

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARDWARE INC.,
Patent Owner

Inter Partes Review Case No. IPR2025-01150
U.S. Patent No. 11,176,538

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,176,538**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '538 PATENT	1
A.	DESCRIPTION OF THE '538 PATENT	1
B.	FIELD OF ENDEAVOR AND PROBLEM SOLVED BY THE INVENTORS	1
C.	PRIORITY AND PROSECUTION HISTORY	2
D.	LEVEL OF SKILL OF A POSITA	3
III.	REQUIREMENTS UNDER 37 C.F.R. § 42.104	3
A.	STANDING UNDER 37 C.F.R. § 42.104(A)	3
B.	IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B)	3
C.	CLAIM CONSTRUCTION UNDER 37 C.F.R § 42.104(B)(3).....	4
1.	<i>Claim limitations directed to printed matter are not entitled to patentable weight... Error! Bookmark not defined.</i>	
IV.	SHOWING OF ANALOGOUS PRIOR ART	5
A.	KALGI.....	5
B.	KHAN	5
C.	HAMMAD.....	6
D.	SMITH.....	7
E.	VARADARAJAN.....	8
F.	BAUER.....	8
G.	KRANZLEY	8
H.	ANALOGOUS ART	9
V.	GROUND 1: CLAIMS 19 AND 24 ARE OBVIOUS OVER KALGI, KHAN, AND VARADARAJAN	9
A.	CLAIM 19	9
1.	<i>19(pre): A method of performing an online payment transaction, the method comprising:</i>	<i>9</i>

2.	<i>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;</i>	<i>11</i>
	a) Khan’s Teachings.....	15
	b) Motivations to Combine.....	16
3.	<i>19(b): a displaying of the payment request notification at a touch-screen display user-interface of the electronic device; and,.....</i>	<i>17</i>
4.	<i>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;.....</i>	<i>18</i>
5.	<i>19(d): receiving, from a valid device user, a payment selection and authorization approval input on the electronic device;.....</i>	<i>20</i>
6.	<i>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</i>	<i>21</i>
	a) Varadarajan’s Teachings	23
	b) Motivations to Combine.....	24
7.	<i>19(f): combining said at least one limited-use numbers, with said selected account information, to form a complete payment information; and, ...</i>	<i>26</i>
8.	<i>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, ...</i>	<i>26</i>
9.	<i>19(h): receiving a user input providing for at least one transaction authorization actions, from a set of</i>	

	<i>actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method; and,.....</i>	<i>27</i>
10.	<i>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.</i>	<i>28</i>
B.	CLAIM 24	30
1.	<i>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.</i>	<i>30</i>
VI.	GROUND 2: CLAIMS 20 AND 22 ARE OBVIOUS OVER KALGI, KHAN, VARADARAJAN, AND HAMMAD.....	31
A.	CLAIM 20	31
1.	<i>20(a): The method of claim 19, further comprising:</i>	<i>31</i>
	<i>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</i>	<i>31</i>
a)	Varadarajan’s Teachings	31
b)	Hammad’s Teachings	32
c)	Motivation to Combine	33
2.	<i>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</i>	

	<i>transaction payment, and said device combining said current transaction sequence count at the instant of generating said cryptogram number.....</i>	34
B.	CLAIM 22	35
1.	<i>22(a): The method of claim 19, further comprising:</i>	35
	<i>generating a limited-use security code number for use in place of a card issuer card security code, by cryptographically combining information from at least one of a set of information comprising: a device transaction sequence counter; a device account number; a payment account information, device secrets; payment processing authority secrets; and.....</i>	35
2.	<i>22(b): displaying the limited-use security code number on the user-interface of the device display.</i>	35
VII.	GROUND 3: CLAIM 21 IS OBVIOUS OVER KALGI, KHAN, VARADARAJAN, AND SMITH.....	36
A.	CLAIM 21	36
1.	<i>21(a): The method of claim 19, wherein at least a portion of said limited-use number comprises a static device account number,.....</i>	36
	<i>and wherein the static device account number is of a limited scope of valid use to a specific device, ...</i>	36
a)	Smith's Teachings.....	37
b)	Motivation to Combine	39
2.	<i>21(b): 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:.....</i>	41
3.	<i>21(c): performing a payment transaction by the electronic device including the dynamically generated limited-use number;</i>	42

4. *21(d): combining the dynamically-generated number and the static device account number within a device-generated complete payment information; and 43*
5. *21(e): conveying said device-generated complete payment information, in place of a selected payment issuer information, when the device is performing payment transactions; and 43*
6. *21(f): 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. 44*

VIII. GROUND 4: CLAIM 25 IS OBVIOUS OVER KALGI, VARADARAJAN, AND SMITH 44

- A. CLAIM 25 44
1. *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:.....44*
 2. *25(a): accept a priming action of the electronic device by an identified valid device user, identified from the device inputs; 45*
 3. *25(b): enable the electronic device for imminent performance of a payment operation responsive to the priming action of said valid user; 47*
 4. *25(c): display a summary of online purchase information including the merchant information and the purchase amount; and, ...49*
 5. *25(d): display at least one selectable issuer payment account methods on a display; and, ...49*
 6. *25(e): receive a payment selection and approval authorization from said valid device user via a human input sensing at the device; and 49*
 7. *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, ... 50*

8. *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, ... 51*
9. *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 52*
10. *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. 52*

**IX. GROUND 5: CLAIMS 28-30 ARE OBVIOUS OVER
KALGI, KHAN, VARADARAJAN, HAMMAD AND
SMITH 54**

A. CLAIM 23 54

1. *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
payment issuer information; a payment processing
authority secrets; a transaction information; and, ... 54*
2. *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 55*
3. *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: 56*

	<i>a mis-matching of the transacted limited-use number; and the authority cryptographically-combined number;.....</i>	<i>57</i>
	<i>a transactional use of a device account number outside of its limited scope of valid payment reader facility use;</i>	<i>57</i>
	<i>a transactional use outside of a valid time window;</i>	<i>57</i>
	<i>a transactional re-use of a number limited to a one-time use; and, ...</i>	<i>57</i>
	<i>a transactional use of an expired number outside of a limited time-of-use.</i>	<i>57</i>
B.	CLAIM 28	58
1.	<i>28(a): The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further causes the one or more processors to perform:</i>	<i>58</i>
	<i>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, ...</i>	<i>58</i>
2.	<i>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, ...</i>	<i>59</i>
3.	<i>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, ...</i>	<i>59</i>
4.	<i>28(d): wherein the one or more device processors are further operable to transmit said complete payment information in place of said user-selected</i>	

	<i>payment account information in a device payment transaction; and,.....</i>	<i>59</i>
5.	<i>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.</i>	<i>59</i>
C.	CLAIM 29	60
1.	<i>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:</i>	<i>60</i>
	<i>a transaction sequence counter,.....</i>	<i>60</i>
	<i>a device account number,.....</i>	<i>60</i>
	<i>.....</i>	<i>60</i>
	<i>a payment processing authority secret, ...</i>	<i>60</i>
	<i>a user information, ...</i>	<i>60</i>
	<i>a payment account information, ...</i>	<i>60</i>
	<i>.....</i>	<i>60</i>
	<i>a payment amount, transactional information; and, ...</i>	<i>60</i>
2.	<i>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, ...</i>	<i>62</i>

3. *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, ...63*
4. *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, ...63*
5. *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, ...63*
6. *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. 63*
- D. CLAIM 30 64
 1. *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: 64*
a transaction sequence counter; 64
a user payment account number; 64
a device payment account number; 64

a device secret; device keys; 64
a payment issuer original account information; 64
a payment issuer device account information; 64
a payment processing authority secret; 64
a transaction information; 64
and a user private information; and, ... 64

2. *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, ... 65*
3. *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, ... 65*
4. *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, ... 65*
5. *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, ... 65*
6. *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. 65*

X. GROUND 6: CLAIM 26 IS OBVIOUS OVER KALGI, VARADARAJAN, HAMMAD, SMITH AND BAUER 66

A. CLAIM 26 66

1. *26(a). The non-transitory, computer-readable medium of claim 25, wherein the executable*

	<i>instructions further cause the one or more processors to:</i>	66
	<i>receive the priming action of a user via the device human input sensors;</i>	66
	<i>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:</i>	67
	<i>a correct passcode touch entry sequence,</i>	67
	<i>a correct touch gesture,</i>	67
		67
	<i>a biometric recognition of a valid user,</i>	67
		67
	<i>a security question which a valid user could answer correctly, and</i>	67
2.	<i>26(c): receiving a correct user response input, from a security challenge presented on the device display; and</i>	67
3.	<i>26(d): 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</i>	68
	a) Bauer’s Teachings	68
	b) Motivations to Combine	69
XI.	GROUND 7: CLAIM 27 IS OBVIOUS OVER KALGI, VARADARAJAN, HAMMAD, SMITH, AND KRANZLEY	70
A.	CLAIM 27	70
1.	<i>27(pre): 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:</i>	70
	a) Khan’s Teachings	70

b)	Motivation to Combine	71
2.	27(a): <i>cryptographically compute a dynamically generated one-time-use cryptogram number, ...</i>	72
3.	27(b): <i>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, ...</i>	72
4.	27(c): <i>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, ...</i>	72
5.	27(d): <i>wherein said transaction sequence counter, said information and said secrets are known to both said device, and to said payment processing authority; and, ...</i>	73
6.	27(e): <i>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, ...</i>	73
a)	Kranzley's Teachings.....	73
b)	Motivations to Combine.....	74
7.	27(f): <i>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,.....</i>	74
8.	27(g): <i>and transmitting said complete device payment information when said issuer payment account method is selected.</i>	75

XII. DISCRETIONARY CONSIDERATIONS	75
XIII. CONCLUSION	76
XIV. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8.....	77
A. REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1).....	77
A. RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2)	77
B. LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3)	77

I. INTRODUCTION

Apple Inc., (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 19-30 (“Challenged Claims”) of U.S. Patent No. 11,176,538 (“’538 Patent”).

II. THE ’538 PATENT

A. Description of the ’538 Patent

The ’538 Patent describes emulating a standard credit card with a device “capable of generating a programmed magnetic field of alternating polarity...when used in electronic credit card readers.” ’538 *Patent* (Ex. 1001), Abstract, 2:14-31. The ’538 Patent also describes “generating a limited-duration payment number...which is limited in scope of use to a predetermined number of authorized transactions.” *Id.*, 2:25-29. The electronic device is capable of using near field communications (“NFC”) to conduct a transaction using the limited-duration number. *Id.*, 2:42-62.

B. Field of Endeavor and Problem Solved by the Inventors

The ’538 Patent “generally relates to electronic or smart payment devices and, more specifically, to more secure, smart multi-function smart tokenizing electronic payment devices and transaction processing thereof.” ’538 *Patent*, Abstract, 2:25-29. Therefore, the field of endeavor at least includes electronic or smart payment devices. *Dec.*, ¶¶84-85.¹

¹ Citations to “*Dec.*” are to Exhibit 1003, Declaration of Dr. Neuman.

The '538 Patent's particular problem with which the invention is involved is the security of payment transactions between electronic devices. '538 *Patent*, 1:63-2:4; *Dec.*, ¶¶86-87. The '538 Patent notes existing devices are “susceptible to theft and/or compromise” and, therefore, “have security limitations” and are further “incompatible with existing credit card infrastructure[.]” *Id.*, 1:63-2:4. Accordingly, the '538 Patent proposes to solve this problem by using “a limited-duration payment number for performing transactions using accounts of the card.” *Id.*, 10:22-26, 12:40-45.

C. Priority and Prosecution History

The '538 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. Because the '538 Patent claims the benefit of a filing date before March 16, 2013, Petitioner applies the pre-AIA versions of §§ 102, 103. For this proceeding, Petitioner applies March 15, 2013 as the priority date for the Challenged Claims.² Unless noted, the below analysis would not change under the AIA.

² Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Unless specifically noted, the analysis presented in this petition remains the same regardless of whether March 15, 2013, or some later date is used as the Critical Date.

After filing, Applicant canceled claims 1-20 and added new claims 23-50. '538 *File History* (EX1002), 92-11. The '538 Patent did not face any prior art rejections during prosecution. *See generally id.*

D. Level of Skill of a POSITA

A POSITA at the time of the '538 Patent would have had a bachelor's degree in computer science, computer engineering, electrical engineering or the equivalent, and one or two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless and online technologies. *Dec.*, ¶¶28-30. Additional industry experience or technical training may offset less formal education, while advanced degrees or additional formal education may offset lesser levels of industry experience. *Id.*

III. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies the '538 Patent is eligible for IPR.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b)

The Challenged Claims are unpatentable on the following grounds under 35 U.S.C. § 103:

Ground	Claim(s)	References
1	19, 24	Kalgi (EX1004), Khan (EX1005), Varadarajan (EX1006)
2	20, 22	Kalgi, Khan, Varadarajan, Hammad (Ex. 1007)
3	21	Kalgi, Khan, Varadarajan, Smith (EX1008)
4	25	Kalgi, Varadarajan, Smith

5	23, 28-30	Kalgi, Khan, Varadarajan, Hammad, Smith
6	26	Kalgi, Varadarajan, Hammad, Smith, Bauer (EX1009)
7	27	Kalgi, Varadarajan, Hammad, Smith, and Kranzley (EX1010)

The earliest claimed priority date of the '538 Patent is March 15, 2013 (the “Critical Date”). Each of the prior art references applied in this Petition qualifies as prior art to the '538 Patent as shown:

Reference	Filed	Published	Prior Art Basis
Kalgi	7/5/2012	1/10/2013	§102(a)/(e)
Khan	9/28/2012	1/16/2014	§102(e)
Varadarajan	1/25/2011	7/28/2011	§102(b)
Hammad	6/18/2007	6/22/2010	§102(b)
Smith	11/17/2009	5/20/2010	§102(b)
Bauer	9/28/2011	4/5/2012	§102(a)/(e)
Kranzley	6/1/2009	5/20/2010	§102(b)

None of these references were cited or discussed during prosecution of the '538 Patent.

C. Claim Construction Under 37 C.F.R § 42.104(b)(3)

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). For purposes of this

proceeding, Petitioner applies the plain and ordinary meaning of all claim terms as understood by a POSITA.³

Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board.

IV. SHOWING OF ANALOGOUS PRIOR ART

A. Kalgi

Kalgi teaches methods and systems for electronic purchase transactions, including transactions via a web browser. *Kalgi*, Abstract, [0003], [0028]. Kalgi describes use of an electronic wallet checkout platform that supplies a consistent user experience across websites. *Id.*, [0027]-[0028]. To initiate a transaction, the user must be authorized and select a payment type. *Id.*, Abstract, [0029], [0043], [0057], [0059], Figs. 1, 5.

B. Khan

Khan teaches commercial transactions between a portable device and a transaction provider in a wireless environment. *Khan*, [0002], [0018], [0021], Figs. 2-4. The portable device generates credit card data, including an alias card number,

³ Petitioner's application of prior art to the Challenged Claims is not a waiver of any argument in litigation that any claim is indefinite, invalid, or requires claim construction.

cryptographic data, a counter, merchant ID, etc. *Id.*, [0022]-[0024], [0028]. This information is sent to a backend server that validates the credit card data. *Id.*, [0025], [0028], Figs. 2, 4.

C. Hammad

Hammad teaches methods and systems for generating verification values on a portable consumer device for use in payment transactions. *Hammad*, 2:10-20, 2:65-3:11. The dynamically generated verification values, which are embedded in payment data sent to a service provider, are generated using two or more dynamic data elements and static data elements. *Id.*, 4:21-6:42.

Hammad claims priority to, and “incorporate[s] by reference in their entirety for all purposes[,]” three U.S. Provisional Applications. *Hammad*, 1:7-13; *see Konda v. Flex Logix Techs., Inc.*, 2022 WL 1436144, at *3 (Fed. Cir. May 6, 2022) (citing 37 C.F.R. § 1.14(a) and M.P.E.P. § 103(VII) to hold a “provisional application became publicly available when the [publication which incorporated it by reference] was published”); *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (“Material not explicitly contained in the single, prior art document may still be considered for purposes of anticipation if that material is incorporated by reference into the document.”). U.S. Provisional Application No. 60/884,089 (“Hammad ’089 Provisional”) describes the use of dCVVs similar to that disclosed in Hammad. EX1011, [0035]-[0042].

D. Smith

Smith teaches a “mobile PAN” for a “mobile device” from which a “user may “request the issuance of a payment account such that the payment account is accessible using a mobile device 104 associated with a customer.” *Smith*, [0014].

Whenever a user wishes to open a payment account, the issuer issues a “temporary PAN...and establishes any risk parameters (e.g., for use in controlling the authorization of transactions involving the temporary PAN)” so the user is able to make purchases while awaiting an actual PAN. *Smith*, [0014]-[0016], [0026]. This “temporary PAN is mapped to a mobile PAN (e.g., such as a PayPass® PAN, or PPAN).” *Smith*, [0026]. The mobile PAN/PPAN is “assigned to the mobile device 104.” *Smith*, [0016].

600

CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE

FIG. 6

Smith, Fig. 6, [0023] (the PPAN is associated with a “related PAN[.]”). The mobile PAN is “stored in the mobile device 204.” *Smith*, [0022]. Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith*, [0026], [0040].

E. Varadarajan

Varadarajan teaches financial transactions between an application on a mobile device and a transaction provider. *Varadarajan* at Abstract, [0026]. The application generates a dynamic card value (“DCV”) that replaces traditional static values, such as CVC, CVV, PAN, or account numbers. *Varadarajan*, [0012], [0021]. The DCV is derived from device-derived information. *Varadarajan*, [0029], [0053]. The DCV is limited in use to one or a specified time. *Varadarajan*, [0023].

F. Bauer

Bauer teaches methods and systems for using and authorizing a mobile payment account on a portable electronic device. *Bauer*, Abstract, [0001], [0019]. Bauer describes use of an electronic wallet that includes data for payment accounts for completing a transaction. *Id.*, [0019]-[0021]. To access the wallet and conduct a transaction, the user must be authenticated, e.g., through providing a PIN. *Id.*, [0084]-[0091], Figs. 9a-b, 10a-f.

G. Kranzley

Kranzley teaches methods and system for conducting payment transactions with a mobile device over a network. *Kranzley*, Abstract, [0010]. The mobile device

has an application stored thereon which, during a transaction generates a static VPAN, VPAN expiration date, and dynamic data, that is sent to a payment network for authorization. *Id.*, [0029], [0035]-[0042], Fig. 1B.

H. Analogous Art

Each of the applied prior art references discloses conducting secure payment transactions and is in the same field of endeavor as the '538 Patent. *Compare '538 Patent*, Abstract, 1:24-28, Fig. 1 *with Kalgi*, Abstract, [0027]-[0030], Fig. 1; *Khan*, [0002], [0018]-[0021], Figs. 2-4; *Hammad*, Abstract, 2:12-20, Fig. 6 *and Hammad '089 Provisional*, [0002]-[0003]; *Smith*, Abstract, [0021]-[0023], Fig. 1; *Varadarajan*, Abstract, [0002]-[0020], Fig. 1; *Bauer*, Abstract, [0001], [0019]-[0021]; *Kranzley*, Abstract, [0010], Figs. 1B, 3; *Dec.*, ¶¶90-112.

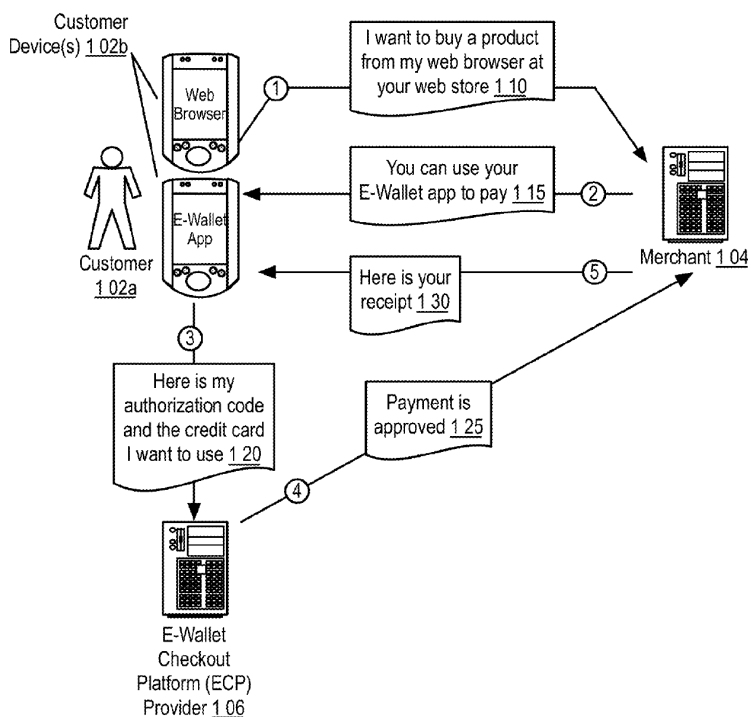
Further, each of the applied prior art references is reasonably pertinent to problems addressed by the '538 Patent such as increasing security of payment transactions. *Compare '538 Patent*, 1:24-28, 1:63-2:4, 9:21-28 *with Kalgi*, [0027]; *Khan*, [0002], [0004]-[0005]; *Hammad*, 1:17-2:6 *and Hammad '089 Provisional*, [0002], [0036]; *Smith*, [0002], [0015], [0020]; *Varadarajan*, [0005], [0009]-[0010]; *Bauer*, [0003]-[0006], [0009]-[0010]; *Kranzley*, [0003]; *Dec.*, ¶¶90-112.

V. GROUND 1: CLAIMS 19 AND 24 ARE OBVIOUS OVER KALGI, KHAN, AND VARADARAJAN

A. Claim 19

- 1. 19(pre): A method of performing an online payment transaction, the method comprising:**

Kalgi teaches “apparatuses, methods, and systems for electronic purchase transactions,” including transactions where “a customer 102a may wish to purchase a product and/or service 110 from a merchant 104 via a web browser (e.g., at the merchant’s website).” *Kalgi*, [0003], [0028].



Kalgi, Fig. 1.

“For example, the customer may be shopping online for an item at the merchant’s website, via consumer device 102b.” *Id.*, [0028], [0033], [0062], [0066], [0083]. *Kalgi* teaches an electronic wallet checkout platform (EWCP) that enables the customer to “engage in a purchase transaction via a secure platform that may

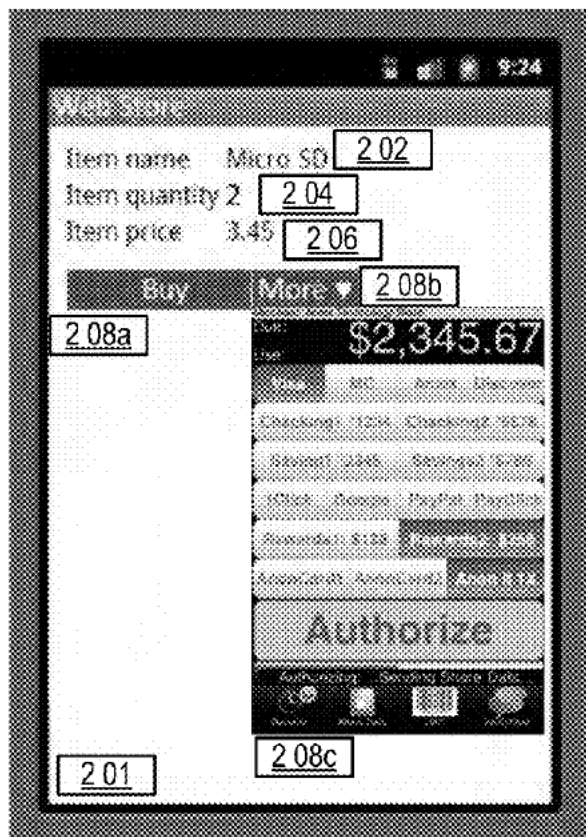
provide a consistent user experience across merchant websites.” *Id.*, [0027]. Thus, Kalgi teaches a method of performing an online payment transaction.⁴

2. ***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;***

Kalgi teaches “a customer may visit a merchant’s website using a mobile device (e.g., a cell phone, a PDA, a tablet, and/or the like).” *Kalgi*, [0034]; *see also*, *id.*, [0027], [0028], Fig. 2. The customer’s mobile device is an electronic device.

Kalgi further teaches a “mobile EWCP application” running on the mobile device to facilitate transactions with the website. *Kalgi*, [0034]-[0036], Fig. 1; *see also*, [00142]-[0143], Figs. 18-19B. “The customer may wish to purchase two 204 Micro SD cards 202 at a price 206 of \$3.45 each” and “may click the ‘Buy’ button 208 a to purchase these items.” *Id.*, [0034].

⁴ Claim language identified with *italics* and underline.



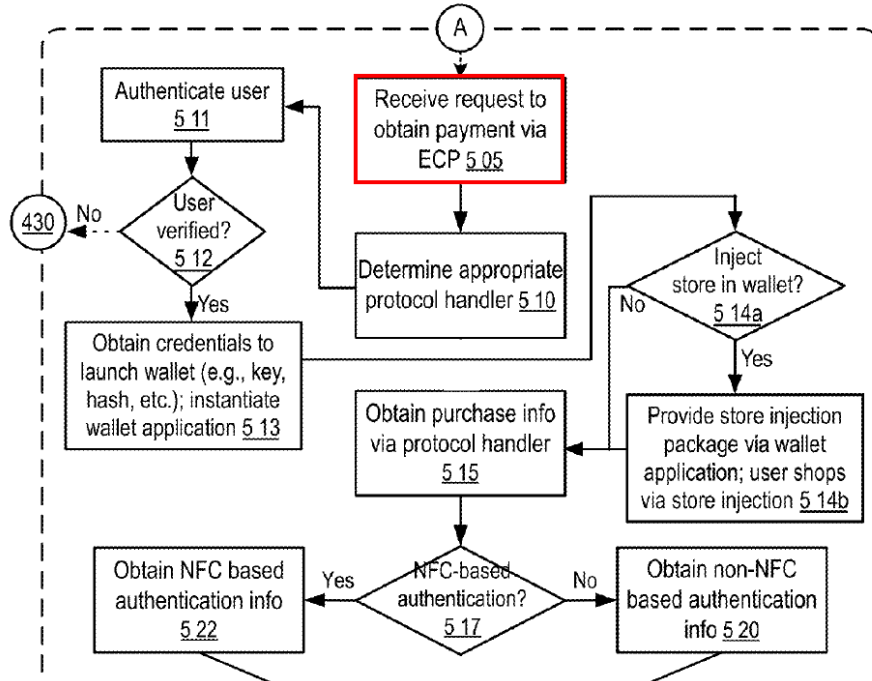
Kalgi, Fig. 2 (excerpt).

After the user indicates that he or she wishes to purchase the items, the mobile EWCP application running on the mobile device “detect[s] that the merchant’s website uses an EWCP-supported protocol” using the method described with regard to Figure 5. *Id.*, [0034]; *see also*, Abstract.

As shown in Figure 5, “a request to obtain payment via EWCP may be received at 505.” *Id.*, [0051]; *see also* Fig. 5. “For example, an EWCP browser extension may detect that a merchant’s webpage is using an EWCP-supported protocol (e.g., by determining existence of a protocol string starting with

‘ewalletcheckout://’, ‘specialcheckout://’, ‘specialwallet://’, and/or the like) to request payment from a user.” *Id.*, [0051]; *see also*, [0039]-[0040], [0047]-[0048].

FIGURE 5
Receive a Request for Payment of an Online Payment Transaction by said Electronic Device



Kalgi, Fig. 5 (annotated excerpt).

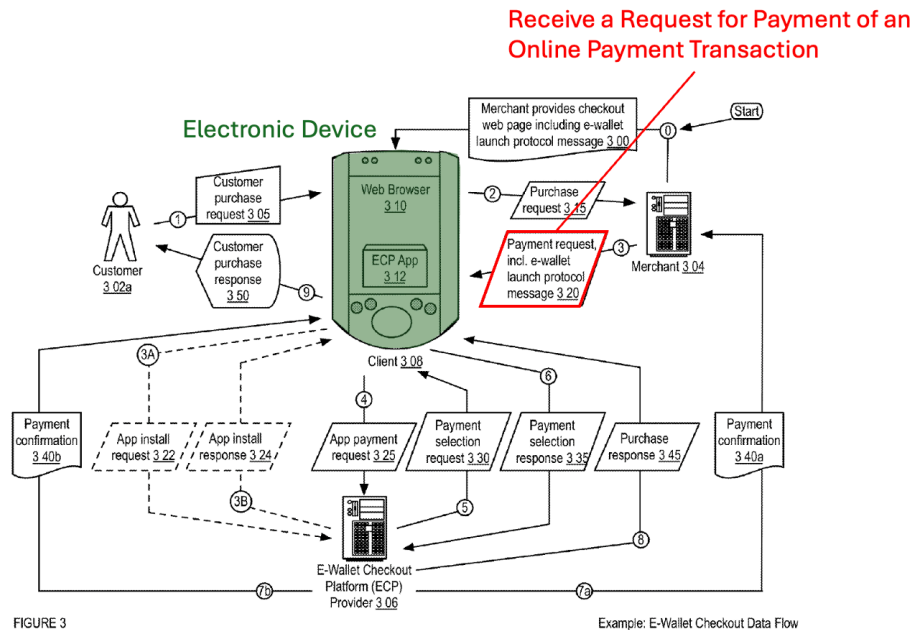


FIGURE 3

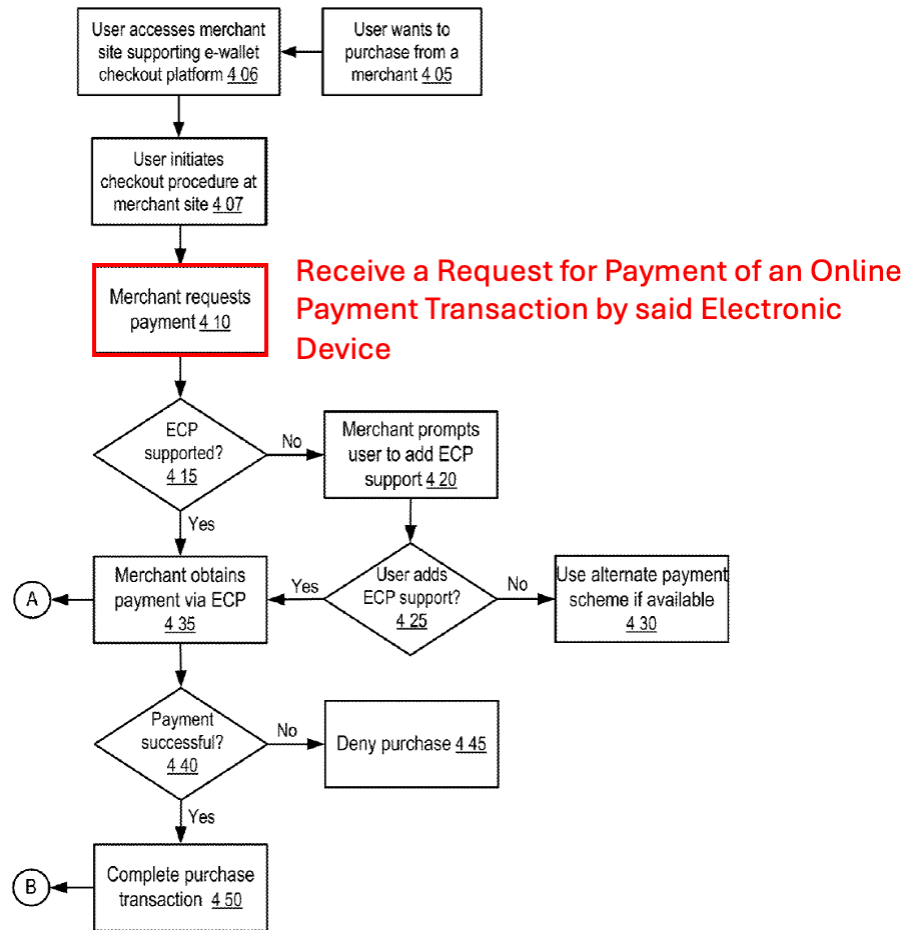
Example: E-Wallet Checkout Data Flow

Kalgi, Fig. 3 (annotated).

Thus, the mobile device receives a protocol string, which is *an input signal corresponding to a request for payment of an online payment transaction by said electronic device.*

The merchant's server may generate a payment request (including the protocol string) and send to the mobile device over a network. *Kalgi*, [0047], [0066], [0068]. A server is a computer that “processes and responds to the requests of remote users across a communications network[,]” including “Wireless Networks.” *Id.*, [0150]; *see also*, Figs. 1, 3, 7. Similarly, the user may communicate with a point-of-sale terminal via “Wi-Fi[.]” *Id.*, [0068], [0084].

A POSITA would have understood that mobile devices, such as *Kalgi*'s smartphone, access a merchant's website via WiFi or cellular data networks, i.e., wireless networks. *See Kalgi*, [0034], [0067]-[0068]. Indeed, a wireless interface would be required for a user and merchant website (or PoS terminal) to communicate wirelessly, as described by *Kalgi*. *Dec.*, ¶121. Thus, a POSITA would have understood that *Kalgi*'s mobile device includes a wireless interface. *Id.*



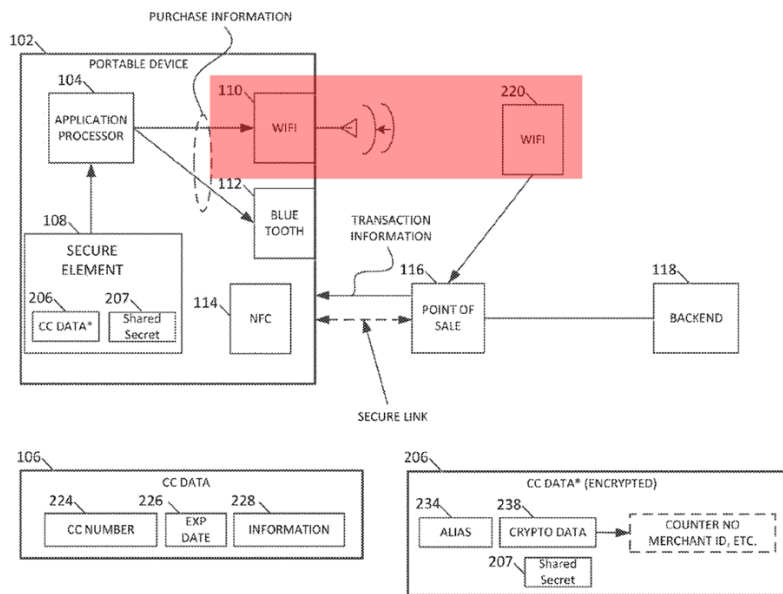
Kalgi, Fig. 4 (annotated).

Alternatively, it would have been obvious to a POSITA to configure Kalgi's mobile device to receive the protocol string via a wireless interface. *Dec.*, ¶122.

a) Khan's Teachings

Khan teaches a similar method of performing online payment transactions using a portable device. *Khan*, [0002], [0006], [0018], [0021]-[0024], [0028], Figs. 2, 4. The portable device includes one or more interfaces, including a WIFI interface. *Id.*, [0018]. "[P]urchase information[,]" such as an alias of a credit card number and

crypto data, are “transferred through the WIFI interface” on the portable device. *Id.*, [0021].



Id., Fig. 2 (annotated). Khan further teaches that its portable device can make mobile payments online, which are authorized by a backend server. *Id.*, [0028], Fig. 4. Thus, Khan teaches a mobile device that communicates payment information via a wireless interface.

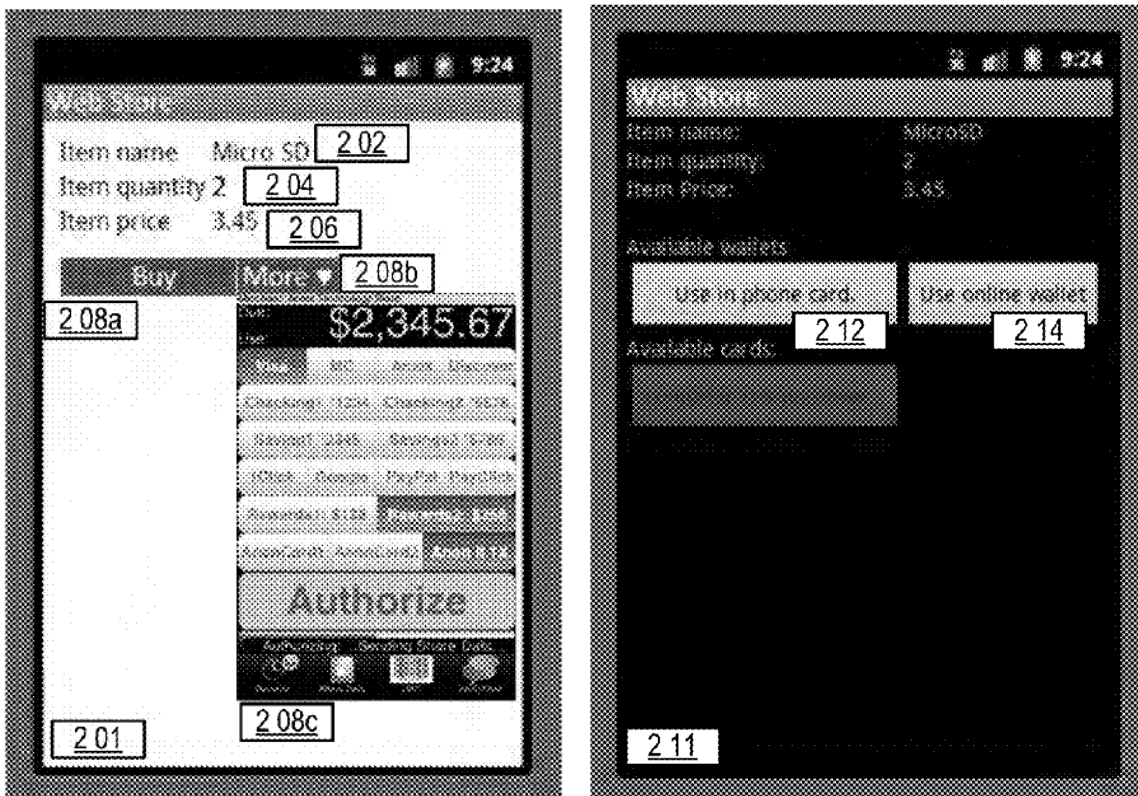
b) Motivations to Combine

It would have been obvious and a POSITA would have been motivated to incorporate a wireless interface, such as Khan’s WIFI interface, so that the mobile device receives a payment request wirelessly. *Dec.*, ¶124. A POSITA would have understood that a mobile device, such as a smartphone, would have a wireless interface to access the internet. *Id.* Thus, a POSITA would have been motivated to

combine prior art elements of Kalgi's mobile device with Khan's WIFI interface to predictably enable Kalgi's mobile device to communicate via wireless networks for online transactions, as Kalgi already describes. *Id.* Given the ubiquity of mobile devices having wireless interfaces, there would have been a reasonable expectation of success configuring Kalgi's mobile device to receive the request via the device's wireless interface. *Id.*

3. *19(b): a displaying of the payment request notification at a touch-screen display user-interface of the electronic device; and,*

Kalgi teaches that the user provides inputs via a touch screen display user interface of the electronic device. Kalgi, [0039], [0062], [0067], [0083], [0113]. After the payment request is received, the user is prompted "to use an EWCP electronic wallet (hereinafter 'E-Wallet' or 'wallet application') to facilitate payment." *Id.*, [0029]. Specifically, the user is "prompted to select an available wallet[,]" such as illustrated on the touchscreen display of screen 211. *Id.*, [0036], Fig. 2; *see also*, [0040] ("The payment request may prompt the customer to provide payment information to pay for the item."). Thus, the screen 211, which prompts the user to select a displayed wallet to perform the payment transaction, serves as a payment request notification.

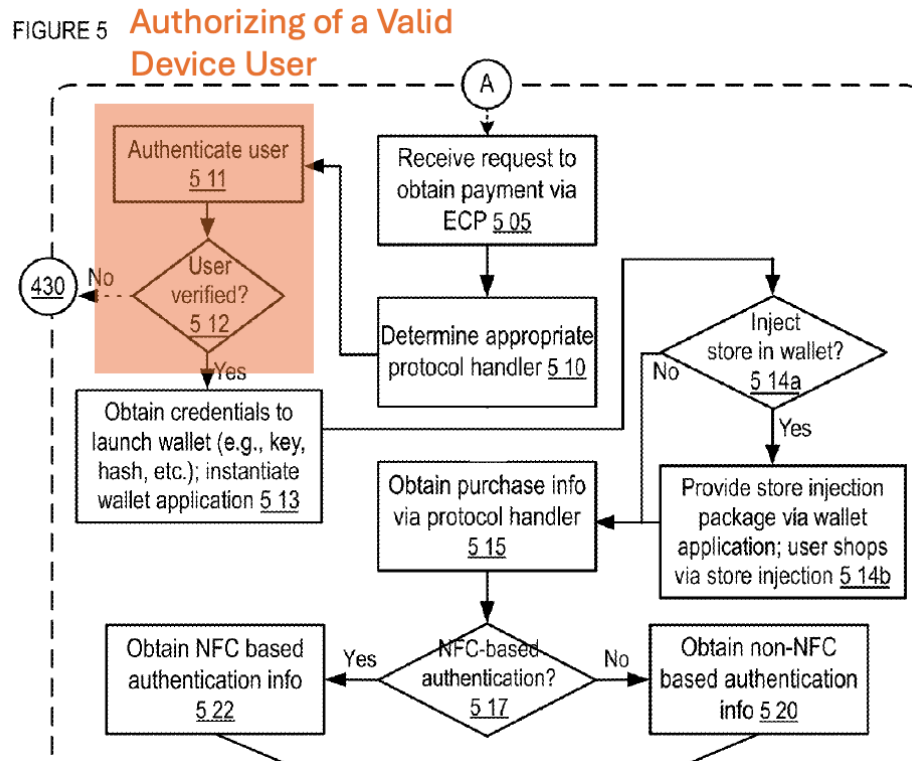


Kalgi, Fig. 2 (excerpts).

4. ***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;***

Kalgi teaches the user must be authorized as a valid device user to launch the wallet application. Kalgi, [0029] (“The customer may be asked to provide authentication and/or authorization information to use the E-Wallet.”), [0036] (“the ‘Buy’ button 208a may trigger the launch of an E-Wallet application and the application may be instantiated.”), [0051], [0054]-[0055], [0067], [0083]. “[T]he user may be required to enter login information, answer a challenge question, submit

a voice/biometric signature, provide a digital certificate, enter into a video call for verification purposes, and/or the like.” *Id.*, [0051].



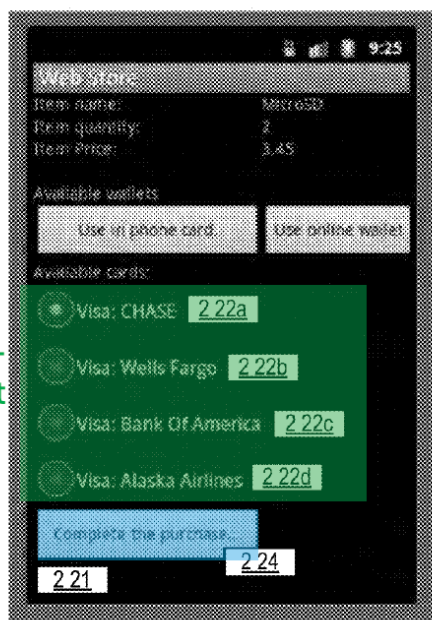
Kalgi, Fig. 5 (annotated excerpt).

Figure 2 (screen 221) displays “a choice of payment methods 222a-222d (e.g., credit cards, debit cards, gift cards, and/or the like) available in the wallet selected by the customer.” *Id.*, [0037], Fig. 2; *see also*, [0035], [0036] (“[U]pon authentication and/or authorization to use the E-Wallet, the customer may be prompted to select an available wallet. In one embodiment, the customer may select a wallet stored on the mobile device 212[.]”). Thus, displaying the list of payment methods 222a-222d on screen 211 is displaying at least one user-selectable payment account option, via the touchscreen display user-interface.

“Upon selecting a payment method (e.g., 222a), the customer may use the ‘Complete the purchase ...’ button 224 to submit payment information.” *Id.*, [0037]. Thus, Kalgi teaches requesting a user approval of payment (i.e., prompting the user to “Complete the purchase” via button 224), via the touchscreen display user-interface.

Displaying at Least One User-Selectable Payment Account Option

Requesting a User Approval of Payment



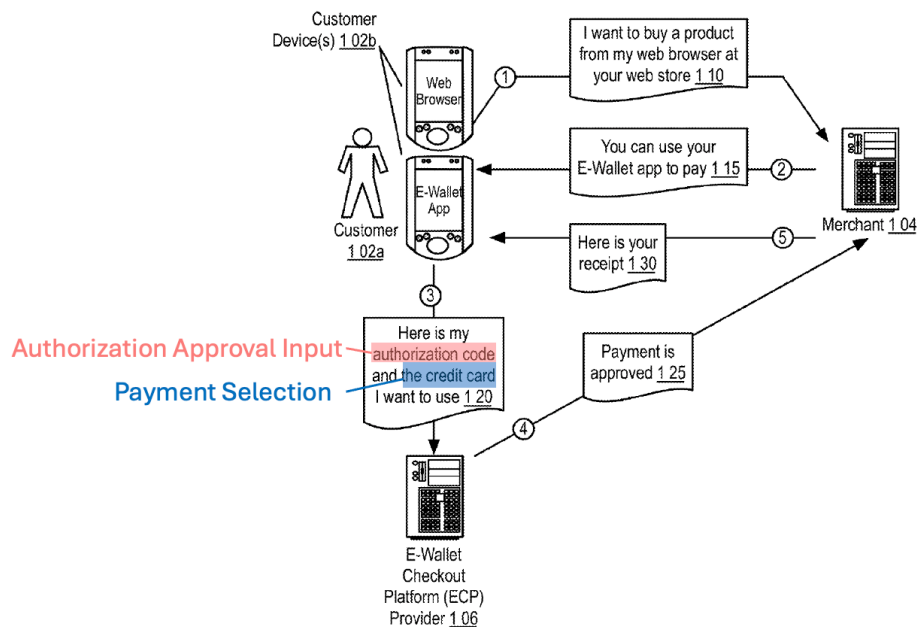
Kalgi, Fig. 2 (annotated excerpt).

5. 19(d): receiving, from a valid device user, a payment selection and authorization approval input on the electronic device;

Kalgi teaches the valid device user “provide[s] a selection of a payment method (e.g., a specific credit card) 120” on the electronic device. Kalgi, [0029], Fig. 1; *see also*, [0057]. The “user may provide a wallet access input ... into the user wallet device” through a touchscreen interface. *Id.*, [0039], [0062], [0067], [0083]. The user must also provide “authentication and/or authorization information”

specific to the selected payment method, such as “a payment method security code.”

Id., [0029], [0043], [0059], Figs. 3, 5. Thus, Kalgi teaches receiving, from a valid device user, a payment selection and authorization approval input on the electronic device.



Kalgi, Fig. 1 (annotated).

6. **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**

Kalgi teaches a user providing a credit card and authorization code to complete a purchase. *Kalgi*, [0029], [0059], Fig. 1. Kalgi additionally teaches that its EWCP includes a User Purchase Checkout and Purchase Transaction Authorization component. *Kalgi*, [0066]-[0092], Figs. 9A-10B. In this context, a user may purchase a product from a merchant’s online site by communicating with

the merchant's PoS client or server. *Id.*, [0062], [0066], [0083], Figs. 9A-10B. When using the E-Wallet, the user provides payment information to the merchant, including an account number, account name, account address, CVV (static or dynamic), and other information, in a compatible data form. *Id.*, [0068]-[0069], [0084].

```

<?XML version = "1.0" encoding = "UTF-8"?>
<transaction_authorization_input>
  <payment_data>
    <account>
      <charge_priority>1</charge_priority>
      <charge_ratio>40%</charge_ratio>
      <account_type>debit</account_type>
      <value_exchange_symbol>USD</value_exchange_symbol>
      <account_number>123456789012345</account_number>
      <account_name>John Q. Public</account_name>
      <bill_add>987 Green St #456, Chicago, IL 94652</bill_add>
      <ship_add>987 Green St #456, Chicago, IL 94652</ship_add>
      <CVV_type>dynamic<CVV_type>
      <CVV>http://www.paynet.com/dcvv.php?sessionID=4NFU4RG94</CVV>
      <cloak_flag>ON</cloak_flag>
      <alert_rules>tar1 tar4 tar12</alert_rules>
      <mode>NFC</mode>
    </account>
    <account>
      <charge_priority>1</charge_priority>
      <charge_ratio>60%</charge_ratio>
      <account_type>rewards</account_type>
      <value_exchange_symbol>VME</value_exchange_symbol>
      <account_number>234567890123456</account_number>
      <account_name>John Q. Public</account_name>
      <bill_add>987 Green St #456, Chicago, IL 94652</bill_add>
      <ship_add>987 Green St #456, Chicago, IL 94652</ship_add>
      <CVV_type>static<CVV_type>
      <CVV>173</CVV>
    </account>
  </payment_data>
</transaction_authorization_input>

```

```

    <cloak_flag>ON</cloak_flag>
    <alert_rules>tar1 tar4 tar1 2</alert_rules>
    <mode>Bluetooth</mode>
  </account>
  <account>
    <charge_priority>2</charge_priority>
    <charge_ratio>100%</charge_ratio>
    <account_number>345678901234567</account_number>
    <account_type>credit</account_type>
    <value_exchange_symbol>USD</value_exchange_symbol>
    <account_name>John Q. Public</account_name>
    <bill_add>987 Green St #456, Chicago, IL 94652</bill_add>
    <ship_add>987 Green St #456, Chicago, IL 94652</ship_add>
    <CVV_type>static<CVV_type>
    <CVV>173</CVV>
    <cloak_flag>ON</cloak_flag>
    <alert_rules>tar1 tar4 tar1 2</alert_rules>
    <mode>NFC</mode>
  </account>
</payment_data>

```

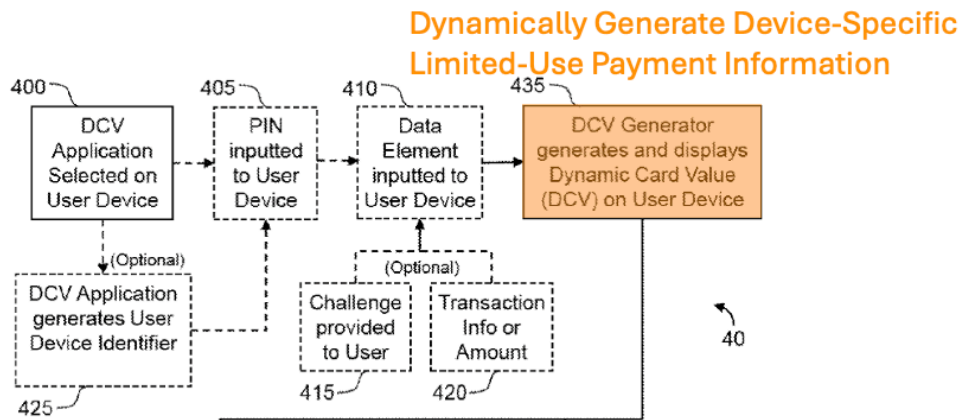
Kalgi, [0069] (annotated).

This information is subsequently transmitted for payment processing. *Id.*, [0070]-[0081], [0085]-[0092], Figs. 9A-10B.

a) Varadarajan's Teachings

Varadarajan teaches a similar mobile payment application on a mobile device. *Varadarajan*, [0011], [0032], [0038]-[0039], [0041]. Specifically, a “user downloads the DCV application to his mobile user device, which can be virtually any hand-held platform[,]” including smart phones. *Varadarajan*, [0026]. The DCV application generates a dynamic card value (DCV), which is used to replace a static value, such as a CVV and/or PAN. *Id.*, [0012], [0022] (describing “both a dynamic PAN and a dynamic CVV may be generated for use in the same transaction”), [0023], [0045], [0056]. The DCV can be a 3 or 4-digit number when replacing a CVV or sixteen-digit number when replacing a PAN. *Id.*, [0021], [0031]. “The DCV

is configured and provided in the same form as the static DCV for which it is being substituted.” *Id.*, [0021].



Varadarajan, Fig. 4 (annotated excerpt).

The DCV can be input to a transaction interface, which can be an online transaction, such as an online shopping cart. *Id.*, [0011], [0021], [0029]-[0030], [0042], [0045], Fig. 4.

The DCV is *limited-use* in that it expires “after a limited number of uses, which may be a single use[.]” *Id.*, [0023], [0020], [0047]. *Dec.*, ¶134.

Thus, Varadarajan’s DCV is at least one limited-use number that is dynamically generated at the device for using ... in place of at least a portion of said selected issuer payment information (e.g., the PAN or CVV, etc.).

b) Motivations to Combine

It would have been obvious and a POSITA would have been motivated to configure Kalgi’s device processor to dynamically generate a DCV or PAN to be

used in place of at least a portion of the selected issuer payment account information responsive to receiving a valid user transaction payment approval. *Dec.*, ¶¶136-137. A POSITA would have understood that Kalgi's device could be vulnerable to attacks where the issuer provided account information (e.g., PAN) is intercepted by an attacker and used for fraudulent transactions. *Dec.*, ¶136. Indeed, Varadarajan recognizes security vulnerabilities" associated with "[c]ard based transactions," including online transactions. *Varadarajan*, [0003], [0005], [0009]-[0010]; *Dec.*, ¶136. Thus, to prevent fraud, a POSITA would have been motivated to configure Kalgi to implement Varadarajan's method of dynamically generating a DCV to be used in place of a PAN or CVV to improve similar mobile payment systems in the same way for online transactions. *Dec.*, ¶136. The concept of dynamic CVVs and PANs was well-known and a POSITA would have been familiar with using such numbers in connection with payment transactions. *Id.* Substitution of Kalgi's CVV or PAN with Varadarajan's DCV is utilizing known techniques to improve similar devices that would have predictably increased the security of Kalgi's payment system and further protected the user's account information. *Id.*

A POSITA would have had a reasonable expectation of success in modifying Kalgi in this way because Kalgi already uses dynamic CVVs in a transaction. *Dec.*, ¶137. Thus, a POSITA would have recognized that modifying Kalgi according to the teachings of Varadarajan required only basic software modifications and routine

skill. *Id.* As such, the modification would have been a combination of known elements that would yield predictable results of generating dynamic account information, such as CVVs, to increase transaction security. *KSR*, 550 U.S. at 415-421; *Id.*

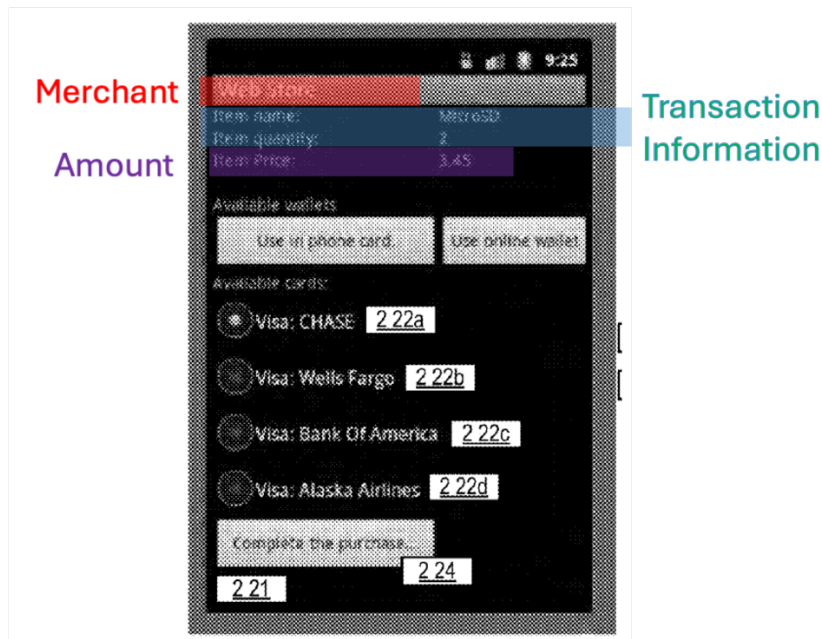
7. *19(f): combining said at least one limited-use numbers, with said selected account information, to form a complete payment information; and,*

As described in Claim 19(e), it would have been obvious to a POSITA to modify Kalgi's mobile device to generate a DCV for use in place of the CVV and/or PAN. *See* Claim 19(e); *Dec.*, ¶138. Kalgi teaches that the user wallet device provides payment information, such as name, address, CVV (static and dynamic), and account number, to a merchant. *Kalgi*, [0069]. Thus, it would have also been obvious to combine the DCV (*said at least one limited-use numbers*) with selected account information in Kalgi's payment data *to form a complete payment information* for the same reasons. *Dec.*, ¶138.

8. *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,*

If this limitation is entitled to patentable weight (*see* Section III.C), as discussed in Claim 19(d), Kalgi teaches receiving authentication and/or authorization information (*a user payment approval authorization*) though the user-

interface of the electronic device. *See* Claim 19(d). Kalgi also teaches displaying the payment request, including merchant, amount, and transaction information. Kalgi, Fig. 2.

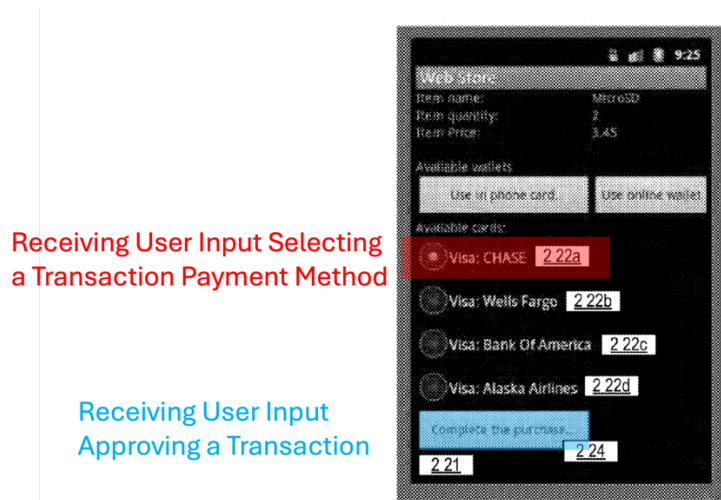


Kalgi, Fig. 2 (annotated excerpt).

9. ***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,***

As discussed above, Kalgi's mobile device receives a user input for approving a transaction and selecting a transaction payment method. *See* Claims 19(c)-(d). Specifically, the mobile device receives approval of a transaction when the user presses "the 'Complete the purchase ...' button 224 to submit payment information."

Kalgi, [0037]. The mobile device also receives a selection of the payment method.
Id.; *see also*, [0029], [0035], [0042]-[0043].



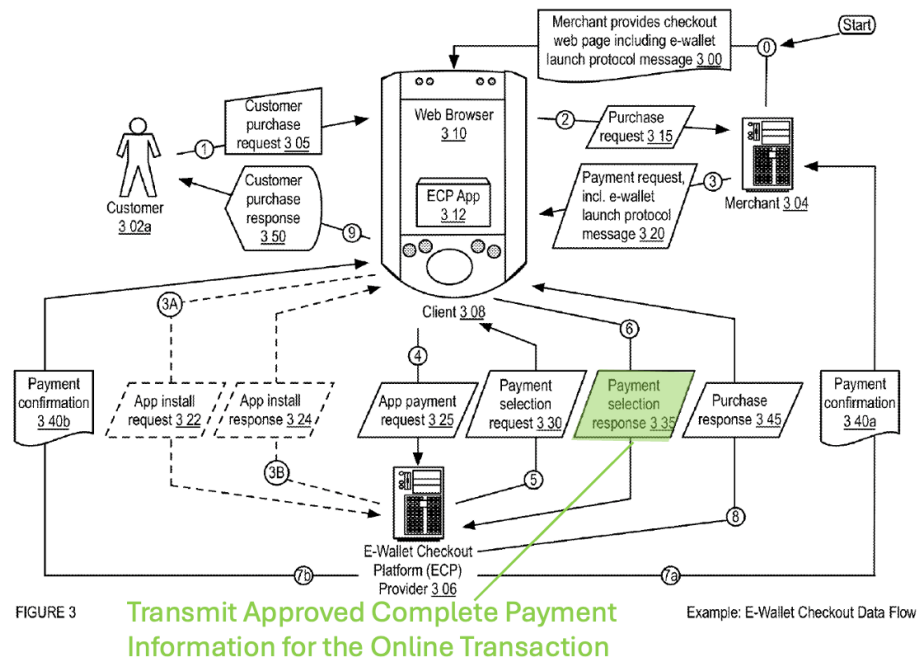
Kalgi, Fig. 2 (annotated excerpt).

10. 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.

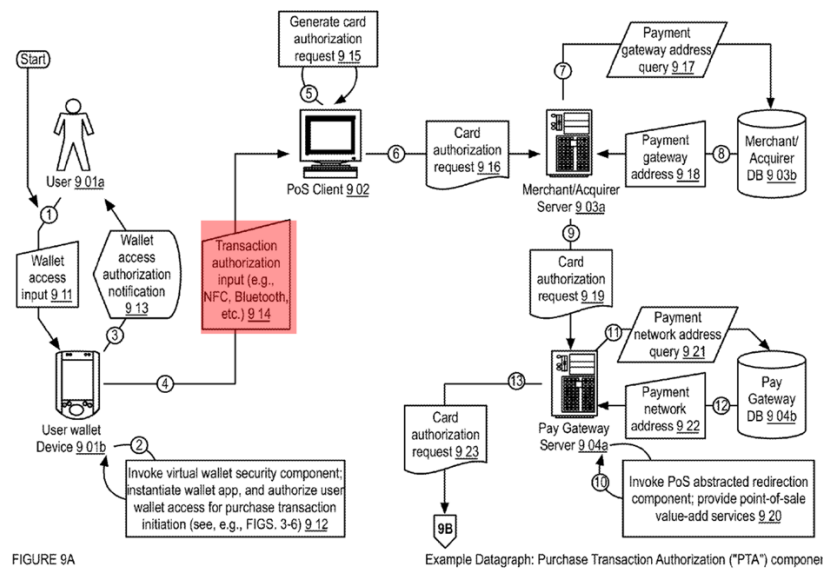
As discussed, *Kalgi* teaches receiving user payment approval authorization input via button 224, which causes the mobile device “to submit payment information.” *See* Claim 19(h); *Kalgi*, [0037], Fig. 2. Specifically, the mobile device transmits “a payment selection response 335 to the EWCP provider.” *Id.*, [0043], [0055], [0069], [0084], Figs. 1, 3, 9A, 10A.

For the reasons discussed above, it would have been obvious to a POSITA to enable *Kalgi*’s mobile device communicate via the wireless interface. *See* Claim 19(a); *Kalgi*, [0067]-[0068], [0083]-[0084]; *Dec.*, ¶142. For the same reasons, it

would have been obvious to enable Kalgi's mobile device to transmit the payment selection response including the approved complete payment information for the online transaction to the EWCP provider the wireless interface. *Id.*; see also Claims 19(e)-(f); Dec., ¶142.



Kalgi, Fig. 3 (annotated).



Kalgi, Fig. 9A (annotated), Fig. 10A.

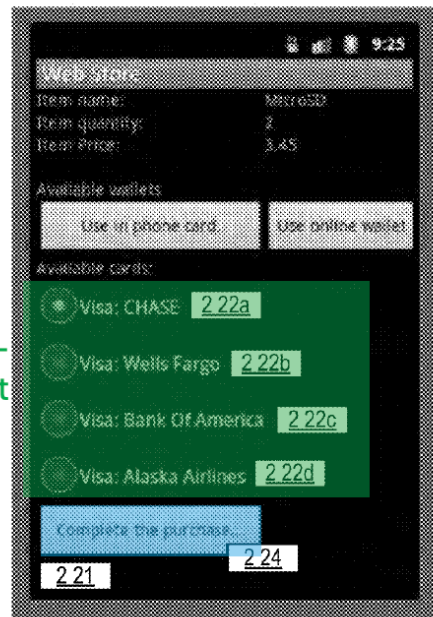
B. Claim 24

- 1. 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.**

As discussed above, Kalgi teaches that the user provides inputs via a touch screen display user interface of the electronic device. Kalgi, [0039], [0062], [0067], [0083], [0113]; *see also*, Claim 19(b). Fig. 2 also depicts a screen shown on the touchscreen display where a user selects a payment method via a touch input selection. *See* Claim 19(c); Kalgi, [0037].

Displaying at Least One User-Selectable Payment Account Option

Requesting a User Approval of Payment



Kalgi, Fig. 2 (annotated excerpt).

VI. GROUND 2: CLAIMS 20 AND 22 ARE OBVIOUS OVER KALGI, KHAN, VARADARAJAN, AND HAMMAD

A. Claim 20

1. 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

a) Varadarajan's Teachings

Varadarajan teaches that the DCV, when used to replace the CVV, is a three-digit number. *Varadarajan (EX1006)*, [0021]. The DCV is generated using an ARQC generating algorithm in compliance with EMV standard protocol.

Varadarajan (EX1006), [0051]. A POSITA would understand that these algorithms generate cryptograms and that a DCV/dCVV are a cryptogram. *Dec.*, ¶141. The DCV/dCVV passes along with any other payment data to the authenticating server. *Varadarajan (EX1006)*, [0011], [0027], [0045], [0056].

b) Hammad's Teachings

Hammad teaches dynamically generating a dCVV (cryptogram number) using an application on a mobile device for use in a mobile payment transaction. *Hammad*, 2:65-3:11, 3:51-4:6. The DCV is generated from “at least two (e.g., at least three or four) dynamic data elements[,]” including an “application transaction counter (ATC),” “a cryptogram, digital signature, or hash value based on transaction data[,]” “a time of day, a current transaction amount, a terminal ID, a merchant ID, and a randomly generated number from a terminal, etc.,” or information “relat[ing] to a consumer’s portable consumer device[.]” *Id.*, 4:21-56, 4:61-7:5, Fig. 1. The dynamic data elements can also be used with “static data elements[,]” including “telephone number, a SIM card number, an account number, birthday, home address, expiration date, etc.” and “service code” to generate a dCVV. *Id.*, 4:52-60, 5:2-5. The dCVV is generated by cryptographically combining this information with multiple encryption keys, including a master derivation key, resulting in a 3-digit dCVV. *Id.*, 4:61-6:34, Figs. 1-3. The master derivation key is provided by the service provider. *Id.*, 5:38-57, Fig. 2.

The dCVV is embedded into the payment data, which is transmitted to the point of sale terminal and then to the service provider, e.g., “payment processing organization or an issuer of the portable consumer device.” *Hammad*, 2:18-20, 4:61-6:34, 6:40-42, 6:49-7:28, 7:29-32, 7:43-46, 7:55-61, Figs. 4-5. The service provider uses the dCVV to determine the authenticity of the payment. *Id.*, 7:29-8:50, Fig. 6.

Thus, Hammad teaches generating a dCVV from an application transaction counter (“ATC”) (device transaction sequence counter count); user information, such as telephone number, birthday, home address; an account number (payment account number); a service code; and expiration date, among other information, that is combined with a master derivation key (information and secrets known to a payment processing authority). *Hammad*, 4:21-44, 4:52-56, 4:63-5:5, 5:34-6:3 Figs. 1-2; *Dec.*, 145-147.

c) Motivation to Combine

A POSITA would have understood that a dCVV, as generated by Hammad, is a cryptogram number used in place of a card validation value (e.g., CVV) originated from the payment issuing authority generated by cryptographically combining the recited elements, among other information. *Dec.*, ¶148. A POSITA would have been motivated to use Hammad’s dCVV generation process for the same reasons recited in Claim 19(e) for using Varadarajan’s DCV. *Id.* Indeed, Hammad is a natural extension of Varadarajan, which teaches generating a DCV from data elements.

Varadarajan, [0055]. Hammad extends this teaching by including at least three or four dynamic data elements and static data elements, including an account number, to generate a dynamic CVV to increase security. *Id.* A POSITA would have recognized that including more data elements in generating a DCV would decrease the likelihood that, even if the payment data were intercepted, that it could be used in a fraudulent manner. *Id.* Therefore, a POSITA would have been motivated to include more data elements in generating a DCV for the CVV in the combination, as taught by Hammad. *Id.* A POSITA would have further recognized that modifications to Kalgi-Khan-Varadarajan would be minimal as it would simply require additional inputs to Varadarajan's DCV generator. *Id.* This modification of known techniques would have yielded the predictable result of increasing security of the transaction. *Id.*

2. ***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.***

Hammad teaches the dCVV is generated for "each transaction" (a one-time limited-use payment information). *Hammad*, 2:65-67, 4:21-31, 4:61-65. The ATC is "incremented with each transaction." *Id.*, 4:25-26; *see also*, 1:50-51. The user device combines the ATC with other dynamic and static data elements at the time of

generating the dCVV. *Id.*, 4:63-6:34. A POSITA would have understood the resulting dCVV, combined with other payment data, is a one-time limited-use payment information generated from combining the current ATC with other data elements. *Dec.*, ¶149.

B. Claim 22

1. 22(a): The method of claim 19, further comprising:

generating a limited-use security code number for use in place of a card issuer card security code, by cryptographically combining information from at least one of a set of information comprising: a device transaction sequence counter; a device account number; a payment account information, device secrets; payment processing authority secrets; and

As discussed in Claims 20(a), Hammad teaches generating a limited-use dCVV (limited-use security code number) by cryptographically combining at least one of an ATC (a device transaction sequence counter), account number (a payment account information), and PIN verification data or master derivation key (payment processing authority secrets).

Varadarajan teaches that a DCV can be configured as a “Card Security Code (CSC).” *Varadarajan*, Abstract, [0002]-[0003], [0013]. A POSITA would have understood that a DCV/dCVV, when configured as a CSC, is used in place of a card issuer card security code. *Dec.*, ¶151; *see also* Claim 20(a).

2. 22(b): displaying the limited-use security code number on the user-interface of the device display.

Varadarajan teaches that the DCV can be displayed on the user device for subsequent entry. *Id.*, [0032] (“The DCV may be displayed to the user ... to be subsequently keyed in ... to the transaction interface.”), [0045], [0056], Fig. 4 (steps 435, 450). A POSITA would have found it obvious to implement the same in Kalgi to enable a user to perform the online transaction by entering the required information on a user interface. Without such information, the transaction could not be completed, which would not be acceptable. *Dec.*, ¶149. A POSITA would have had a reasonable expectation of success in implementing the same as Kalgi already teaches a user interface for displaying and entering information, such as a card security code. *Kalgi (EX1004)*, [0059], [0062], [0106], Fig. 2; *Dec.*, ¶149. The combination, therefore, is simply a combination known methods to yield the predictable result of enabling a user to securely conduct an online transaction. *Dec.*, ¶149.

VII. GROUND 3: CLAIM 21 IS OBVIOUS OVER KALGI, KHAN, VARADARAJAN, AND SMITH

A. Claim 21

- 1. 21(a): The method of claim 19, wherein at least a portion of said limited-use number comprises a static device account number, and wherein the static device account number is of a limited scope of valid use to a specific device,***

As discussed in Claim 19(e), Varadarajan teaches generating a DCV (limited-use number) for a PAN and/or CVV. In the case of a DCV being generated for a

portion of the “static PAN[,]” Varadarajan teaches that the DCV may replace a portion of the PAN, e.g., the last ten digits, referred to as a “dynamic partial PAN.” *Varadarajan*, [0012]-[0013], [0021], [0030]-[0031]. A POSITA would understand that at least a portion of a dynamic PAN, therefore, includes parts of a static PAN. *Dec.*, ¶153.

a) Smith’s Teachings

In related art, Smith teaches a “mobile device” from which a user may “request the issuance of a payment account such that the payment account is accessible using a mobile device 104 associated with a customer.” *Smith*, [0014]. Whenever a user wishes to open a payment account, the issuer issues a “temporary PAN...and establishes any risk parameters (e.g., for use in controlling the authorization of transactions involving the temporary PAN)” so the user is able to make purchases while awaiting an actual PAN. *Smith*, [0026].

This “temporary PAN is mapped to a **mobile PAN (e.g., such as a PayPass® PAN, or PPAN).**” *Smith*, [0026] (emphasis added). The PPAN (device account number) is “assigned to the mobile device 104.” *Smith*, [0016]. The PPAN is “stored in the mobile device 204.” *Smith*, [0022]. The PPAN is, therefore, a device account number. *Dec.*, ¶¶154-155.

Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith*, [0026], [0040]. The PPAN (device account number) is then associated

with a “related PAN[.]” *Smith*, [0023]. The PPAN is “initially...mapped to the temporary PAN” but whenever the issuer issues the “actual PAN” the actual PAN “replace[s] the temporary PAN” so the PPAN is now an alternate number mapped to the actual PAN. *Smith*, [0040]. The PPAN, therefore, is a different number from the actual PAN. *Dec.*, ¶156.

600

CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE

FIG. 6

Smith, Fig. 6.

The issuer can “implement dual account number structures” so that “multiple NFC-enabled handsets may be managed for a single account.” *Smith*, [0029]. Accordingly, *Smith*’s PPAN is a distinct account number for a payment account on a particular “mobile device” (a specific device). *Dec.*, ¶157.

Even if the same user wants to register a new device, a user will get a different PPAN for that device to use because the PPAN is assigned immediately upon registering the device. *Smith*, [0026] (“an instantly-issued payment account that may be used by the customer almost immediately after submitting a request for a new payment account.”); *Dec.*, ¶158.

Smith further teaches an expiration date associated with the account may be updated without updating the PPAN. *Smith*, [0041] (“update an NFC-enabled payment account (e.g., to update an expiration month and/or year”)). Therefore, a POSITA would understand because the PPAN is associated with a specific account and mobile device, it is a static device account number for a specific device. *Dec.*, ¶159. A POSITA would further understand the PPAN is of limited scope of valid use in that it is only able to be used by the mobile device 104 within the expiration period. *Id.* Thus, Smith’s PPAN is a static device account number [] of a limited scope of valid use to a specific device.

b) Motivation to Combine

A POSITA would have found it obvious and been motivated to use Smith’s PPAN in place of Kalgi’s account number. *Dec.*, ¶¶160-164. A POSITA would have appreciated that storing a PPAN would be safer than storing the actual account number on Kalgi’s device. *Dec.*, ¶160.

A POSITA would have been motivated to use Smith's PPAN in place of Kalgi's account number so that Kalgi's mobile device would not be required to store the account number, which is a sensitive financial number. *Dec.*, ¶161. It was well known in the art that a mobile device could be vulnerable to malicious attacks and therefore storing Smith's PPAN instead of the account number on Kalgi's mobile device would have increased security for the user's account. *Id.* For example, a POSITA would have understood that it is valuable to remove account numbers from a user device so that if the device were stolen, the thief would have access only to PPAN(s). *Id.* A POSITA would have recognized that this is beneficial because if a user's device is lost or stolen, only the PPAN(s) would have to be cancelled. *Id.*

A POSITA would have had a reasonable expectation of success in implementing Smith's PPAN in Kalgi's payment application without undue experimentation because Kalgi already teaches use of an account number and a POSITA would have been familiar with using PAN-alternatives. *Dec.*, ¶162. In the combination, Smith's PPAN would perform the same function—provide an account number that can be used for a payment transaction. *Id.*; *Smith*, [0023]. A POSITA would have understood that using Smith's PPAN in place of Kalgi's account number would be combining prior art elements according to known methods to yield the predictable result of increased security. *Dec.*, ¶162; *KSR*, 550 U.S. at 415-421. A POSITA would have been motivated to apply Kalgi and Smith's teachings and

appreciated the compatibility of their teachings because both discuss payment systems that rely on similar functionalities. *Dec.*, ¶162.

A POSITA would have substituted Smith’s PPAN for Kalgi’s account numbers when making payment transactions, as taught by Smith. *Smith*, [0018] (“the process of personalizing the mobile device 104 with the software (including the PPAN...[o]nce the personalization or loading of the payment application is complete, the customer 102 may use the mobile device 104 to complete payment transactions.”). A POSITA would again have recognized that substitution of a PPAN would have increased security since sensitive information like an account number would not be transmitted. *Smith*, [0023] (“the payment network 218 identifies the PPAN and requests a look up of the related PAN”); *Dec.*, ¶163. This is a simple substitution of one known element for another and a POSITA would have understood to predictably increase the security of Kalgi’s payment system and protected the user’s sensitive account information. *Dec.*, ¶163.

A POSITA would have further found it obvious and been motivated to use the PPAN to generate a dynamic partial PPAN, as taught by Varadarajan. *Dec.*, ¶164; *see* Claim 19(e). Thus, in combination, Kalgi-Khan-Varadarajan-Smith would generate a dynamic CVV and dynamic partial PPAN (DCV + portion of the PPAN, which is of limited scope of valid use to the user’s specific device. *Dec.*, ¶164.

2. 21(b): 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:

Smith teaches that the PPAN (device account number unique for the specific electronic device) is provided to the mobile device by an issuer system in place of the real account number (payment issuer information). *Smith*, [0016]-[0018], [0026], [0029] Figs. 1-4, 6. Specifically, after a user requests an account, the issuer provides a temporary PAN to an OTA provisioning service. *Smith (EX1008)*, [0015]. The OTA provisioning service forwards the temporary PAN to a PAN mapping/account generation service, which assigns the PPAN to a mobile device and maps the PPAN to the temporary PAN, and subsequently to the real PAN. *Smith (EX1008)*, [0016], [0019], Figs. 1, 6. The OTA and PAN mapping/account generation services, which generate and provide the PPAN to the mobile device, are operated on behalf of a payment network, such as MasterCard. The PPAN is used in payment transactions by the mobile device. (*EX1008*), [0022]-[0023]. A POSITA would have understood, therefore, that the OTA and PAN mapping/account generation service are a payment processing authority that provides the device account number for the specific mobile device in place of the temporary and actual PAN for use in transactions. *Dec.*, ¶165.

3. ***21(c): performing a payment transaction by the electronic device including the dynamically generated limited-use number;***

Varadarajan teaches performing a payment transaction using a DCV. Specifically, Varadarajan teaches sending a DCV and other transaction information to an issuer/authenticating server. *Varadarajan*, [0027], [0045]; *see also* Claim 19(e). The issuer/authenticating server independently regenerates the DCV to authenticate the transaction. *Varadarajan*, [0027], [0043], [0045], [0056], Fig. 4. A POSITA would have found it obvious to perform a transaction using Varadarajan's DCV for the same reasons discussed in Claim 19(e). *Dec.*, ¶166.

4. *21(d): combining the dynamically-generated number and the static device account number within a device-generated complete payment information; and*

A POSITA would have found it obvious to combine the DCV, i.e., dynamic PAN and/or CVV, (dynamically-generated number) and Smith's PPAN (static device account number) in the payment data (device-generated complete payment information) sent to the merchant and financial institution in Kalgi. *Dec.*, ¶167; *see also* Claims 19(e)-(f).

5. *21(e): conveying said device-generated complete payment information, in place of a selected payment issuer information, when the device is performing payment transactions; and*

A POSITA would have found it obvious to convey the DCV(s), PPAN, and other payment data (device-generated complete payment information) in place of selected payment issuer information (e.g., CVV and/or PAN) when the device is performing payment transactions. *Dec.*, ¶168; *see also* Claims 19(e), 21(a).

6. ***21(f): 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.***

In the proposed combination, if an invalid DCV is sent with the PPAN, the financial institution authenticating the transaction would not be able to regenerate the DCV. *Varadarajan*, [0027], [0043], [0045], [0056], Fig. 4; *Dec.*, ¶169. In that case, the transaction would not be authenticated because it would indicate that device is not able to conduct the requested transaction. *Varadarajan*, [0027], [0043], [0045], [0056], Fig. 4. A POSITA would understand, therefore, that using Smith's PPAN without a valid DCV would be denied as invalid and outside the scope of use for the mobile device. *Dec.*, ¶169.

VIII. GROUND 4: CLAIM 25 IS OBVIOUS OVER KALGI, VARADARAJAN, AND SMITH

A. Claim 25

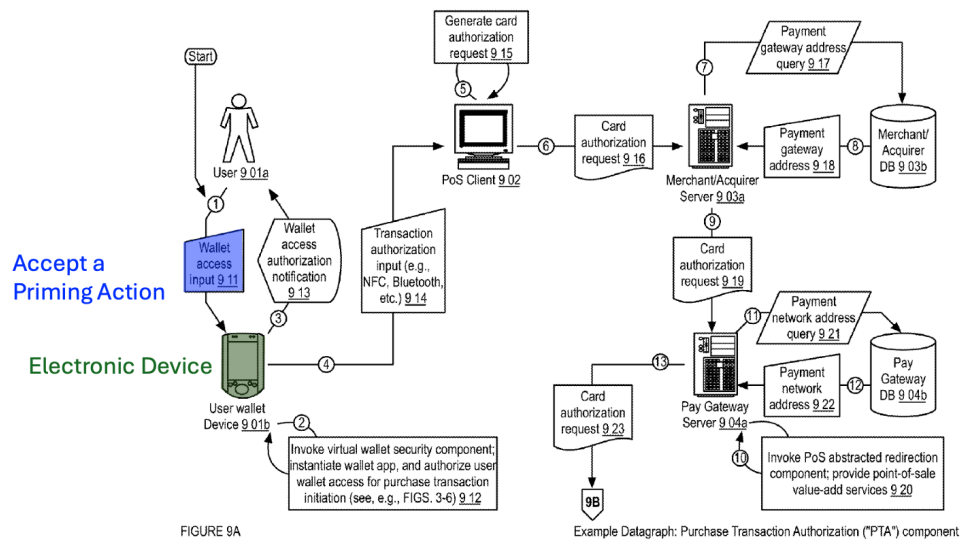
1. ***25(pre): A non-transitory, computer-readable medium storing computer executable instructions that when executed by one or more processors, cause the one or more processors to:***

To the extent the preamble is limiting, Kalgi teaches a user device, such as a mobile device, that executes “an E-Wallet application” (computer executable instructions) that causes the device to perform e-wallet functions. *Kalgi*, [0048]; *see also*, Abstract, [0033] (“The user device may have executing thereon a wallet application, including features such as those as described herein.”), Figs. 1

(illustrating E-Wallet application on mobile device 102(b)), 2 (depicting wallet application interface). Kalgi further describes an “e-wallet checkout apparatus embodiment, comprising: a processor; and a memory disposed in communication with the processor and storing processor-issuable instructions to: ... receive a merchant payment request; ... instantiate, via the processor, a wallet application ...; obtain a payment method selection via the wallet application; provide a transaction execution request for a transaction ...; receive a purchase response ...; and output purchase response information” *Kalgi*, [0259]-[0268]; *see also*, [0198]-[0205], [0229]-[0236]. Therefore, that the E-Wallet application is stored on the mobile device’s non-transitory, computer readable medium as computer executable instructions that when executed by the device’s processor, cause it to perform the functions recited below.

2. 25(a): accept a priming action of the electronic device by an identified valid device user, identified from the device inputs;

Kalgi’s user device (the electronic device) accepts “a wallet access input” from the user. *Kalgi*, [0067], [0083], Fig. 9A.



Kalgi, Fig. 9A (annotated).

The wallet access input is “a single tap (e.g., a one-tap mobile app purchasing embodiment) of a touchscreen interface, keyboard entry, card swipe, activating a RFID/NFC equipped hardware device (e.g., electronic card having multiple accounts, smartphone, tablet, etc.) within the user device, ... single/multi-touch gestures on a touch-sensitive interface, touching user interface elements on a touch-sensitive display[.]” *Id.*, [0067]. “[T]he user wallet device may authenticate the user based on the user’s wallet access input, instantiate a wallet application (see, e.g., FIGS. 13-19B) upon authenticating the user, and provide virtual wallet features for the user via the wallet application.” *Id.*; *see also*, [0029], [0054]-[0055], [0083], Fig. 5.

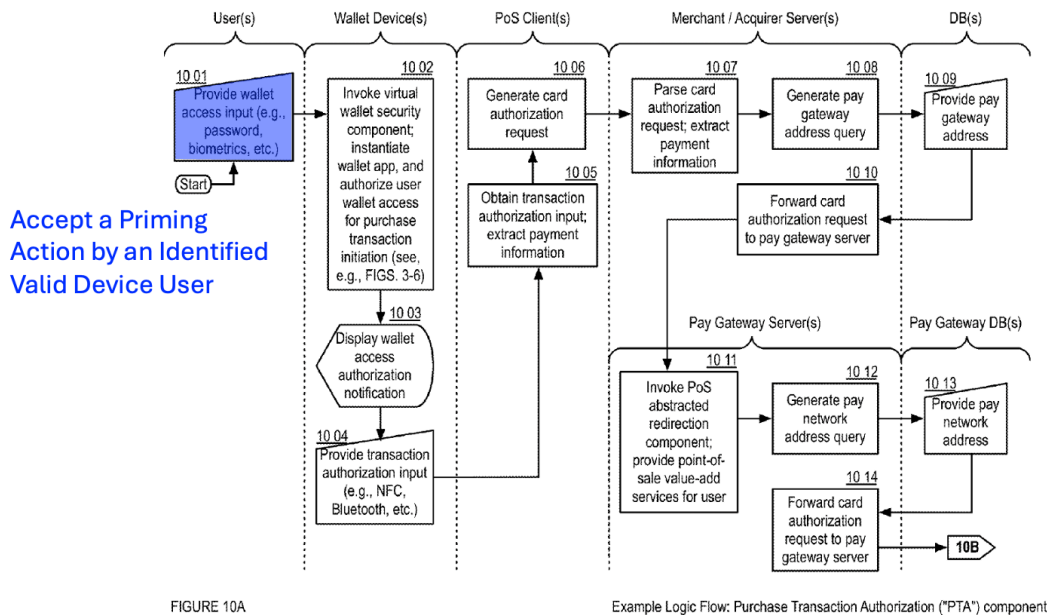


FIGURE 10A

Example Logic Flow: Purchase Transaction Authorization ("PTA") component

Kalgi, Fig. 10A (annotated).

To perform the authentication, “the user may be required to enter login information, answer a challenge question, submit a voice/biometric signature, provide a digital certificate, enter into a video call for verification purposes, and/or the like.” *Id.*, [0051], [0067], [0083], [0145]. Thus, Kalgi’s user device accepts a wallet access input by an identified valid device user, identified from the device inputs.

This mapping is consistent with the ’538 Patent’s description that bringing a device within range of a reader or a key input may form part of the priming operation. ’538 Patent at 11:67-12:3, 13:65-14:1.

3. **25(b): enable the electronic device for imminent performance of a payment operation responsive to the priming action of said valid user;**

Kalgi teaches that after accepting the wallet access input of the authenticated user (*said valid user*), the device “instantiate[s] a wallet application (see, e.g., FIGS. 13-19B) upon authenticating the user, and provide[s] virtual wallet features for the user via the wallet application.” *Kalgi*, [0067]-[0068], [0083]-[0084]. “For example, the user wallet device may utilize the components described above in the description with respect to FIGS. 3-6 to provide e-wallet checkout services for the user via the wallet application.” *Id.*, [0067].

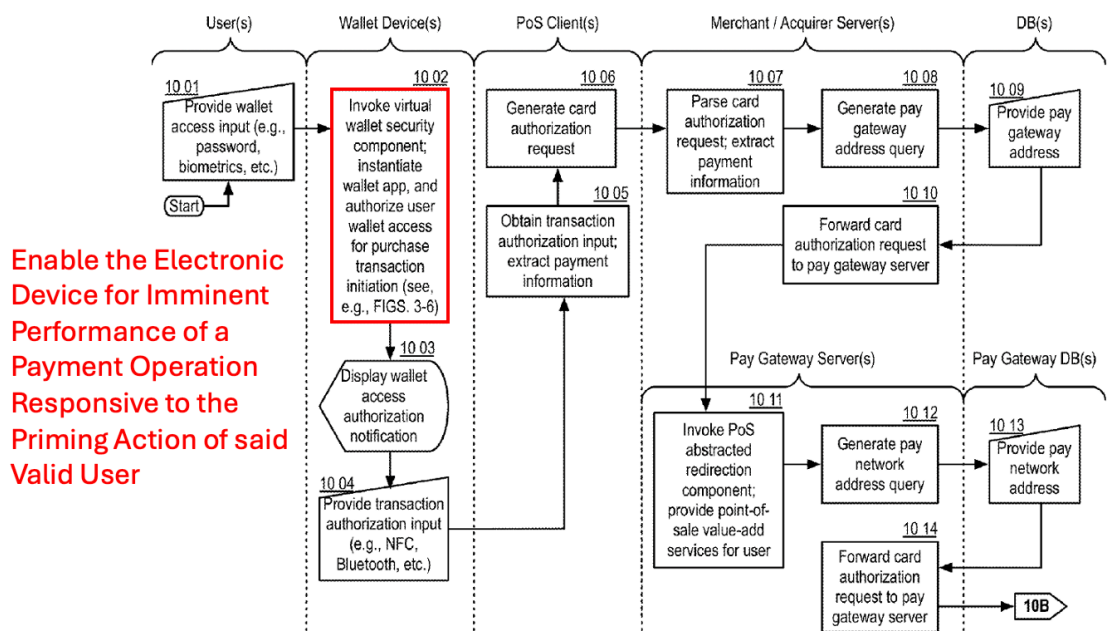


FIGURE 10A

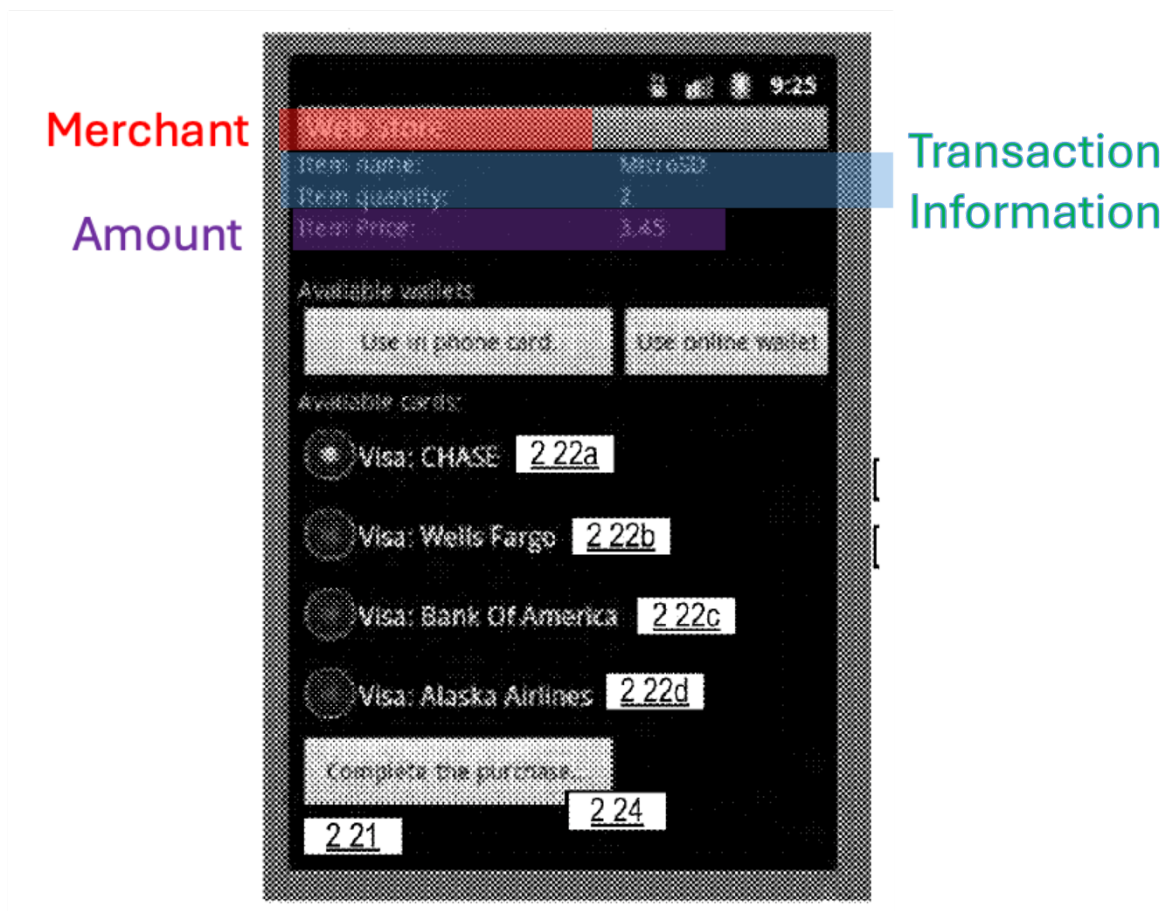
Example Logic Flow: Purchase Transaction Authorization ("PTA") component

Kalgi, Fig. 10A (annotated), Fig. 9A.

By instantiating the wallet application and providing the wallet application features, *the electronic device* is enabled for *imminent performance of a payment operation responsive to the* wallet input of a valid user.

4. ***25(c): display a summary of online purchase information including the merchant information and the purchase amount; and,***

As shown in Figure 2, Kalgi's e-wallet application causes the processor to display a summary of online purchase information including the merchant information and purchase amount.



Kalgi, Fig. 2 (annotated excerpt).

5. ***25(d): display at least one selectable issuer payment account methods on a display; and,***

Kalgi teaches this limitation. See Claim 19(c).

6. ***25(e): receive a payment selection and approval authorization from said valid device user via a human input sensing at the***

device; and

See Claim 19(d). A POSITA would understand that Kalgi's touchscreen interface performs human input sensing at the device. Dec., ¶179.

7. ***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,***

As discussed in Claim 19(c), Kalgi teaches that a user wallet device includes payment information, including an account number, account name, account address, CVV (including a dynamic CVV), and other information, in a compatible data form that is provided to a PoS client. *Id.*, [0068]-[0069], [0084]. As discussed in Claim 21(a), a DCV can be generated and used as part of a PPAN. See Claim 21(a); see also Claim 19(e); Dec., ¶180. Because the PPAN is device-specific, a POSITA would understand a dynamic partial PPAN is device-specific limited-use payment information that is used in place of the PPAN. Dec., ¶180.

Additionally, or alternatively, Varadarajan's DCV is also device-specific because the DCV generator uses "a device derived identification parameter ... which is unique to the user device or machine used to host the DCV generating application." *Id.*, [0029]; see also, [0053] ("By including a device identifier in the DCV generator, where the included device identifier is unique to each user device

accessing a joint account, **each transaction and DCV is further identifiable to the user device conducting a transaction** or requesting a DCV.”); Claim 19(e).

Thus, Varadarajan’s DCV, e.g., dynamic PAN and/or CVV, is device-specific limited-use payment information that is dynamically generated for use in place of at least a portion of said selected issuer payment account information (e.g., the PAN, CVV, etc.) on the device. Dec., ¶180-181.

8. 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,

As discussed above, Kalgi teaches device payment information for a credit card including, e.g., account number, account name, billing address, and CVV values. Kalgi, [0069]-[0070]. In addition, Kalgi teaches that the user wallet is stored on the mobile device, such as in memory. Kalgi, [0036]; see also, [0067]-[0069]. The user wallet includes issuer provided payment information, such as PAN and CVV, that is provided to the PoS client. Kalgi, [0069]. As discussed above, it would have been obvious to replace at least a portion of the issuer provided payment information, such as the CVV, with Varadarajan’s DCV. See Claim 25(f); Kalgi, [0069], [0083]; Dec., ¶183.

Thus, it would have been obvious to further configure Kalgi’s electronic device to form a complete combined payment information from Varadarajan’s DCV (e.g., CVV) (a dynamically generated portion) and (mobile wallet) account number,

account name, billing address, etc. (a statically generated portions stored in a memory of the device) for the same reasons. *Dec.*, ¶184; *see* Claims 19(e), 21(a).

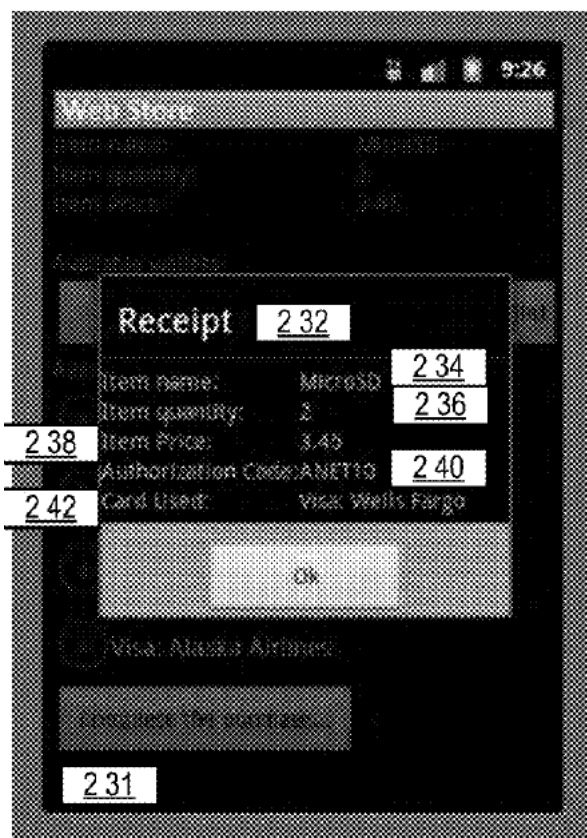
- 9. 25(h): wherein the communication interface is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction; and**

Kalgi teaches that the user wallet device can provide payment information to the merchant PoS client using various communication technologies, including Wi-Fi, Bluetooth, NFC. *Kalgi*, [0068], [0084]; *see also* Claim 19(a). The payment information is “formatted according to a data formatting protocol appropriate to the communication mechanism employed in the communication between the user wallet device and the PoS client.” *Kalgi* at [0069], [0084]. A POSITA would have understood that the user wallet device includes interfaces for communicating with the PoS client using these technologies. *Dec.*, ¶185. Thus, the combination also teaches that the communication mechanism (communication interface) is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction.

- 10. 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.**

The processor of Kalgi's device is further operable to receive a receipt from the EWCP provider or payment/issuer servers (*an online payment facility*). *Kalgi*, [0030], [0033], [0038], [0081]-[0082], [0092]; *see also*, [0259]-[0268] (“... receive a purchase response to the transaction execution request; and output purchase response information derived from the received purchase response.”). Because the receipt is only sent when the transaction is approved, it qualifies as *an approval confirmation*. *Id.*, [0038].

As shown in Figure 2, the receipt 232 is displayed on screen 231 to *visually convey the status of the online purchase transaction*.



Kalgi, Fig. 2 (annotated excerpt); *see also*, Figs. 9B, 10B.

Kalgi also teaches “[i]f the payment was unsuccessful, the purchase may be denied[.]” *Id.*, [0050]. “For example, the user may be directed to a webpage that informs the user that the payment was unsuccessful[.]” *Id.*; *see also*, Figs. 4, 10B (“Display ... transaction declined notice for user”). The approval or denial are only sent once the payment information is received and processed by EWCP provider or one or more payment processing facilities. *Id.*, [0044], [0072]-[0082], [0086]-[0092], Figs. 9A-9B, 10A-B.

Thus, Kalgi’s processor is also operable to receive 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.

IX. GROUND 5: CLAIMS 28-30 ARE OBVIOUS OVER KALGI, KHAN, VARADARAJAN, HAMMAD AND SMITH

A. Claim 23

1. ***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 payment issuer information; a payment processing authority secrets; a transaction information; and,***

As discussed in Claims 20(a) and 21, it would have been obvious to generate a DCV/dCVV (limited-use number) by cryptographically combining an ATC (transaction sequence count information), PPAN (device account number), information relating to a user, such as telephone number or home address (user

account information), expiration date or service code (payment issuer information), PIN verification data or master derivation key (payment processing authority secrets), and payment amount (transaction information).

Hammad further teaches that the dCVV may be generated using time as one of the dynamic data elements. *Hammad*, 3:9-11, 4:37-40, 4:61-5:5, 6:49-57, 7:4-14, Figs. 4-5. The service provider can use the time of day (time of use) to determine whether it is within a certain range in authenticating the transaction. *Id.*, 8:28-36.

A POSITA would have found it obvious, and been motivated, to implement Hammad's time of use check in authorizing a transaction or use the time of day in generating the dCVV. *Dec.*, ¶192. A POSITA would have recognized that using the time of day provides an additional layer of security to the authorization process. *Id.* Implementing this feature in Kalgi would have predictably yielded the result of increased security by limiting the time for which a generated DCV/dCVV could be used. *Id.* This modification would not change the operation of the combination or require any additional hardware; rather, it would require only minor programmatic changes. *Id.*

2. ***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***

Kalgi teaches a provider sending and displaying a receipt or payment confirmation message to a customer confirming the purchase transaction

(authorization of said transaction). *Kalgi*, [0038], [0044]-[0046], [0050], [0060]-[0061], [0064], [0081]-[0082], [0092], Figs. 2 (element 231), 3, 6, 8, 9B, 10B (“Display purchase receipt ... declined notice for user”). *Varadarajan* and *Hammad* teach a financial institution verifying the limited-use DCV/dCVV, and other payment information, used in the payment transaction. *Varadarajan*, [0045], [0056], Fig. 4; *Hammad*, 7:55-8:44, Fig. 6.

A POSITA would have understood that in the combination, *Kalgi*’s receipt/payment confirmation would only be received by the mobile device if the DCV/dCVV generated and sent by the mobile device in place of the payment issuer account information, and other payment information, was verified by the service provider. *Dec.*, ¶¶193-194.

3. ***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.

Kalgi teaches that if the payment was unsuccessful, the purchase may be denied by the provider and the user notified of the same in the display. *Kalgi*, [0050], Figs. 4, 10B (“Display ... transaction declined notice for user”).

Varadarajan teaches the authenticating server independently generates a DCV to determine if the inputted DCV matches. *Varadarajan*, [0033], [0045], [0056], Fig. 4. Varadarajan further teaches the server determines whether the DCV is expired, based on number of uses or time. *Id.*, [0045], [0047], [0056], Fig. 4.

Hammad teaches that if the service provider generated dCVV (authority cryptographically-combined number) does not match (mis-matching) the dCVV provided by the mobile device (transacted limited-use number), the transaction is terminated. *Hammad*, 8:47-50, Fig. 6. Hammad also teaches that if a dCVV is being used outside of a time window (valid time window), “the transaction may be declined.” *Id.*, 8:34-36. As discussed, it would have been obvious to implement such a time window check to increase security. *See* Claim 23(a); *Dec.*, ¶¶195-197.

B. Claim 28

1. ***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,

Hammad teaches a user device maintaining and combining static data elements, such as a telephone number, account number, home address, expiration date, birthday, etc. (user and account information), with dynamic data elements to generate a dCVV (device generated information). See Claim 19(e); *Hammad*, 4:21-60.

Smith teaches assigning and storing a PPAN (static device-specific account information) on a user's device. See Claim 21(a); *Smith*, [0016], [0021]-[0022].

Varadarajan teaches using a “unique device identifier ... generated from unique data collected from the user device” (device generated information) to generate a DCV. *Varadarajan*, [0049]. By including the device identifier in this process, “each transaction and DCV is further identifiable to the user device conducting a transaction or requesting a DCV.” *Id.*, [0053].

Thus, a POSITA would have understood, or found it obvious, to store this information in the user device while performing a transaction. *Dec.*, ¶¶198-201. It

would have been obvious to modify Kalgi with the teachings of Hammad, Smith, and Varadarajan to combine this information in generating a DCV/dCVV for the same reasons discussed above in Claims 19, 20, 21(a), 21(e), and 25(f). *Dec.*, ¶192.

When combined in this way, the stored information uniquely identiff[ies] the specific user, specific selected account, and the specific device. *Id.*

2. ***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,***

See Claims 19(e), 20(a).

3. ***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,***

See Claims 19(f), 20(a), 21(d), 25(g).

4. ***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,***

See Claim 19(i), 25(g)-(h).

5. ***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.***

See Claims 19(c), 25(d).

C. Claim 29

1. *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 payment processing authority secret,

a user information,

a payment account information,

...

a payment amount, transactional information; and,

Varadarajan, Hammad, and Smith render obvious cryptographically combining various pieces of information stored on a device to generate a DCV/dCVV (one-time limited-use cryptogram number). See Claim 28(a); see also Claims 19(f), 20(a), 21(d); Dec., ¶206. Hammad teaches a user device maintaining (store) and combining data elements, such as a telephone number, account number, home address, expiration date, birthday, etc. (payment account information and user information); an ATC (transaction sequence counter); information relating to the consumer's portable consumer device; current transaction amount (payment amount,

transactional information); and master derivation key (payment processing authority secret) to generate a dCVV. *See* Claim 19(e); *Hammad*, 4:21-60, 5:38-57.

Varadarajan teaches using a “unique device identifier ... generated from unique data collected from the user device” (information unique to the device and device secret), which is known to the provisioning and authenticating servers, to generate a DCV. *Varadarajan*, [0049]-[0050]; *see also* Claim 28(a). Varadarajan also teaches using the payment amount to generate a DCV. *Varadarajan*, [0055].

Smith teaches assigning and storing a PPAN (device account number) on a user’s device. *See* Claim 21(a); *Smith*, [0016], [0021]-[0022].

Thus, a POSITA would have understood, or found it obvious, to store this information in the user device before generating a DCV/dCVV. *Dec.*, ¶¶206-209. It would have been obvious to modify Kalgi with the teachings of Hammad, Smith, and Varadarajan to combine this information in generating a DCV/dCVV for the same reasons discussed above in Claims 19(e), 20, 21(a), 21(e), 22(b), and 25(f). *Dec.*, ¶209.

Further, Hammad teaches that the ATC is stored at the service provider. *Hammad*, 8:2-5, 8:41-47. Smith teaches that the PPAN is stored at the issuer system. *Smith*, [0012], [0016], [0038]-[0040], Fig. 6.

Varadarajan teaches that the service provider independently generates a DCV using the same process as the user device, i.e., using the same DCV generator and

DCV key as used by the user device. *Varadarajan*, [0045]; *id.*, [0033], [0056]. A POSITA would understand that the user account information used to generate the DCV key that is used to generate the DCV generator would have also been stored at the authenticating and/or provisioning server in order to verify the same. *Dec.*, ¶211; *Varadarajan*, [0043], [0045]. Thus, a POSITA would understand this information is stored at the authenticating server to independently generate a DCV. *Dec.*, ¶211.

Alternatively, it would have been obvious to store this information at the payment processing authority and/or payment issuer. *Dec.*, ¶212. For example, Hammad teaches that the payment processing authority and issuer both “validate cryptogram” (i.e., dCVV). *Hammad '089 Provisional (EX1011)*, p. 78. Some payment processing entities perform the functions of payment processor and issuer. *Id.*, [0025]. Thus, a POSITA would understand that in order to validate the cryptogram (i.e., dCVV), each authority (whether the same entity or different entities) would need to store the information from which the dCVV was generated, as described above. *Dec.*, ¶211.

2. ***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,***

As discussed, a DCV/dCVV is used in place of an issuer's CVV or account number (*static payment information*) in a payment transaction using the selected payment account. *See* Claims 19(e), 20(a); *Dec.*, ¶213.

3. ***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,***

As discussed in Claim 23(b)-(c), the authority verifying the DCV/dCVV re-generates the DCV/dCVV in the same way and using the same information as the user device. *Dec.*, ¶214. The authority-generated DCV/dCVV are compared with the user-device generated DCV/dCVV. *See* Claim 23(b)-(c); *see also* Claims 21(f), 23(f). A POSITA would understand that in order to re-generate a DCV/dCVV, the verifying authorities would need to recognize what information needs to be used to perform such a re-generation. *Dec.*, ¶214; *see also* Claim 29(a).

4. ***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,***

See Claims 23(c), 25(i).

5. ***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,***

See Claims 23(b), 25(i).

6. ***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.

The proposed combination teaches or renders this limitation obvious. See Claims 23(b)-(c), 25(i).

D. Claim 30

1. *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 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,

As discussed in Claim 29 (a), it would have been obvious to generate a DCV/dCVV (one-time limited-use cryptogram number) by cryptographically combining information, including at least one of: account number, home address, expiration date, birthday, etc. (user payment account number and user private

information), ATC (*transaction sequence counter*), current transaction amount (*transaction information*), device identifier (*device secret*), master derivation key (*payment processing authority secret*), and PPAN (*device payment account number*) that is *unique to the device*. See Claim 29(a); see also Claim 20(a), 23(a); Dec., ¶218. Further, as discussed in Claims 29(a), this information would be known to the user device, payment processing authority, and payment issuer authority. Dec., ¶218.

2. ***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,***

See Claim 29(b).

3. ***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,***

See Claim 29(d).

4. ***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,***

See Claim 29(e).

5. ***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,***

Kalgi teaches this limitation. See Claims 23(b)-(c), 25(i), 29(f).

6. ***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.

A POSITA would understand that when a user device is used as described in Claims 25 and 30, the device emulates the behavior of a payment transaction involving an issuer account, i.e., credit card, when the payment information is received and processed by the payment authorities. *Dec.*, ¶223.

X. GROUND 6: CLAIM 26 IS OBVIOUS OVER KALGI, VARADARAJAN, HAMMAD, SMITH AND BAUER

A. Claim 26

- 1. 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;

Kalgi teaches that user device accepts a “wallet access input” via the device human input sensors (e.g., NFC hardware, touchscreen interface, voice, etc.) as part of a priming action. *See* Claim 25(a).

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 biometric recognition of a valid user,

...

***a security question which a valid user could answer correctly,
and***

As described in Claim 25(a), Kalgi teaches authenticating a user by requiring at least one security challenge, including entry at a touchscreen (human device input) of login information (a correct passcode touch entry sequence), answering a challenge question (a security question which a valid user could answer correctly), single/multitouch gestures on a touchscreen interface (a correct touch gesture), submitting voice/biometric signature (a biometric recognition of a valid user), among other authorization measures. *Id.*, [0051], [0067], [0083], [0145].

2. *26(c): receiving a correct user response input, from a security challenge presented on the device display; and*

Kalgi teaches the “user wallet device ... authenticate[s] the user based on the user’s wallet access input,” and if the user is verified, “the client may obtain security credentials ... from the client’s memory, to launch the wallet application, and may instantiate the wallet application[.]” *Kalgi*, [0051], [0067]-[0068], [0083]-[0084], [0145]; *see also* Claim 26(b).

3. ***26(d): 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.***

Kalgi teaches that if the authentication information is not valid (*incorrect user response input*), the user is informed that login information was incorrect. *Kalgi*, [0055]. Kalgi also teaches that “if the number of failed authorization attempts exceeds a threshold,” e.g., when the payment options have insufficient funds, the server may “abort the authorization process, and provide an ‘authorization fail’ message to the ... user device[.]” *Id.*, [0078], [0090]. A POSITA would have found it obvious to apply Kalgi’s threshold attempts to the user authentication process. *Dec.*, ¶227. Using a threshold of authentication attempts at a user device was commonplace at the time. *Id.* A POSITA would have been motivated to implement such a process in Kalgi’s device to increase device security and prevent unauthorized users from making purchases if they had access to the mobile device. *Id.* This modification would have been using known techniques to improve a device in a known way and a POSITA would have had a reasonable expectation of success in making this modification to yield the predictable result of increased security. *Id.*

To the extent that Patent Owner argues that such a modification would not have been obvious, it would have been obvious in view of Bauer.

a) Bauer’s Teachings

Bauer teaches a process for conducting a payment transaction using a mobile device that stores a wallet application for one or more accounts, such as a credit. *Bauer*, [0073]-[0074], [0087]. A user provides input to activate a payment feature with the wallet application. *Id.*, [0086]. If required, the mobile device prompts the user for entry of a PIN and compares the entered PIN to a pre-defined PIN. *Id.*, [0087], [0090]. If the entered PIN is incorrect, the mobile device updates a count of the incorrect PIN entry attempts and if a PIN is entered incorrectly a defined number of times, lock the PIN, which “effectively prohibits the payment feature for the mobile payment account[.]” *Id.* A POSITA would understand that through this process a user is offered a reduced number of additional challenge attempts before failing user authorization and denying payment authorization. *Dec.*, ¶229.

b) Motivations to Combine

It would have been obvious and a POSITA would have been motivated to configure an electronic device to offer a pre-defined number of security challenge attempts before failing user authorization, as taught by Bauer. *Dec.*, ¶230. This modification would have predictably reduced the possibility that an unauthorized person would gain access to the mobile device wallet. *Id.* Therefore, a POSITA would have been motivated to improve similar devices and methods in the same way. *Id.* There would have been a reasonable expectation of success because Bauer’s methodology was commonplace at the time and would have required minimal

software changes to Kalgi's device as it constitutes a combination of known elements that yield a predictable result of preventing an unauthorized user from accessing a payment application. *Id.*

XI. GROUND 7: CLAIM 27 IS OBVIOUS OVER KALGI, VARADARAJAN, HAMMAD, SMITH, AND KRANZLEY

A. Claim 27

- 1. 27(pre): *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:***

Kalgi teaches “instantiating, via a processor, a wallet application[.]” *Kalgi*, [0201], [0232]; *see also* [0198]-[0205], [0229]-[0236], [0259]-[0268]. Hammad's “portable consumer device” includes a microprocessor and performs various encryption techniques, including generating encryption keys and encrypting static and dynamic data elements to generate a dCVV. *Hammad*, 3:51-54, 5:2-6:34, Figs. 1-3. Hammad also teaches that its system can be implemented using hardware or a combination of hardware and software. *Id.*, 9:31-38. A POSITA would understand Hammad's processor is a cryptographic processor because it performs cryptographic functions, including multi-level encryption. *Dec.*, ¶231; *see '538 Patent*, 1:42-47.

Alternatively, it would have been obvious to modify Kalgi based on the teachings of Khan.

a) Khan's Teachings

Khan discloses a mobile device having a secure element (“SE”) (*cryptographic processor*) for use in generating dynamic payment data for conducting payment transactions, including online. *Khan*, [0018], [0021], [0022]-[0025], [0028], Figs. 2, 4. Specifically, Khan discloses a portable device with an SE configured to store and process credit card information. *Id.*, [0018], Fig. 2. In conducting an online or in-store transaction, the SE generates an “alias” of the credit card number and encrypts the alias and “crypto data[,]” which is a digitally-signed combination of the alias, a counter value, a merchant identifier, or any other important value, using a shared key. *Id.*, [0023]-[0024], [0028], Figs. 2, 4. This information is sent to a backend server that validates the combination of alias and crypto data using a shared secret key. *Id.*, [0025], [0028]. A POSITA would have understood that Khan’s SE is a cryptographic processor because it is a hardware component isolated from an application processor and that stores encryption keys and secrets and performs cryptographic functions. *Dec.*, ¶233.

b) Motivation to Combine

It would have been obvious to configure Kalgi’s processor in combination to include a secure element for cryptographically combining payment data, as taught by Khan. *Dec.*, ¶234. A POSITA would have understood that a general purpose processor accessing payment data could be compromised. *Id.* A POSITA would have been motivated to include a secure element to handle and process the payment data

and perform the cryptographic functions of Varadarajan and Hammad in order to prevent this risk. *Id.* Indeed, Khan expressly recognizes how the secure element reduces that risk. *Khan*, [0004], [0018], [0024]. As the use of an SE in mobile devices for this purpose was well-known around this time, a POSITA would have had a reasonable expectation success in modifying Kalgi's device to include the same for performing cryptographic functions recited by Claim 27. *Dec.*, ¶234. This combination of known elements to achieve recognized benefits would have yielded the predictable result of more secure payment transactions. *Dec.*, ¶234.

2. ***27(a): cryptographically compute a dynamically generated one-time-use cryptogram number,***

See Claim 20(a)-(b).

3. ***27(b): 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,***

See Claims 19(f), 21(a)-(e), 29(a).

4. ***27(c): 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,***

See Claims 20(a), 28(a). As discussed in Claim 25(f), Varadarajan teaches using a DCV generator to generate the DCV using a DCV key. *Varadarajan*, [0015], [0034] [0050]. The DCV generator is stored in the device and is specific to the device

because it is generated from, and uses, a device identifier in generating a DCV. *Id.*, [0049], [0053]. Further, the device identifier is stored in and specific to the device and does not pass in the transaction. *Id.*, [0049]; *Dec.*, ¶237. A POSITA would have found it obvious to use a device identifier, as information “relat[ing] to a consumer’s portable consumer device,” as an additional data element in generating a DCV/dCVV, as taught by Hammad, in the proposed combination. *See* Claim 20(a); *Dec.*, ¶237.

5. ***27(d): wherein said transaction sequence counter, said information and said secrets are known to both said device, and to said payment processing authority; and,***

See Claims 20(a), 28(a), 29(a).

6. ***27(e): 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,***

See Claim 21(a)-(c).

a) Kranzley’s Teachings

Kranzley teaches a system for conducting payment transactions using a mobile device having a payment application installed thereon. *Kranzley*, Abstract, [0016], [0019], [0021], [0038]. The payment application can store a virtual payment account number (“VPAN”), which is different than, but associated with, a PAN, and can be used in a transaction. *Id.*, [0036], Fig. 5. The VPAN “may have its own virtual expiry date.” *Id.*, [0036], [0064], [0068], Fig. 5. The VPAN is used, along with

expiry date and dynamic data (used in place of a CVV), in the transaction and sent to the issuer, which will deny or allow the transaction based on the VPAN (and associated PAN) and expiry date. *Id.*, [0023]-[0027], [0035], [0037]-[0049], Fig. 6.

b) Motivations to Combine

A POSITA would have found it obvious and been motivated to use an expiration date with Smith's PPAN in the combination, as taught by Kranzley. *Dec.*, ¶¶240-241. As noted by Kranzley, the expiry date is sent to a payment processor and used to conduct an initial authorization check on the VPAN. *Kranzley*, [0056], [0068], Fig. 3. The use of expiration dates in this manner was well-known long before the '538 Patent. *Dec.*, ¶241. A POSITA would have been motivated to use this information to improve similar mobile wallet systems in the same way. *Id.* A POSITA would have had a reasonable expectation of success implementing this modification because the combination already contemplates including the expiration date in the combined payment information sent to the payment processing authority. *See Hammad*, 7:1-3, 7:25-28, Figs. 4-5; *Dec.*, ¶241. As such, this modification would be combining prior art elements according to known methods that would yield the predictable result of ensuring a valid (i.e., not expired) account number is being used. *Dec.*, ¶241; *KSR*, 550 U.S. at 415-421.

7. ***27(f): 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,

As discussed in Claim 20(a), the DCV/dCVV is generated from at least the account number (static device-specific device account number), expiration date (device account expiration date), telephone number, home address, etc. (user information), service code (payment account information), and DCV/dCVV (dynamically generated cryptogram). In the combination, it would have been obvious to use the PPAN and expiration date as an additional data element. *Dec.*, ¶242; *Hammad*, 4:52-56. Hammad further teaches the information used to generate a DCV/dCVV is part of the payment data sent to a payment processing authority. *Hammad*, 4:61-6:34, 6:49-7:54, Figs. 1, 4-5; *see also* *Kranzley*, [0023]-[0027], [0035], [0037]-[0049], Fig. 6. A POSITA would have had a reasonable expectation of success implementing this modification for the same reasons recited in Claims 19(e), 20(a), 27(f). *Dec.*, ¶242.

8. 27(g): and transmitting said complete device payment information when said issuer payment account method is selected.

See Claim 21(e), 25(d)-(e), (h).

XII. DISCRETIONARY CONSIDERATIONS

Pursuant to the Office's Interim Process Concerning Institution published March 26, 2025, Petitioner reserves the right to address in further briefing any discretionary denial issues raised by CardWare.

XIII. CONCLUSION

For the forgoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

XIV. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

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

Petitioner is the real party-in-interest.

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

The '538 patent is the subject of a civil action in *CardWare Inc. v. Apple Inc.*, 1:25-cv-00446 (W.D. Tex.). The '538 Patent is also the subject of a civil action in *CardWare Inc. v. Google Inc.*, 7:24-cv-00278 (W.D. Tex.).

The '538 patent was previously the subject of an *inter partes* review petition in *Samsung Electronics Co., Ltd., v. CardWare Inc.*, IPR2023-00219, which is no longer pending.

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

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Adam Seitz (Reg. No. 52,206) Adam.seitz@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	Mark Lang (Reg. No. 55,356) Mark.Lang@eriseip.com Lydia Raw (Reg. No. 76,436) Lydia.raw@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 11,176,538 to Wyatt (“the ’538 Patent”)
Exhibit 1002	Prosecution History of the ’538 patent (“the Prosecution History”)
Exhibit 1003	Expert Declaration of Dr. Clifford Neuman
Exhibit 1004	WO Publ. No. 2013/0013499 (“Kalgı”)
Exhibit 1005	U.S. Pub. No. 2014/0019367 (“Khan”)
Exhibit 1006	U.S. Pub. No. 2011/0184876 (“Varadarajan”)
Exhibit 1007	U.S. Patent No. 7,740,168 (“Hammad”)
Exhibit 1008	U.S. Pub. No. 2010/0125508 (“Smith”)
Exhibit 1009	WO Publ. No. 2012/042262 (“Bauer”)
Exhibit 1010	U.S. Pub. No. 2010/0125509 (“Kranzley”)
Exhibit 1011	U.S. Provisional Application No. 60/884,089 (“Hammad ’089 Provisional”)
Exhibit 1012	Intentionally Left Blank
Exhibit 1013	Intentionally Left Blank
Exhibit 1014	Intentionally Left Blank
Exhibit 1015	Intentionally Left Blank
Exhibit 1016	Intentionally Left Blank
Exhibit 1017	Intentionally Left Blank
Exhibit 1018	Intentionally Left Blank
Exhibit 1019	Intentionally Left Blank
Exhibit 1020	IBM, <i>The Magnetic Stripe</i> , IBM, https://www.ibm.com/history/magnetic-stripe . (“IBM”)
Exhibit 1021	<i>Vedat Coskun, Near Field Communication: Theory to Practice</i> (John Wiley & Sons, 1st ed. 2012) (“Coskun”)
Exhibit 1022	<i>MagTek, Magnetic Stripe Card Standards</i> , (MagTek Inc. eds., 2011) (“MagTek”)
Exhibit 1023	<i>EMVCo, LLC, EMV Integrated Circuit Card Specifications for Payment Systems: Book 2 – Security and Key Management</i> (EMVCo, LLC eds., Version 4.3 2011) (“EMV”)
Exhibit 1024	<i>Klaus Finkenzeller, RFID Handbook</i> (John Wiley & Sons, 3rd ed. 2010) (“Finkenzeller”)
Exhibit 1025	MasterCard, <i>MasterCard PayPass™ in Action</i> , MASTERCARD (Jun. 11, 5:35 PM), https://www.mastercard.com/us/company/en/ourbusiness/paypass_in_action.html#:~:text=MasterCard%20PayPass%E2%84%A2%20in

	%20Action&text=Developed%20to%20replace%20the%20need,the%20way%20they%20view%20cash. (“PayPass”)
Exhibit 1026	<i>Smart Card Alliance, EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value-Added Functionality</i> (Smart Card Alliance, Inc. eds., 2012) (“Smart”)
Exhibit 1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. (“Pitroda”)
Exhibit 1028	MasterCard, <i>MasterCard Approved Mobile Devices</i> , MASTERCARD (Aug. 3, 2012), http://www.mastercard-mobilepartner.com/docs/MasterCard_Aproved_Mobile_Devices.pdf , [https://web.archive.org/web/20120906234255/http://www.mastercard-mobilepartner.com:80/docs/MasterCard_Aproved_Mobile_Devices.pdf] (“MasterCard Mobile Partner”)
Exhibit 1029	U.S. Patent Publication No. 2013/0054474 to Yeager (“Yeager”)
Exhibit 1030	EMVCo, LLC, <i>EMV Chip At-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World</i> , EMVCo (2002), https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf (“EMVCo”)
Exhibit 1031	<i>Scoping SIG & Tokenization Taskforce PCI Security Standards Council, PCI Data Security Standard (PCI DSS) – Information Supplement: PCI DSS Tokenization Guidelines</i> (pci Security Standards Council eds., Version 2.0 2011) (“PCI SSC”)
Exhibit 1032	<i>Alessandro Vizzarri et al., Security in Mobile Payments</i> (2013) (“Vizzarri”)
Exhibit 1033	U.S. Patent Publication No. 2008/00110983 to Ashfield (“Ashfield”)
Exhibit 1034	Intentionally Left Blank
Exhibit 1035	“Smart Card Technology: New Methods for Access Control” (“Smart Card Tech.”)
Exhibit 1036	U.S. Patent No. 5,528,222 (“Moskowitz”)
Exhibit 1037	“The Electronic Purse” (“Wenninger”)
Exhibit 1038	U.S. Patent No. 5,594,233 (“Kenneth”)
Exhibit 1039	U.S. Patent No. 7,004,385 (“Douglass”)
Exhibit 1040	U.S. Pub. No. 2007/0265984 (“Santhana”)
Exhibit 1041	U.S. Pub. No. 2012/0197691 (“Grigg”)
Exhibit 1042	U.S. Patent Publication No. 2010/0125509 (“Kranzley”)
Exhibit 1043	U.S. Pub. No. 2011/0140841 (“Bona”)
Exhibit 1044	WIPO Publ. No. 2010/039337 (“Lin”)

Exhibit 1045	U.S. Patent No. 7,653,883 (“Hotelling”)
Exhibit 1046	“ <i>A Note on the Use of Timestamps as Nonces</i> ,” B. Clifford Neuman, et al., ACM SIGOPS Operating Systems Review, Volume 27, Issue 2, pp. 10 – 14 (April 1993)
Exhibit 1047	U.S. Pub. No. 2002/0174075 (“Mirlas”)
Exhibit 1048	U.S. Patent No. 5,903,721 (“Sixtus”)
Exhibit 1049	U.S. Patent No. 8,127,999 (“Diamond”)
Exhibit 1050	U.S. Patent No. 8,646,059 (“von Behren”)
Exhibit 1051	SmartCard Alliance, “ <i>The Mobile Payments and NFC Landscape: A U.S. Perspective</i> ” (Sept. 2011)

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,311 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: June 24, 2025

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

**CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105(a)**

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on June 24, 2025, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '538 patent:

David Wyatt
c/o Murabito, Hao & Barnes
1500 E Hamilton Ave, Suite 118
Campbell, CA 95008

A courtesy copy of the Petition for *Inter Partes* Review was emailed to counsel of record in the parallel litigation:

Caroline M. Walters (cwalters@reichmanjorgensen.com)
Navid Cyrus Bayar (nbayar@reichmanjorgensen.com)
Timothy A. Trost (ttrost@reichmanjorgensen.com)
Khue V. Hoang (khoang@reichmanjorgensen.com)
Matthew G. Berkowitz (mberkowitz@reichmanjorgensen.com)
Patrick R. Colsher (pcolsher@reichmanjorgensen.com)
Yue (Joy) Wang (ywang@reichmanjorgensen.com)
Eric H. Findlay (efindlay@findlaycraft.com)

Respectfully submitted,
ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

IPR2025-01150
U.S. Patent No. 11,176,538
COUNSEL FOR PETITIONER