUNG-1003, ¶249. Royyuru's IKCV and Card-Key (CK) provide examples of information and secrets known to the payment processing authority. *Id*. The CK is described as "system-generated by payment processor when an institution requests that a card be added to the service." SAMSUNG-1004, [0057]. The IKCV is "generated when each card (device) is being customized" and can be generated by the payment processor or issuer. *Id.*, [0057], [0046].

The dynamic PAN and DTC are used to validate the payment transaction and are therefore utilized in place of a card validation value. *Supra*, Elements [1.g],

[1.j], [4], [5.c]; SAMSUNG-1003, ¶250. Royyuru describes that 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. SAMSUNG-1004, [0057]; SAMSUNG-1003, ¶250. The DTC is provided as part of "Track 1" "verification information" in place of traditional card validation values (CVC). *Supra*, [18.a]; SAMSUNG-1004, [0049]; SAMSUNG-1005, [0059]; SAMSUNG-1003, ¶250.

[20.b]

Supra, Element [18.b]; SAMSUNG-1003, ¶¶251-252.

[21.a]-[21.b]

The IKCV is a "card-specific" ("customized" for the specific device) static device account number that is limited in scope of valid use to the specific device. *Supra*, [1.e], [8.a], [11]; SAMSUNG-1004, [0057], [0046], [0032]-[0033], [0054]-[0055]; SAMSUNG-1003, ¶¶253-254. The IKCV is used in generating both the DTC and dynamic PAN. SAMSUNG-1004, [0005]-[0010], [0057].

[21.c]

Royyuru describes that the IKCV "can be generated for the presentation instrument 305 by the payment processor system" and "loaded into the device" and therefore is provided by the payment processing authority in place of payment issuer information. SAMSUNG-1004, [0046], [0057]; SAMSUNG-1003, ¶255.

Specifically, the IKCV is "a card variant of an institution key" and therefore is provided by the payment processing authority in place of the institution key. SAMSUNG-1004, [0091]-[0096], [0057] ("A card-specific variation of the IK (IKCV) can be loaded into the device").

[21.d]

Supra, Elements [1.h]-[1.j], [19.i]; SAMSUNG-1003, ¶256.

[21.e]

Supra, Element [1.h]; SAMSUNG-1003, ¶257.

[21.f]

Supra, Elements [1.g]-[1.j], [19.i]; SAMSUNG-1003, ¶258.

[21.g]

Royyuru describes that the "payment processor system or at the financial institution" uses the DTC to validate the transaction and that the dynamic PAN is used to determine the real PAN used to process the device by the issuer. SAMSUNG-1004, [0006], [0034], [0039], [0048], [0055], [0050]. For example, the payment processor will "decline the transaction if the DTC is incorrect." *Id.*, [0057]. In some examples, the real PAN is determined from the dynamic PAN and the real PAN is then used to validate the DTC. *Id.*, [0039], [0055]. A POSITA

would therefore have recognized that if either of the DTC or dynamic PAN is invalid or not provided, the transaction is deniable as invalid and outside a valid scope of device-limited usage. SAMSUNG-1003, ¶¶259-260.

[23.a]

As discussed with respect to Elements [1.j] and [5.c], *supra*, Royyuru describes that the transaction is authenticated "based on the DTC" by "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." SAMSUNG-1004, [0006], [0034], [0048]. A POSITA would have recognized that it would have been obvious for the validation system of the payment processor to use the unique card-level key to validate the DTC (as expressly described by Royyuru) by using the unique card-level key to generate a DTC value and then comparing the DTC generated at the payment processor to the received DTC to ensure that the received DTC is correct. SAMSUNG-1003, ¶¶262-263.

The DTC can be generated based on each of the factors recited by claim 23. SAMSUNG-1003, ¶263. Specifically, Royyuru discloses that the cryptogram (the DTC or dynamic PAN) for authenticating the transaction can be generated by combining a time of use ("a time of day"), a transaction sequence count (ATC), a device account number (IKCV), a user account information (PAN, cardholder name,

expiration date), a payment issuer information (PAN, routing information, IKCV, expiration date), a payment processing authority secrets (IKCV, CK), and transaction information (all of the above plus "one or more factors from the payment device or the POS reader"). SAMSUNG-1004, [0051], [0057], [0006], [0009], [0032], [0046], [0091]-[0096]; SAMSUNG-1003, ¶¶263, 126-129, 149-150.

[23.b]

As described by Casey, in the Phillips-Royyuru-Casey combination, "***[a]fter the payment transaction has been confirmed***, the device 10 may ***receive*** and display (block 78) ***a receipt for the payment transaction***." SAMSUNG-1006, 10:47-53, *see also* 10:20-29, 16:3-20; SAMSUNG-1003, ¶¶264-266. Royyuru discloses that in the predictable combination, the transaction is completed dependent on validation of complete device payment information by the payment processor authority and therefore the transaction status indicating authorization of the payment conveyed in the receipt is dependent on this validation. SAMSUNG-1004, [0047]-[0048], [0044], [0050], [0055]; SAMSUNG-1003, ¶¶133-134, 264.

Royyuru describes "[t]he transaction can be authenticated at the payment processor system or at the financial institution based on the DTC." SAMSUNG-1004, [0006], [0047] ("The dynamic PAN 326 and DTC 327 can then be submitted to the payment processor system 350 and/or financial institution 370 and 375 via the payment network 345 for approval and/or processing of the transaction."),

[0010], [0044], [0050]; *see also Supra* Elements [1.j], [5.c], [2]-[3], [21.g]; SAMSUNG-1003, ¶265.

The DTC and dynamic PAN are "sent in place of the real PAN" in transactions. *Supra*, Elements [1.g], [4], [8.d]; SAMSUNG-1004, [0057], [0032]-[0034], [0006]-[0010]; SAMSUNG-1003, ¶266.

[23.c]

Royyuru discloses that in the predictable combination, 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 (transactional re-use of a number limited to a one-time use). SAMSUNG-1004, [0005], [0033], [0047], [0053], [0057], Abstract; SAMSUNG-1003, ¶¶267-268. In another example, the DTC and dynamic PAN are rejected based on comparing the ATC "to that in the previously received transaction to detect gaps…and duplication" indicating fraud. *Id.*, [0057].

[24]

FIG. 8 of Phillips shows a user interface for selecting of a payment method which "may be a touch screen." SAMSUNG-1005, [0039]-[0041], [0018]; SAMSUNG-1003, ¶¶269-272.

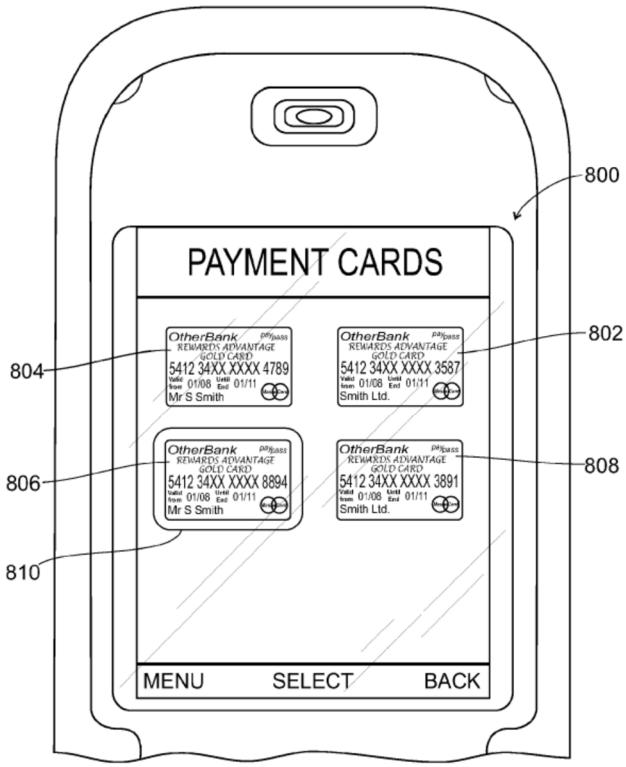


FIG. 8

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. A POSITA would have recognized that in the touch screen implementation this selection would have been made via a user touch input. SAMSUNG-1003, ¶271.

[25.pre]

Phillips describes "[a] computer readable medium storing non-transitory instructions for controlling a mobile device processor, the instructions configured to

cause the processor" to perform the described functions. SAMSUNG-1005, Cl. 13, [0020], [0029], [0055]; SAMSUNG-1003, ¶273.

[25.a]

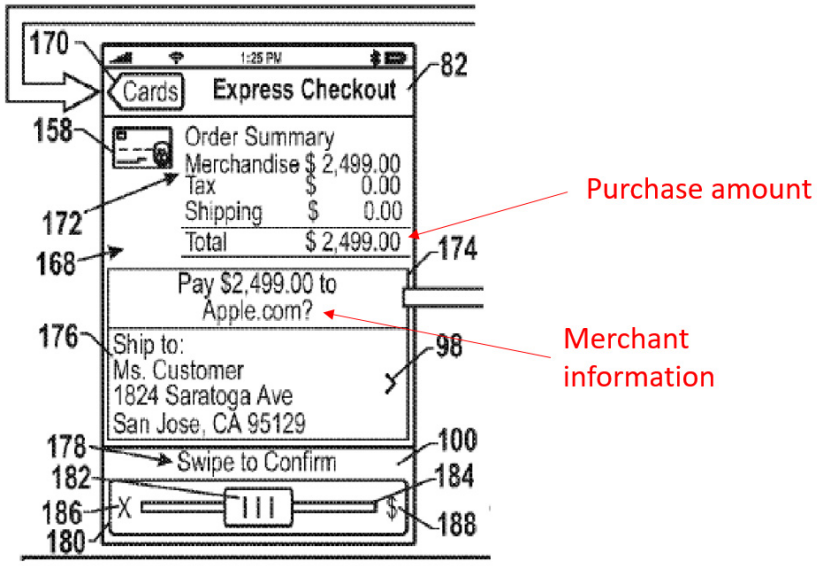
Phillips teaches that in the resulting combination the user is required to "enter a PIN" to initiate a financial transaction. SAMSUNG-1005, [0035], [0038]-[0039], [0058], [0061], [0066], [0072]-[0073]; SAMSUNG-1003, ¶274.

[25.b]

Phillips describes that after the user enters her PIN to confirm the payment method, "[t]he mobile phone may then operate, in some cases, to transmit the code to the website to consummate the transaction." SAMSUNG-1005, [0072]-[0073], *see also* [0035], [0038]-[0039], [0058], [0061]; SAMSUNG-1004, [0005]; SAMSUNG-1003, ¶275.

[25.c]

Phillips describes receiving "an on-line merchant identifier." SAMSUNG-1005, [0049], [0071], [0082]. Casey discloses that in the predictable combination, the merchant information and purchase amount are displayed on the user device. SAMSUNG-1006, 2:33-35, 13:14-51; SAMSUNG-1003, ¶276.



SAMSUNG-1006, FIG. 5 (annotated), *see also* FIG. 6.

[25.d]-[25.e]

Supra, Elements [19.c]-[19.d].

[25.f]-[25.g]

Supra, Elements [1.e]-[1.h]. Additionally, Casey discloses that the resulting combination receives a valid user transaction payment approval. Casey discloses that in the resulting combination "***[a]fter selection of a payment instrument***, the electronic device may display one or more ***graphical elements for confirming the payment transaction***" and "[u]pon confirmation, the electronic device may transmit transaction and account information." SAMSUNG-1006, 3:20-37, 8:32-44, 9:9-43, FIGs. 5-6; SAMSUNG-1003, ¶278. Furthermore, Royyuru discloses that it is initiation of the transaction that causes the device of the resulting combination to "trigger the processor 320 of the presentation instrument 305 to read the

IKCV 315, the unique card-level key 317 and real PAN 316 from memory 310" and use these values to generate the DTC and dynamic PAN. SAMSUNG-1004, [0047]. A POSITA would have recognized that in the resulting combination, this calculation would have occurred in response to user transaction payment approval so as to not waste computing resources to generate the DTC and dynamic PAN for transactions rejected/cancelled/changed by the user. SAMSUNG-1003, ¶278.

[25.h]

Supra, Element [19.i]

[25.i]

Supra, Elements [1.j]-[1.k], [6.d]-[6.e].

[28.a]

Royyuru discloses that the resulting combination includes combining a static device-specific payment account information (IKCV), a device generated information (DTC, ATC, dynamic PAN, undeterminable number), other user information (cardholder name, "information known by the owner…a PIN or other identifying information"), other account information stored on the device (PAN, expiration date, IKCV) which uniquely identifies the specific user (user name, "a PIN or other identifying information"), specific selected account (PAN, IKCV), and the specific device (IKCV) when generating the DTC and dynamic PAN. SAMSUNG-

1004, [0005]-[0010], [0032]-[0034], [0047]-[0048], [0050]-[0053], [0057], [0091]-[0096]. SAMSUNG-1003, ¶¶282-283.

[28.b]

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

[28.c]

Supra, Element [1.h].

[28.d]

Supra, Element [1.i].

[28.e]

Supra, Elements [19.c]-[19.d]. As shown in FIGs. 8 and 11 of Phillips (*supra*, Elements [19.c]-[19.d]), a portion of the payment account number of the user selected payment account is displayed. SAMSUNG-1003, ¶287.

[29.a]

Supra, Elements [8.e], [9], [18.a], [28.a].

[29.b]

Supra, Elements [1.g], [4], [5.b].

[29.c]

"The real PAN of the financial account can be determined at the payment processor system. The transaction can be authenticated at the payment processor

system or at the financial institution based on the DTC." SAMSUNG-1004, [0006].

The transaction is authenticated "based on the DTC" by "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." *Supra*, Element [1.j]; SAMSUNG-1004, [0006], [0034], [0048]. A POSITA would have recognized that it would have been obvious for the validation system of the payment processor to use the unique card-level key to validate the DTC (as expressly described by Royyuru) by using the unique card-level key to generate a DTC value and then comparing the DTC generated at the payment processor to the received DTC to ensure that the received DTC is correct. SAMSUNG-1003, ¶¶292-293. Therefore, in order to generate the DTC at the payment processor for such comparison, the payment processor would need to know the correct set of user, device and account specific information to be cryptographically combined into an authority computed cryptogram. *Supra* [28.a], [8.e], [9], [18.a], [18.c]; SAMSUNG-1003, ¶293.

[29.d]-[29.e]

"The transaction can be authenticated at the payment processor system or at the financial institution based on the DTC." SAMSUNG-1004, [0006]. Therefore, in the scenario described above in which the payment processor authenticates the

DTC through comparison to a payment processor generated DTC, the transaction would be denied as invalid if the payment processor generated DTC does not match the received DTC and would be approved as valid if the generated DTC matches the received DTC. SAMSUNG-1003, ¶294.

[29.f]

Supra, Elements [1.j]-[1.k], [6.d]-[6.e].

[30.a]

The Phillips-Royyuru-Casey combination provides a processor and a non-transitory, computer-readable medium storing computer executable instructions to perform the disclosed functions when executed. *Supra*, [25.pre]. Both the DTC and dynamic PAN of Royyuru provide the claimed dynamically generated, one-time limited-use cryptogram number. SAMSUNG-1004, [0005]-[0009] (describing "a set of dynamic cryptograms that are valid for a single transaction" including the DTC and dynamic PAN), [0051], [0057]. Both the DTC and dynamic PAN can be generated using the IKCV. SAMSUNG-1004, [0005]-[0010], [0057]; SAMSUNG-1003, ¶¶297-298. The "IKCV ***of the device***" is static and unique to the device in that it 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" before being provided to the device and is therefore at least a payment issuer device account information, device payment account number, user

payment account number, or payment processing authority secret that is known to the device, the payment issuer authority, and the payment processing authority. *Supra*, [28.a], [8.e], [9], [18.a]; SAMSUNG-1004, [0055]-[0057], [0046], [0033], [0091]-[0096]; SAMSUNG-1003, ¶298.

[30.b]

Supra, Elements [1.g], [4].

[30.c]-[30.d]

Supra, Elements [29.d]-[29.e].

[30.e]

Supra, Elements [1.j]-[1.k], [6.d]-[6.e].

[30.f]

Both Phillips and Royyuru disclose that the device of the Phillips-Royyuru-Casey combination can be used to conduct payment transactions in electronic payment facilities in addition to online transactions. SAMSUNG-1003, ¶¶302-303. Specifically, the device can "interact with an RFID proximity reader (or a NFC proximity reader) that may be associated with a POS terminal to provide a card account number (stored in the payment circuit **224**) for a purchase transaction at the POS terminal." SAMSUNG-1005, [0023], [0057]. Similarly, Royyuru describes "providing the DTC and dynamic PAN to a Point-of-Sale (POS) device." SAM-

SUNG-1004, [0005]-[0006]. For example, the user "passes or taps the presentation instrument 305 on or near the point-of-sale device 330." *Id.*, [0047], [0002]. Providing the DTC and dynamic PAN to a POS device to facilitate a transaction provides, or at least renders obvious, emulating the behavior of an issuer account payment transaction using the complete payment information in electronic payment facilities. SAMSUNG-1003, ¶302.

D. [GROUND 2B] – Obviousness based on Phillips-Royyuru-Casey-Rans (Claims 23, 28-30)

1. Phillips-Royyuru-Casey-Rans Combination

A POSITA would have applied Rans to the Phillips-Royyuru-Casey combination in the same manner and for the same reasons as the described application of Rans to the Royyuru-Phillips-Casey combination. *Supra*, Ground 1B; SAMSUNG-1003, ¶¶304-306, 217-218.

2. Application of Phillips-Royyuru-Casey-Rans Combination

[23]

Royyuru discloses that the cryptogram (the DTC or dynamic PAN) for authenticating the transaction can be generated by combining a time of use ("a time of day"), a transaction sequence count (ATC), a device account number (IKCV), a user account information (PAN, cardholder name, expiration date), a payment issuer information (PAN, routing information, IKCV, expiration date), a payment processing authority secrets (IKCV, CK), and transaction information (all of the

above plus "one or more factors from the payment device or the POS reader"). SAMSUNG-1004, [0051], [0057], [0006], [0009], [0032], [0046], [0091]-[0096]; SAMSUNG-1003, ¶¶307-310.

As discussed with respect to Ground 1B, *supra*, Rans discloses that in the resulting combination all of this "data that may be used to generate the second authentication data" is stored at the payment processor and/or issuer and is used to generate "second authentication data" at the "authentication agent or other entity involved in the transaction" which is then compared to the DTC and/or dynamic PAN received from the user device to approve the transaction if "the first authentication data and second authentication data are equal" or reject the transaction if there is a mismatch in the payment processor generated data and the received data. SAMSUNG-1014, [0022]-[0023], [0037]-[0039]; SAMSUNG-1003, ¶309. All other elements of claim [23] are provided by the Phillips-Royyuru-Casey-Rans combination for the reasons discussed in Ground 2A, *supra*. SAMSUNG-1003, ¶¶309-310.

[28]

To the extent claim [28] or Royyuru's disclosures are interpreted narrowly, Rans discloses that the dynamic authentication data (applicable to Royyuru's DTC and dynamic PAN) can be generated using "***any other piece of data***" available to

the device, including all information discussed in Ground 2A with respect to claim [28]. SAMSUNG-1014, [0039], [0023]-[0024]; SAMSUNG-1003, ¶¶311-314.

All other elements of claim [28] are provided by the Phillips-Royyuru-Casey-Rans combination for the reasons discussed in Ground 2A, *supra*. SAMSUNG-1003, ¶¶313-314.

[29]

Rans discloses that in the predictable combination, the payment processor stores and identifies "the PIN, the challenge, the unpredictable number, a synchronized transaction counter, or ***any other data that may be used to generate the authentication data***" and uses such information to generate a second authentication data that is compared to the received DTC and/or dynamic PAN of Royyuru to identify a match and confirm or deny the transaction. SAMSUNG-1014, [0022]-[0023], [0037]-[0039]; SAMSUNG-1003, ¶¶315-318. The transaction is approved as valid when the authentication information (Royyuru's DTC and/or dynamic PAN in the predictable combination) generated at the payment processor and the received DTC and/or dynamic PAN "are equal" and denied when the values do not match. SAMSUNG-1014, [0037]; SAMSUNG-1003, ¶¶316. Rans further discloses that transactional payment information (e.g., "data from which a PAN can be determined") is received from the user device and used to identify the correct set of information to generate the second authentication data, such as the user's

PIN and other user data. SAMSUNG-1014, [0037]-[0039] ("any other piece of data"); SAMSUNG-1003, ¶316.

All other elements of claim [29] are provided by the Phillips-Royyuru-Casey-Rans combination for the reasons discussed in Ground 2A, *supra*. SAMSUNG-1003, ¶¶317-318.

[30]

Rans discloses that in the predictable combination, the payment processor generates "second authentication data" (e.g., Royyuru's DTC and/or dynamic PAN in the predictable combination) "based on data held by the card issuer, authentication agent or other entity involved in the transaction." SAMSUNG-1014, [0022]-[0023], [0037]-[0039]; SAMSUNG-1003, ¶¶319-322. The transaction is approved as valid when the authentication information (Royyuru's DTC and/or dynamic PAN) generated at the payment processor and the received DTC and/or dynamic PAN "are equal" and denied when the values do not match. SAMSUNG-1014, [0037]; SAMSUNG-1003, ¶320.

All other elements of claim [30] are provided by the Phillips-Royyuru-Casey-Rans combination for the reasons discussed in Ground 2A, *supra*. SAMSUNG-1003, ¶¶321-322.

E. [GROUND 2C] – Obviousness based on Phillips-Royyuru-Casey-Rans-Carlson (Claim 27)

1. Phillips-Royyuru-Casey-Rans-Carlson Combination

Carlson describes a mobile device for "conducting transactions using pseudo primary account identifiers." SAMSUNG-1013, [0012], [0029]; SAMSUNG-1003, ¶¶96-101. The pseudo account identifier can be "similar in format to a consumer's real account identifier" without revealing the real account identifier. SAMSUNG-1013, [0030]. The pseudo account identifier is generated by the payment processor, specific to the device, 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 Carlson to the Phillips-Royyuru-Casey-Rans 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, ¶¶323-327. 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, ¶326. Therefore, setting an expiration for the IKCV can prevent fraudulent use of

the IKCV to generate DTCs and dynamic PANs by unauthorized devices. *Id*. 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*.

Application of Carlson to the Phillips-Royyuru-Casey-Rans 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 Phillips-Royyuru-Casey-Rans-Carlson Combination to Claim 27

[27.a]-[27.b]

Royyuru discloses that the resulting device includes a "***processor*** to detect initiation of the transaction, ***generate a Dynamic Transaction Cryptogram (DTC)*** using the unique card-level key and a dynamic PAN" and therefore provides at least as much (if not more) detail of a cryptographic processor that generates authentication cryptograms as the '538 patent specification. SAMSUNG-1004, [0007]; SAMSUNG-1001, 1:42-47. The DTC and dynamic PAN are "***valid for a single transaction***." SAMSUNG-1004, [0005], [0033], [0047], [0053], [0057], Abstract; SAMSUNG-1003, ¶¶328-329.

[27.c]

Supra, Elements [1.e], [1.g]-[1.h], [8.a]. The IKCV is generated by, and therefore known to, Royyuru's payment processor. SAMSUNG-1004, [0057], [0046], [0033], [0055]; SAMSUNG-1003, ¶¶330, 169, 177.

[27.d]

Supra, Elements [18.a], [20.a]. Furthermore, a POSITA would have recognized that the IKCV is information stored in the device and specific to the device and which is not communicated in the transaction. *Supra*, Ground 1A, Elements [1.e], [1.i]; SAMSUNG-1003, ¶¶331, 168.

[27.e]

The transaction is authenticated "based on the DTC." *Supra*, Element [1.j]; SAMSUNG-1004, [0006], [0034], [0048]. Rans discloses that in the predictable combination, the payment processor stores and identifies "the PIN, the challenge, the unpredictable number, a synchronized transaction counter, or ***any other data that may be used to generate the authentication data***" and uses such information to generate a second authentication data that is compared to the received DTC and/or dynamic PAN of Royyuru. SAMSUNG-1014, [0022]-[0023], [0037]-[0039]; SAMSUNG-1003, ¶¶332-333. Therefore, Rans demonstrates that the Phillips-Royyuru-Casey-Rans-Carlson combination provides that the above listed information and secrets used to generate the DTC and/or dynamic PAN are known to both the device and the payment processing authority. SAMSUNG-1003, ¶332; *see*

also SAMSUNG-1004, [0057] (ATC, IKCV, PAN, user information, and other information known to payment processor), [0048], [0091]-[0096].

For example, the "ATC [is] received by the payment processor" for each transaction. SAMSUNG-1004, [0057]. The IKCV and CKs are generated by or "used by" (and therefore known to) the payment processor. *Id.*, [0057], [0046]. The PAN is an input to generating the IKCV and therefore known to the payment processor. *Id.*, [0091]-[0096].

[27.f]

Royyuru's IKCV "is a variant of an institution key of an issuer of the financial account" and can be generated by (and is therefore known to) the financial institution "or other issuer of the instrument." SAMSUNG-1004, [0007], [0046]. As described above, Carlson would have been predictably applied to the Phillips-Royyuru-Casey-Rans combination such that the IKCV is "set to expire…after a certain time period" by the payment processor or issuer. SAMSUNG-1013, [0036], [0044], [0086]; SAMSUNG-1003, ¶334. Because the IKCV is device specific, the expiration date of the IKCV in the predictable combination is a device-specific expiration date of limited duration of validity. SAMSUNG-1003, ¶334; SAMSUNG-1004, [0046], [0033], [0055], [0057].

[27.g]

Royyuru's DTC and dynamic PAN can be generated using both the IKCV and any "unpredictable number" including any "number…***received by the presentation instrument***" and/or "one or more factors from the payment device or the POS reader." SAMSUNG-1004, [0051], [0057], [0006]; SAMSUNG-1003, ¶335. Furthermore, as discussed in Ground 1B, *supra*, Rans confirms that the dynamic authentication data (applicable to Royyuru's DTC and dynamic PAN) can be generated using an undeterminable number or "secret value" generated from a "cryptographic key," "a number or ***any other piece of data***." SAMSUNG-1014, [0039], [0023] ("any other data that may be used to generate the authentication data"); SAMSUNG-1003, ¶335. Therefore, in the predictable combination, generating the complete combined device payment information includes combining any and all of the above described information including the static device-specific device account number (IKCV), the IKCV expiration date, the user information ("information known by the owner of the presentation instrument 305, e.g., a PIN or other identifying information"), payment account information (real PAN, PAN expiration date, IKCV), and the dynamically generated cryptogram (either the DTC or dynamic PAN of Royyuru). SAMSUNG-1003, ¶335. Specifically, the complete payment information is formed by combining the DTC and dynamic PAN (*supra*, Element [1.h]) and because all of the above information can be used in generating the

DTC and/or the dynamic PAN, the combining of the DTC and dynamic PAN in the complete payment information provides this element. SAMSUNG-1003, ¶335.

[27.h]

Phillips discloses that after user selection of the desired payment option and confirmation of the transaction (e.g., entering of a PIN), the complete payment information for the selected payment method is transmitted to the merchant. SAMSUNG-1005, [0073]; SAMSUNG-1006, 14:11-24; *supra*, Element [19.i]. A POSITA would have recognized that in the Phillips-Royyuru-Casey-Rans-Carlson combination, this payment information comprises the DTC and dynamic PAN described by Royyuru. SAMSUNG-1003, ¶¶336-337; SAMSUNG-1004, [0006], [0047].

F. [GROUND 2D] – Obviousness based on Phillips-Royyuru-Casey-Law (Claim 26)

1. Phillips-Royyuru-Casey-Law Combination

Law describes methods "for providing a more seamless purchasing experience using a mobile device" while increasing security of sensitive payment information. SAMSUNG-1015, Abstract, [0056], [0084]-[0085], [0129]; SAMSUNG-1003, ¶¶105-107. A verified user for an account can be authenticated based on "supplemental information" such as "biometric data (e.g. voice data, finger prints, eye scan, etc.)" or a security question such as "favorite color." SAMSUNG-1015, [0053], [0067], [0124]. If incorrect information is provided by the user, the device

can "limit[] retry attempts to reduce the probability of a brute force attack being successful." SAMSUNG-1015, [0139]-[0142]. If incorrect information is provided, the system "requests from the user, a second, third, or nth time, either a correction to the information provided by the user or supplemental information." SAMSUNG-1015, [0149], [0155]. If the system does "not successfully verify the transaction after a third attempt (or some other number reasonable to the circumstances)" the transaction is denied. *Id.*

A POSITA would have been prompted to apply Law to the Phillips-Royyuru-Casey combination such that the resulting device requires supplemental verification information (in addition to the PIN described by Phillips and Casey) and limits the number of attempts at providing such supplemental verification information before denying the transaction to achieve known benefits. SAMSUNG-1003, ¶¶338-342. Such a modification would have "further mitigate[d] security risk…to help reduce the likelihood of successful brute force attacks" and "mitigate fraudulent transactions." SAMSUNG-1015, [0129], [0139]-[0142] ("limiting retry attempts to reduce the probability of a brute force attack being successful"). This technique would have also allowed for "triggering of an early-warning system." *Id.*

A POSITA would have recognized that application of Law to Phillips-Royyuru-Casey 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, ¶342.

2. Application of Phillips-Royyuru-Casey-Law Combination to Claim 26

[26.a]

Phillips discloses that "the display component **110** is a touch screen capable of accepting user input" and therefore the PIN entry described by Phillips (*supra*, Element [25.a]) is received via the device human input sensor. SAMSUNG-1005, [0020], [0045]; SAMSUNG-1003, ¶¶343-344.

[26.b]

A POSITA would have recognized the entry of a PIN as described by Phillips as a correct passcode touch entry sequence that identifies the authorized valid device user. SAMSUNG-1005, [0035] ("a prompt **710** that instructs the user to enter his/her personal identification number (PIN)"), [0038]-[0039], [0058], [0061], [0066], [0072]-[0073]; SAMSUNG-1003, ¶¶345-346. Law demonstrates that human to device inputs in addition to the PIN entry priming action described by Phillips can be used to provide additional security of user validation. SAMSUNG-1003, ¶345. The device of the resulting system verifies the user based on "supplemental information" such as "biometric data (e.g. voice data, finger prints, eye scan, etc.)," "passwords," or a security question such as "favorite color." SAMSUNG-1015, [0053], [0067], [0124].

Law describes that the user provides biometric data for a "retina scan, finger print, voice analysis, etc." using "a microphone, a finger print scanner, a camera, etc." or enter a password or security question answer. SAMSUNG-1015, [0124], [0053], [0067]. A POSITA would have found it beneficial and obvious to provide a visual prompt for the user on the display of the device to alert the user as to when to provide the fingerprint, retina scan, voice data, password, or security question answer. SAMSUNG-1003, ¶346. For example, Law describes "contact[ing] the user through the mobile device 10 and asks the user for their favourite color." SAMSUNG-1015, [0067]. In another example, Law describes that the device "prompts the user for" the supplemental information/ID and a POSITA would have found it obvious and beneficial to provide such prompt visually. SAMSUNG-1015, [0176], [0053], [0148], [0153]; SAMSUNG-1003, ¶346. A POSITA would have recognized from Law's disclosures as a whole that, in at least some scenarios, the user provides a correct user response input. SAMSUNG-1003, ¶346.

[26.c]

Law discloses that in the resulting combination, if incorrect verification information is provided, the system "requests from the user, a second, third, or nth time, either a correction to the information provided by the user or supplemental information." SAMSUNG-1015, [0149], [0155], [0139]-[0142] ("limiting retry attempts to reduce the probability of a brute force attack being successful."). If the

system does "not successfully verify the transaction after a third attempt (or some other number reasonable to the circumstances)" the transaction is denied. *Id.* Although Law describes this denying of the transaction after the reduced number of additional challenge attempts as being performed at the server, a POSITA would have recognized that it would have been obvious and beneficial to perform such failing of the user authorization and denial of the payment authorization at the device to beneficially reduce the amount of network communication required and increase the efficiency of the verification process. SAMSUNG-1003, ¶¶347-348.

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 '538 patent that are the same as those raised in this Petition.[5] 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

[5] Petitioner reserves all rights to pursue these invalidity grounds in the Related Litigation if IPR is not instituted.

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 justifies 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)

The '538 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 '538 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:IPR39843-0146IP1@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 IPR39843-0146IP1@fr.com (referencing No. 39843-0146IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, jjm@fr.com, bisenius@fr.com, nstephens@fr.com and batzli@fr.com).

Respectfully submitted,

Dated November 28, 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.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070 / F: 877-769-7945

(Control No. IPR2023-00219)

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 13,995 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated November 28, 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.
60 South Sixth Street, Suite 3200
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 28, 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