

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. IPR2025-01149
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)	4
	C. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3).....	4
IV.	SHOWING OF ANALOGOUS PRIOR ART	5
	A. LIN.....	5
	B. SMITH	6
	C. VARADARAJAN	7
	D. HAMMAD	8
	E. KRANZLEY	8
	F. ANALOGOUS ART.....	9
V.	GROUND 1: CLAIMS 1-5, 7-18 ARE OBVIOUS OVER <i>LIN</i>, <i>SMITH</i>, <i>VARADARAJAN</i> AND <i>HAMMAD</i>	9
	A. CLAIM 1	9
	1. <i>1(Pre): A method of performing a payment transaction, the method comprising:</i>	<i>9</i>
	2. <i>1(a): receiving an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user; and, ...</i>	<i>11</i>
	3. <i>1(b): wherein [] authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface, a</i>	

	<i>gesture sensor, a motion sensor, and a biometric sensor; and, ...</i>	<i>13</i>
4.	<i>1(c): receiving a request for a transaction payment at said electronic device via an NFC interface of the device; and, ...</i>	<i>15</i>
5.	<i>1(d): displaying, on a display of the device, [the] request and at least a portion of an original static issuer-supplied payment account information associated with a [selected] payment method, for a user selection in paying the [] request; and, ...</i>	<i>17</i>
6.	<i>1(e): retrieving from a memory attached to a processor of the device, a device-specific static limited-use payment information, associated with said selected payment method; and, ...</i>	<i>19</i>
	a) Lin's Teachings	19
	b) Smith's Teachings	21
	c) Motivation to Combine	23
7.	<i>1(f): dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method; and, ...</i>	<i>25</i>
	a) Varadarajan's Teachings	25
	b) Motivation to Combine	27
8.	<i>1(g): using said limited-use payment information[s] in place of at least a portion of said selected original issuer-supplied payment information for the transaction; and, ...</i>	<i>29</i>
9.	<i>1(h): combining [] said dynamically-generated limited- use payment information with said static limited-use payment information, to generate a complete device payment information; and, ...</i>	<i>30</i>
10.	<i>1(i): transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction; and, ...</i>	<i>30</i>

11.	<i>1(j): receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the [] complete device payment information by a payment processor authority and a payment issuer authority; and, ...</i>	33
	a) Hammad's Teachings	34
	b) Motivation to Combine	37
12.	<i>1(k): visually conveying the transaction payment authorization status via a user-interface displayed on said display.</i>	37
B.	CLAIM 2	39
1.	<i>2: The method of claim 1, further comprising receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.</i>	39
C.	CLAIM 3	40
1.	<i>3: The method of claim 1, further comprising receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device.</i>	40
D.	CLAIM 4	42
1.	<i>4(a): The method of claim 3, wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment transactions performed by said device, in place of said selected issuer-payment information; and, ...</i>	42
2.	<i>4(b): wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.</i>	44
E.	CLAIM 5	45

1.	<i>5(a): The method of claim 3, wherein the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information; and, ...</i>	<i>45</i>
	a) Hammad's Teachings	45
	b) Motivation to Combine	47
2.	<i>5(b): wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction; and, ...</i>	<i>48</i>
3.	<i>5(c): wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device; and, ...</i>	<i>49</i>
4.	<i>5(d): a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number; and, ...</i>	<i>50</i>
5.	<i>5(e): an adjusting of said transaction sequence counter count on a per transaction basis; and, ...</i>	<i>52</i>
6.	<i>5(f): an authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching.</i>	<i>53</i>
F.	CLAIM 7	54
1.	<i>7: The method of claim 3, wherein the visual conveying of the transaction status is further comprising at least</i>	

	<i>one, of a set of visual information including: ... a transaction payment amount, ... a merchant information, an original issuer payment account information, an original payment issuer information, ... [and] a payment completion status.</i>	54
G.	CLAIM 8	54
1.	<i>8(a): The method of claim 1, wherein the generating the limited-use payment information is comprising: a device-specific account number; and,</i>	54
2.	<i>8(b): a device-internal transaction sequence counter count; and,</i>	55
3.	<i>8(c): an information unique to the user and device which does not pass in the transaction; and,</i>	55
4.	<i>8(d): at least one payment authority-supplied information which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements, and,</i>	55
5.	<i>8(e): wherein said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information.</i>	57
H.	CLAIM 9	58
1.	<i>9: The method of claim 8, wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number, capable of passing in at least a portion of the device transaction payment information.</i>	58
I.	CLAIM 10	58

1.	<i>10: The method of claim 9, wherein the generating the limited-use payment information further utilizes a secure combination with a device key, and a payment issuer secret.....</i>	<i>58</i>
J.	CLAIM 11	59
1.	<i>11(a): The method of claim 1, wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of:.....</i>	<i>59</i>
2.	<i>11(b) a device payment transaction sequence counter count, and</i>	<i>59</i>
3.	<i>11(c): at least one of a set comprising:</i>	<i>59</i>
	a device-specific internal information associated with said device and also known to a payment processing authority; and, ...	59
	at least one payment processing authority-specific information provided by a payment processing authority; and,.....	59
	a payment issuer specific information provided by a payment issuer.....	59
K.	CLAIM 12	59
1.	<i>12: The method of claim 1, wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information.</i>	<i>59</i>
L.	CLAIM 13	60
1.	<i>13: The method of claim 1, wherein the generating the limited-use payment information utilizes a merchant identifying information.</i>	<i>60</i>
M.	CLAIM 14	60
1.	<i>14: The method of claim 1, wherein the generating the limited-use payment information utilizes a transaction facility information.</i>	<i>60</i>
N.	CLAIM 15	61

1.	<i>15: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment amount.</i>	<i>61</i>
O.	CLAIM 16	61
1.	<i>16: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment facility type.</i>	<i>61</i>
P.	CLAIM 17	62
1.	<i>17: The method of claim 1, wherein the generating the limited-use payment information utilizes an online transaction information.</i>	<i>62</i>
Q.	CLAIM 18	62
1.	<i>18(a): The method of claim 1, further comprising:</i>	<i>62</i>
	dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number; and	62
2.	<i>18(b): wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number, via the incrementing of said transaction sequence counter count on a per-transaction basis, and using said updated transaction sequence counter count in said generation of said cryptogram; and, ...</i>	<i>63</i>
3.	<i>18(c): wherein said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device.</i>	<i>63</i>
VI.	GROUND 2: CLAIM 6 IS OBVIOUS OVER LIN, SMITH, VARADARAJAN, HAMMAD AND KRANZLEY	64
A.	CLAIM 6	64

1.	<i>6(a): The method of claim 3, wherein the generating the limited-use payment information further utilizes a secure combination of said information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information; and, ...</i>	<i>64</i>
2.	<i>6(b): a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority; and, ...</i>	<i>64</i>
3.	<i>6(c): a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid; and, ...</i>	<i>65</i>
4.	<i>6(d): a conveying of said validation result as a declining or accepting of said transaction payment; and, ...</i>	<i>65</i>
5.	<i>6(e): upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction.</i>	<i>66</i>
	a) Kranzley’s Teachings	67
	b) Motivation to Combine	67
VII.	DISCRETIONARY CONSIDERATIONS	69
I.	CONCLUSION.....	69
II.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8	70
A.	REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1).....	70
B.	RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2)	70
C.	LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3).....	70

I. INTRODUCTION

Apple Inc., (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 1-18 (“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* (EX1001), 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 states the “FIELD OF THE INVENTION” “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.*, ¶¶32-33.¹

¹ Citations to “*Dec.*” are to EX1003, 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.*, ¶¶34-35. The '538 Patent describes existing smart card devices having built-in microprocessors with cryptographic capabilities. '538 *Patent*, 1:42-45. These smart card devices, and existing RFID credit card devices, require contact with a reader to perform a transaction. *Id.*, 1:45-62. The '538 Patent notes that these cards 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” as an added security feature. *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 unless noted otherwise below.² Unless noted, the below analysis would not change under the AIA.

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 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.

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.

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	1-5, 7-18	Lin (EX1004), Smith (EX1005), Varadarajan (EX1006), Hammad (EX1007)
2	6	Lin, Smith, Varadarajan, Hammad, Kranzley (EX1008)

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
Lin	8/11/2009	4/8/2010	§102(b)
Smith	11/17/2009	5/20/2010	§102(b)
Varadarajan	1/25/2011	7/28/2011	§102(b)
Hammad	6/18/2007	6/22/2010	§102(b)
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. Lin

Lin teaches “electronic devices configured to initiate and process” financial transactions, including using near field communications (“NFC”). *Lin*, Abstract, 1:6-8. Before initiating a payment transaction, Lin teaches a user may enter credit card information for one or more accounts in the application, which information is verified by the card issuer and stored on the portable device. *Id.*, 3:2-6, 37:16-22, 38:17-39:31, 40:19-42:2, Figs. 5A-5B. The credit card information includes card number, expiration date, and CVV values. *Id.*, 31:25-32:6, 37:16-20, 40:19-28. The portable device is further configured to initiate payments by transmitting payment information to another device using a transaction application on the device. *Id.*, 3:16-22, 14:22-25, 20:4-9, 31:16-28, 55:7-56:5, Figs. 1 (icon 34), 11B. Lin further teaches

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.

that payment information is sent and received via NFC. *Id.*, 3:29-4:5, 14:5-9, 19:13-20:9, 24:19-25:21, 31:1-15, 56:21-60:2, Figs. 12A-C, 13, 14B, 14I, 15B.

B. 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].

C. 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 specific amount of time or uses. *Varadarajan*, [0023].

D. 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. Ex. 1011, [0035]-[0042]; *Hammad*, Abstract, 4:21-6:42.

E. 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.

F. 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 Lin*, Abstract, 1:6-9, 3:1-4:5, Figs. 1, 3-4, 11A-B; *Smith*, Abstract, [0021]-[0023], Fig. 1; *Varadarajan*, Abstract, [0002]-[0020], Fig. 1; *Hammad*, Abstract, 2:12-20, Fig. 6 *and Hammad '089 Provisional*, [0002]-[0003]; *Kranzley*, Abstract, [0010], Figs. 1B, 3; *Dec.*, ¶¶90-107.

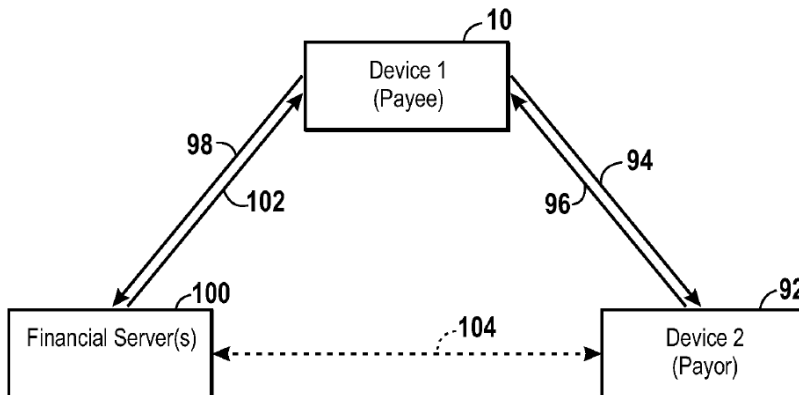
Further, each of the applied prior art references is reasonably pertinent to problems addressed by the '538 Patent such as increasing security of payment transactions. *Compare* '538 Patent, 1:24-28, 1:63-2:4, 9:21-28 *with Lin*, 26:27-27:14; *Smith*, [0002], [0015], [0020]; *Varadarajan*, [0005], [0009]-[0010]; *Hammad*, 1:17-2:6 *and Hammad '089 Provisional*, [0002], [0036]; *Kranzley*, [0003], [0065]; *Dec.*, ¶¶90-107.

V. GROUND 1: CLAIMS 1-5, 7-18 ARE OBVIOUS OVER *LIN*, *SMITH*, *VARADARAJAN* AND *HAMMAD*

A. Claim 1

- 1. *1(Pre): A method of performing a payment transaction, the method comprising:***

Lin teaches a method of performing a payment transaction⁴ using a portable device. *Lin*, Abstract, 1:6-8, Fig. 1.



Lin, Fig. 4.

Specifically, a payee transmits an invoice to a payor that, in turn, provides payment information to the payee. *Id.*, 52:25-53:9, 55:7-25. A financial server subsequently authorizes the transaction and the payor is informed. *Id.*, 53:15-55:6, 55:26-56:5.

⁴ Claim language identified with *italics* and underline.

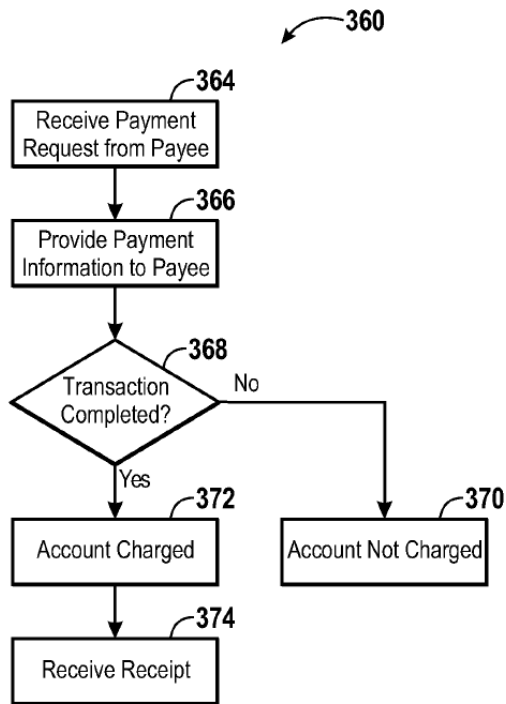


FIG. 11B

Lin, Figs. 11B; *see also* Fig. 11A.

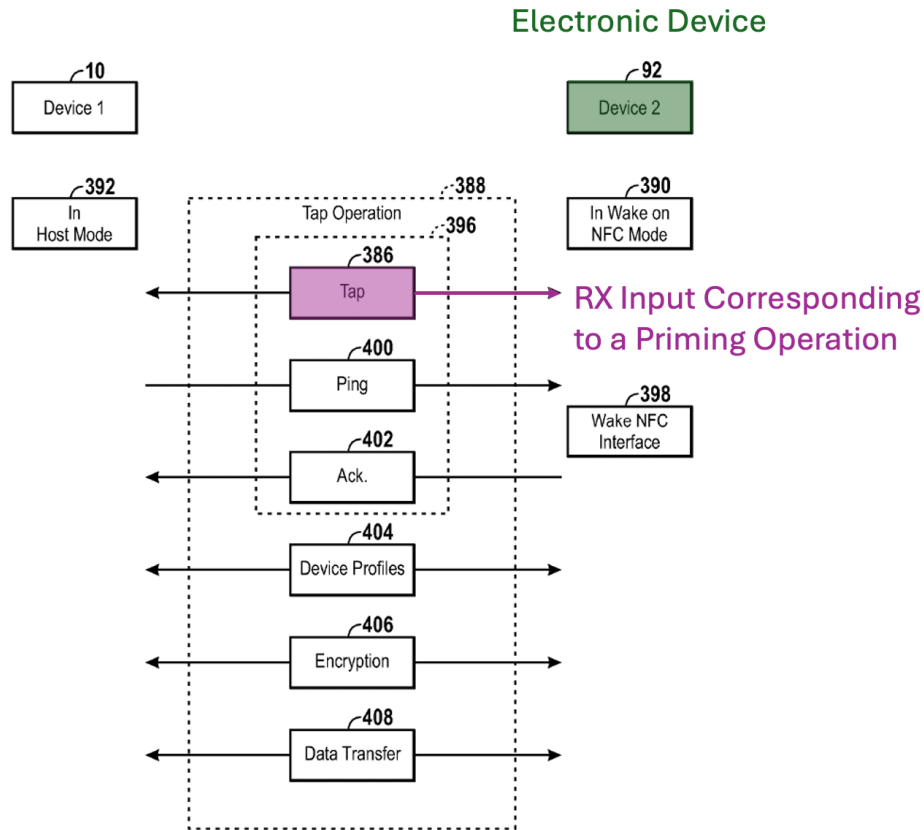
2. ***1(a): receiving an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user; and,***

Lin teaches receiving an input at a cellular phone (electronic device) corresponding to an NFC tap operation by an authorized user.

Lin teaches an “electronic device,” such as a cellular phone, having a transaction application for conducting a transaction. *Lin*, 14:22-29, Fig. 1. The electronic device receives input of an NFC tap operation, which is “the action of placing one NFC-enabled device within the proximity of one or more additional NFC-enabled devices such that an NFC-based connection may be established

between the devices,” to initiate a transaction between the two NFC-enabled devices.

Lin, 56:9-12, 57:3-6; *see also id.*, 56:28-58:9.



Lin, Fig. 13 (annotated).

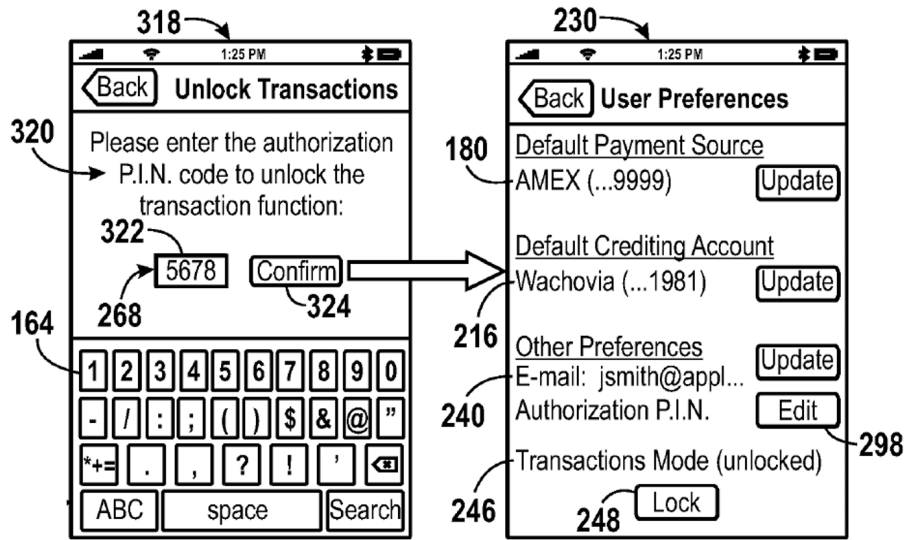
This mapping is consistent with the '538 Patent's description that bringing a device within range of a reader may form part of the priming operation. '538 *Patent*, 13:65-14:1 (“The priming action can be a tap of the multi-function electronic device 601a, or tapping the multi-function electronic device 601a against the multi-function electronic device 601b.”).

As discussed in more detail in Claim 1(b) below, the NFC tap operation is performed by an authorized user who has “unlocked” transactions by “providing an authorization PIN[.]” *Lin*, 47:25-29.

3. ***1(b): wherein [⁵] authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface, a gesture sensor, a motion sensor, and a biometric sensor; and,***

Lin teaches authorizing a user of the electronic device by recognizing a PIN (*user input*) entered on a touchscreen display (*human input sensor*). Lin teaches security features that “prevent the device 10 from being used to make payments by unauthorized persons.” *Lin*, 28:13-15. Specifically, the user is “unable to send or receive payments using the device” until the device’s transactions application is “unlocked upon [the user] providing an authorization PIN[.]” *Lin*, 47:25-29; *see also, id.*, 28:4-15, 47:27-29. As shown in FIG. 10B, the user inputs an authorization PIN using “numerical keyboard 164[.]” which is “provided for entry of the authorization PIN 268 into the text field 322.” *Lin*, 52:1-15; *see also* 75:5-13, Fig. 9.

⁵ The word “the” was deleted in a May 10, 2022 Certificate of Correction.



Lin, Fig. 10B (excerpt).

Lin's electronic device receives input of the PIN via "a touch screen interface" that "function[s] as an additional user input" and allows a user to "select elements displayed on the display 24 such as, for example, by touching certain elements using the user's finger or a stylus." *Lin*, 16:16-22; *see also, id.*, 20:26-30, 28:28-29:14, FIG. 3.

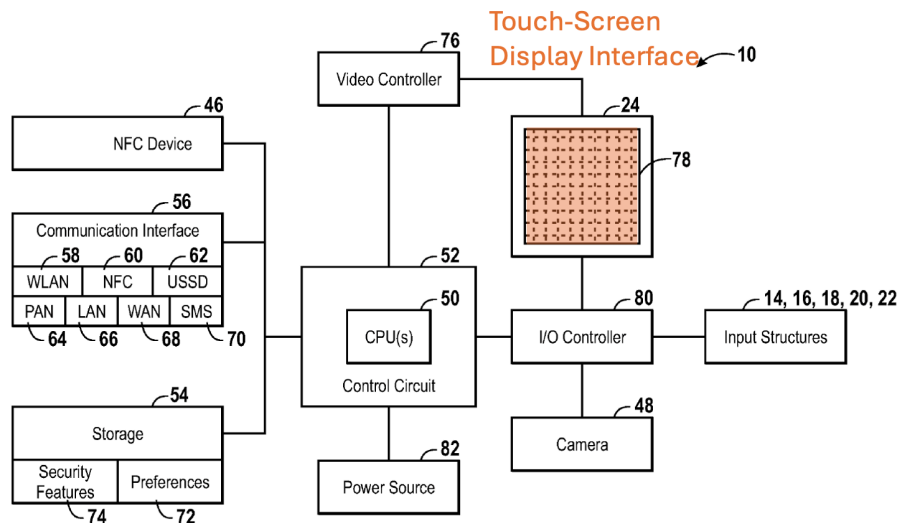


FIG. 3

Lin, Fig. 3 (annotated).

Thus, Lin teaches that the authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor (user input of authorization PIN using a touch-screen display interface), wherein the human input sensor is a touch-screen display interface.

4. 1(c): receiving a request for a transaction payment at said electronic device via an NFC interface of the device; and,

Lin teaches receiving a request for a transaction payment at the payor electronic device via its NFC interface. Specifically, Lin teaches the payor and payee devices include a NFC device and NFC interface. *Lin*, 31:1-3; *see also id.*, 19:13-20:9.

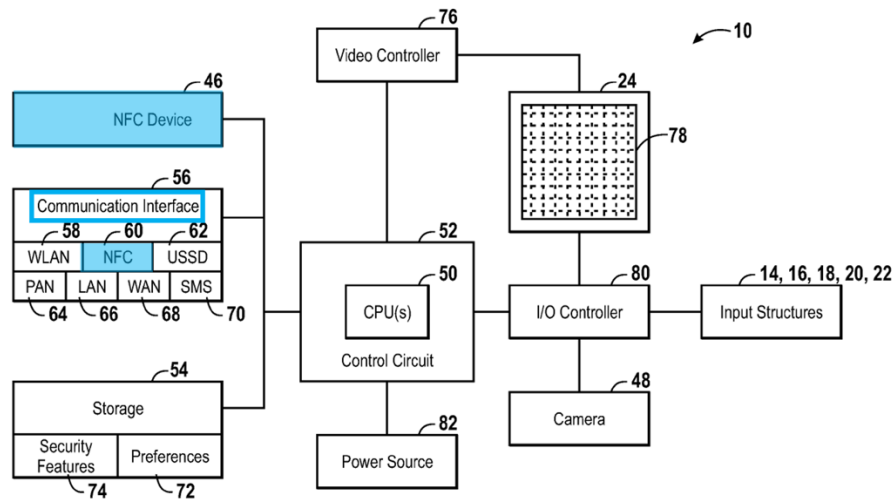


FIG. 3

Lin's payor electronic device receives a payment request, such as invoice information, from a payee device. *Lin*, 55:7-15; *see also id.*, 56:24-57:2, 67:25-27, Fig. 12A.

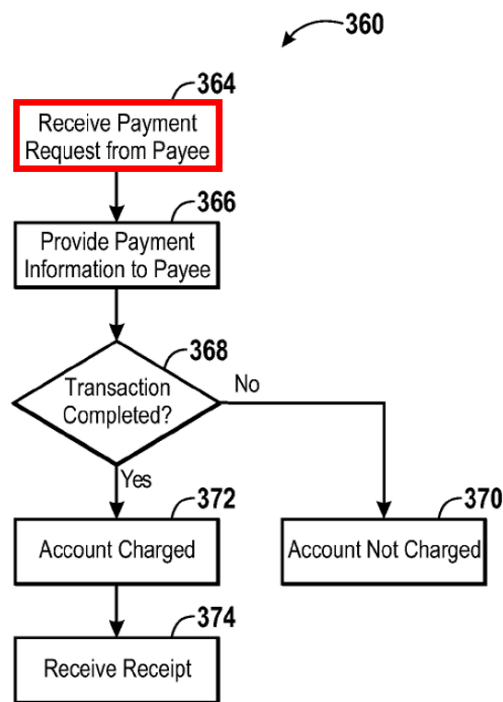
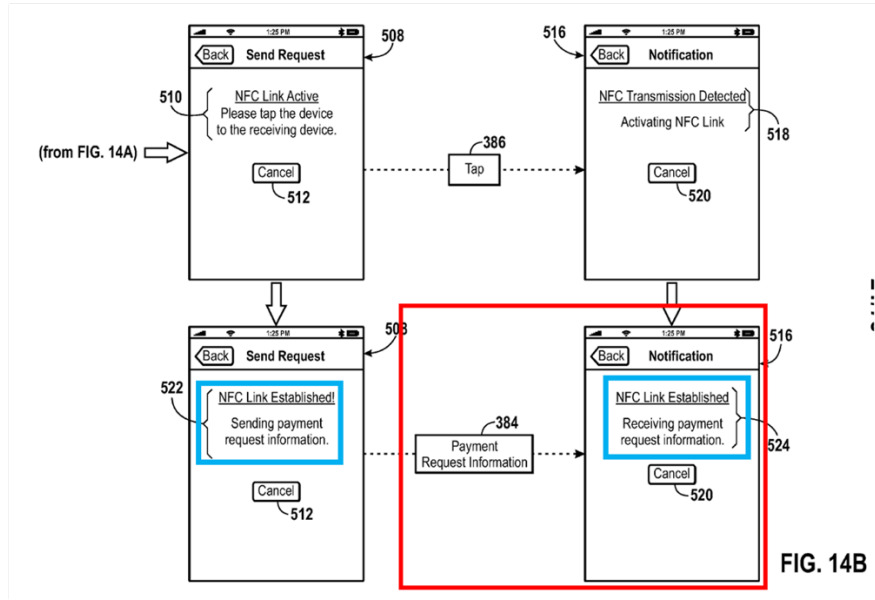


FIG. 11B

Lin, Fig. 11B (annotated).

The “payment request information is ... transmitted from the payee device 10 and received by way of the corresponding NFC interface 60 in the payor device 92.” *Lin*, 69:28-70:4; *see id.*, 55:19-22, 56:24-59:3, 59:16-18, 70:8-27, Figs. 13, 15A-B.



Lin, Fig. 14B (annotated).

5. ***1(d): displaying, on a display of the device, [the]⁶ request and at least a portion of an original static issuer-supplied payment account information associated with a [selected]⁷ payment method, for a user selection in paying the [I]⁸ request; and,***

Lin teaches displaying the invoice information (transaction payment request) and ... (at least a portion of an original static issuer-supplied account information associated with a payment) for selection by the user in paying the request.

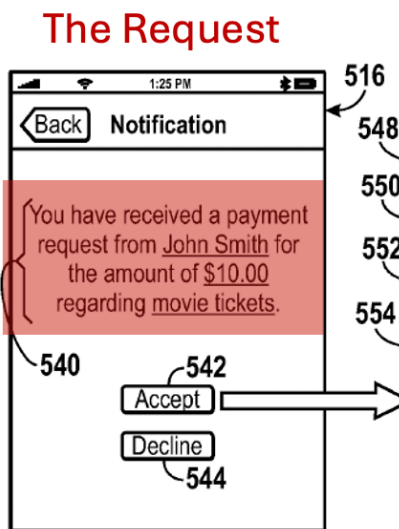
Specifically, Lin teaches that a payor device includes a “a display 24 configured to display various images generated by the device 10.” Lin, 16:7-8. The

⁶ The phrase “a transaction payment” was deleted and replaced with “the” in a May 10, 2022 Certificate of Correction.

⁷ The word “selected” was added in a May 10, 2022 Certificate of Correction.

⁸ The word “payment” was deleted in a May 10, 2022 Certificate of Correction.

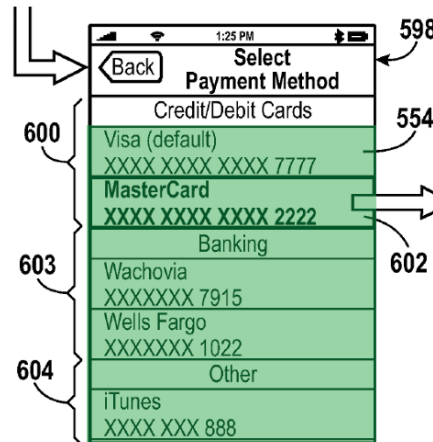
display “display[s] a graphical user interface (‘GUI’) 28 that allows a user to interact with the device 10.” *Id.*, 16:23-25. Figure 14E shows GUI “screens that may be displayed on payor device illustrating various methods for selecting a payment account in response to the payment request of FIG. 14A[.]” *Id.*, 8:6-8. As shown in FIG. 14E, “once the payment request information has been received by the payor device, the screen 516 may be updated to display the details 540 of the payment request, which may generally reflect information entered by the payee into the fields 496, 498, and 500 on the screen 492 of FIG. 14A.” *Id.*, 71:7-13.



Lin, Fig. 14E (annotated excerpt).

When paying the request, *Lin* also teaches GUI screen 598, which displays “a listing of all selectable payment accounts stored on the payor device 92, which may be provided by the screen 598.” *Id.*, 72:27-30; *see id.*, 70:28-71:6. The payor may choose to view all available payment accounts before making a payment account

selection. *Id.*, 72:24-73:3. Each available payment account represents a payment method.



At Least a Portion of an Original Static Issuer-Supplied Payment Account Information

Id., Fig. 14E (annotated excerpt).

As shown in Fig. 14E, the last four digits of each payment account (at least a portion of an original static issuer-supplied payment account information associated with a payment method) is displayed for a user selection in paying the selected request. The user then selects a payment account from the list to pay the selected payment request. *Id.*, 73:7-13; *see id.*, 55:12-19, 59:18-22, 75:14-17.

6. ***1(e): retrieving from a memory attached to a processor of the device, a device-specific static limited-use payment information, associated with said selected payment method; and,***

a) Lin's Teachings

Lin teaches an electronic device that includes a CPU (processor) attached to a storage device (memory) via a data bus. *Lin*, 20:26-21:12, 22:5-8.

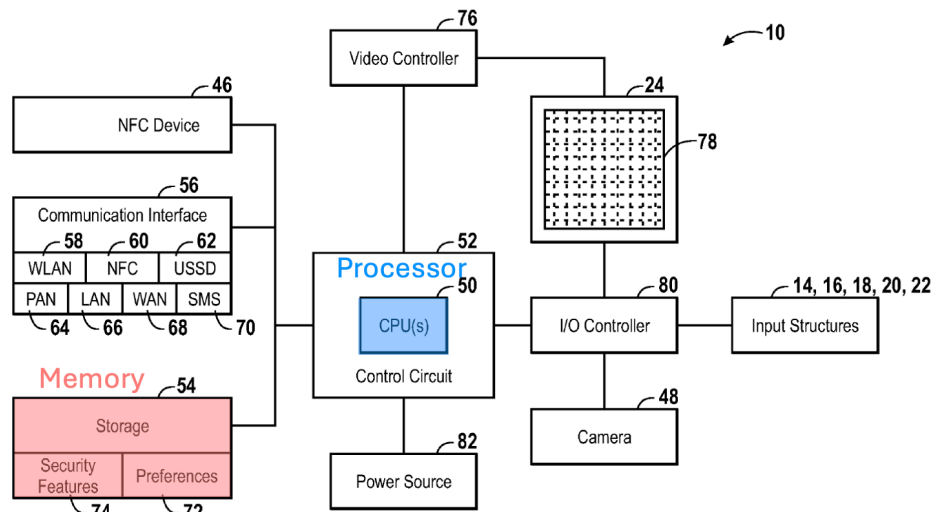


FIG. 3

Lin, Fig. 3 (annotated). *Lin* generally teaches “a secure access-restricted storage area (e.g., within the storage device 54) to limit access to the data that may be required by the certain aspects of the security features 74, such as encryption keys, passcodes and passwords, digital certificates, or the like.” *Lin*, 27:8-11. *Lin* also teaches that the portable device “initiates payments ... by transmitting payment information corresponding to a credit account stored on the device ... to an external device[.]” *Id.*, 3:17-21, 55:17-22, Fig. 11B. As discussed in Claim 1(d), *Lin* further teaches that the user is presented with payment account information from which the user selects an account to conduct the transaction (i.e., an account associated with said selected payment method). See *Lin*, 8:6-8, 70:28-30 (“[I]n response to a payment request 384 received from the payee device 10, may select an appropriate payment method on the payor device 92[.]”); see also, 70:28-71:6, 71:24-75:4, Figs. 14E-14G.

b) 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 is “assigned to the mobile device 104.” *Smith*, [0016]. The PPAN is “stored in the mobile device 204.” *Smith*, [0022]. The PPAN is used in an NFC payment transaction. *Smith (EX1005)*, [0022]. The PPAN is, therefore, a device-specific payment information. *Dec.*, ¶125.

Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith*, [0026], [0040]. The PPAN (device-specific payment information) 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 is a different number from the actual PAN.

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]. It was well known that a dual account number has separate and distinct numbers for each device the overall account is used on. *Dec.*, ¶127. Accordingly, *Smith*’s PPAN is a distinct payment information for a payment account on a particular “mobile device” (device-specific). *Id.*

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.*, ¶128.

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 (having an expiration date) and assigned to a mobile device, it is a device-specific static limited-use payment information associated with a payment method. *Dec.*, ¶129.

c) Motivation to Combine

A POSITA would have found it obvious and been motivated to store Smith’s PPAN in place of Lin’s payment account number. *Dec.*, ¶130. A POSITA would have appreciated that storing a PPAN would be safer than storing the actual account number on Lin’s device. *Dec.*, ¶130. Thus, this modification prevents bad actors from obtaining access to the actual account number if a user device is stolen. *Id.* A POSITA would have been motivated to configure the processor executing Lin’s mobile wallet application on the electronic device to retrieve the PPAN associated with the selected payment account from storage device to improve similar mobile wallet systems in the same way, i.e., preventing bad actors from accessing payment account numbers by not storing them on the mobile device. *Id.*

A POSITA would have had a reasonable expectation of success in implementing Smith's PPAN in Lin's payment application without undue experimentation because Lin already teaches use of an account number and a POSITA would have been familiar with using account number alternatives when making mobile payments. *Dec.*, ¶131. In the combination, Smith's PPAN would perform the same function—provide an alternative account number that can be used for a payment transaction. *Dec.*, ¶11; *Smith*, [0022]-[0023]. A POSITA would have understood that using Smith's PPAN in place of Lin's account number, such that the PPAN is retrieved from memory by Lin's processor, would be combining prior art elements according to known methods to yield the predictable result of increased security. *Dec.*, ¶131. A POSITA would have recognized that modifying Lin's system according to the teachings of Smith required only basic software modifications and routine skill. *Dec.*, ¶132. For example, because the constituent hardware components are largely the same, a POSITA would realize that the electronic device of Lin could be modified to incorporate Smith's PPAN into device memory. *Id.*

The simple substitution of Lin's account number with Smith's PPAN is a substitution of one known element for another and a POSITA would have understood that the substitution would have predictably increased the security of Lin's payment system and protected the user's sensitive PAN information. *Dec.*, ¶133. Because Smith's PPAN is used in a transaction in the same way as a payment

account number in Lin, there would have been a reasonable expectation of success configuring Lin's device to use the processor to retrieve the PPAN from memory to make payments using the PPAN, as such would have been a combination of known elements that would yield predictable results of increased security because the PAN is not transmitted. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007); *Dec.*, ¶133.

7. ***1(f): dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method; and,***

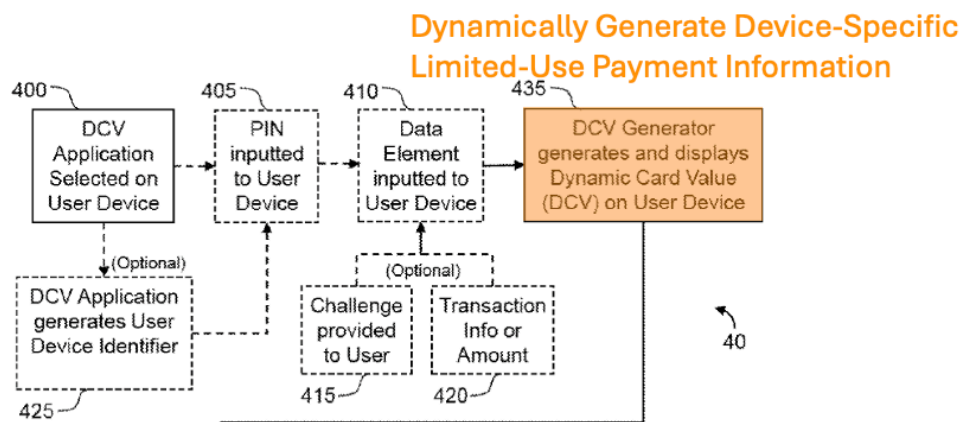
It would have been obvious to modify Lin-Smiths to dynamically generat[e], by a processor of the device, device-specific limited-use payment information, for said selected payment method in view of Varadarajan. *Dec.*, ¶¶134-144.

a) Varadarajan's Teachings

Varadarajan teaches a similar mobile payment application on a mobile user device for conducting contactless payment transactions. *Varadarajan*, [0011], [0032], [0038]-[0039], [0041]. Specifically, the "user downloads the DCV application to his mobile user device, which can be virtually any hand-held platform[,]" including "'smart' phones such as the ... iPhone™[.]" *Id.*, [0026]. A DCV generator, generated by the issuer/card provider, on the user device may be identified by a logo associating it with the card provider, which is then selected by the user through the application. *Id.*, [0038], [0045]-[0049], [0052] ("[T]he DCV

application can store DCV generators for multiple credit cards, debit cards, ... and for cards from different issuers or providers, on a single user device.”). Varadarajan recognizes that “[c]ard based transactions ... have certain security vulnerabilities[,]” including that “[t]he security of the CVV encoded on the magstripe can be compromised in a number of ways.” *Id.*, [0003], [0005], [0009].

To solve these problems, Varadarajan proposes using the DCV application and generator on the user’s mobile device to generate a dynamic card value (“DCV”), which is used to replace a static value, such as “a CVC, CVV, CSC, PAN, account number, partial PAN and a portion of an account number[.]” *Id.*, [0011]-[0012], [0020]-[0021] (“The DCV is configured and provided in the same form as the static DCV for which it is being substituted.”).



Varadarajan, Fig. 4 (annotated excerpt).

The DCV is provided over “any of a number of contactless communication technologies, including but not limited to Bluetooth, RFID, transponders, proximity

card communication techniques, and other methods known to those skilled in the art of near field communication technologies.” *Varadarajan (EX1006)*, [0032].

The DCV is limited use in that it expires “after a limited number of uses, which may be a single use[,]” which limits attacks on credit/debit card transactions. *Id.*, [0023]; *see also*, [0020]; *Dec.*, ¶138.

Varadarajan teaches, and a POSITA would understand, the 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” such that “the included device identifier is unique to each user device ... [and] each transaction and DCV is further identifiable to the user device conducting a transaction or requesting a DCV.” *Varadarajan*, [0029], [0053]; *see also*, [0043], [0049], [0054]; *Dec.*, ¶139.

Thus, Varadarajan’s DCV is device-specific limited-use payment information that is dynamically generated for a specific payment method (e.g., specific credit card).

b) Motivation to Combine

Based on the teachings of Varadarajan, it would have been obvious to configure the processor of the Lin-Smith electronic device to dynamically generate a DCV to be used in place of a CVV. *Dec.*, ¶¶141-144.

As noted above, the Lin-Smith PPAN prevents attackers from accessing a primary account number from an electronic device that has been lost or stolen. However, a POSITA would have understood that the Lin-Smith electronic device would still be vulnerable to attacks where the PPAN and CVV values are intercepted by an attacker and used for fraudulent transactions, as taught by Varadarajan. *Dec.*, ¶141. To prevent this type of attack, a POSITA would have been motivated to configure the Lin-Smith processor to implement Varadarajan's method of dynamically generating a DCV to be used in place of the selected payment method's CVV to improve similar mobile payment systems in the same way. *Id.*

The concept of dynamic CVVs was well-known at this time and a POSITA would have been familiar with using such numbers in connection with mobile payment transactions. *Dec.*, ¶142. The substitution of Varadarajan's DCV with Lin-Smith's CVV with Varadarajan's DCV is a substitution of one known element for another and a POSITA would have understood that the substitution would have predictably increased the security of Lin-Smith's payment system and further protected the user's sensitive account information. *Id.*

A POSITA would have appreciated that this would have predictably prevented the risk of attacks where the PPAN and CVV are stolen by an attacker even if the user's mobile device has not been lost or stolen. *Dec.*, ¶143. Likewise, because the PPAN is still being used in place of the PAN, the Lin-Smith-Varadarajan

device would still retain the benefits of allowing the user to easily cancel PPANs without cancelling the payment devices in his or her mobile wallet if the mobile device is lost or stolen, while also increasing security by preventing fraudsters from stealing the payment device data required to perform transactions. *Id.*

A POSITA would have had a reasonable expectation of success in modifying Lin-Smith in this way because Lin-Smith already teaches a transaction application for conducting payment transactions. *Dec.*, ¶144. Thus, a POSITA would have recognized that modifying Lin-Smith’s system according to the teachings of Varadarajan required only basic software modifications and routine skill. *Id.* For example, because the constituent hardware components are largely the same, a POSITA would realize that the electronic device of Lin-Smith could be modified to incorporate Varadarajan’s DCV into the payment information transmitted during the payment transaction. *Id.* As such, the modification would have been a combination of known elements that would yield predictable results of more secure payment transactions by dynamically generating a code verification value. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007); *Dec.*, ¶144.

8. *1(g): using said limited-use payment information[s]⁹ in place of at least a portion of said selected original issuer-supplied*

⁹ The word “information” was replaced with “informations” in a May 10, 2022 Certificate of Correction.

payment information for the transaction; and,

For the reasons discussed above, it would have been obvious to a POSITA to use Varadarajan's DCV (said limited-use payment information) in place of the selected payment method's CVV values (a portion of said selected original issuer-supplied payment information for the transaction). See Claim 1(f); Dec., ¶145.

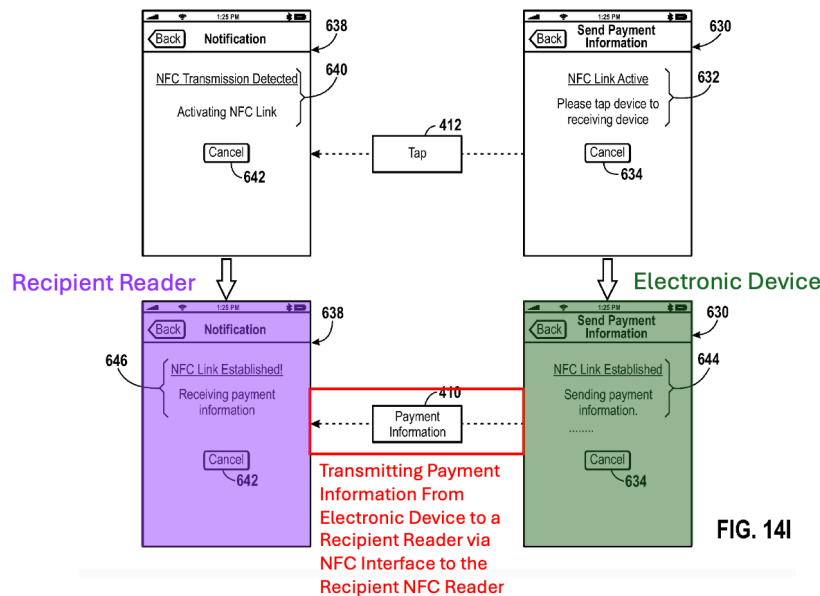
- 9. 1(h): combining [1]¹⁰ said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information; and,**

Per Lin, complete device payment information for a credit card includes card number, expiration date, and CVV values. Lin, 37:16-20, Fig. 5A; see also id., 31:29-32:6, 40:19-28. As discussed above, it would have been obvious to replace the card number/PAN with the PPAN (said static limited-use payment information), and the CVV with the DCV (said dynamically generated limited-use payment information). See Claims 1(e)-(f); Dec., ¶146. Thus, it would have been obvious to further configure Lin's electronic device to combine the PPAN and DCV as a substitute for the card number and the CVV to form complete device payment information for the same reasons. Id., Dec., ¶146.

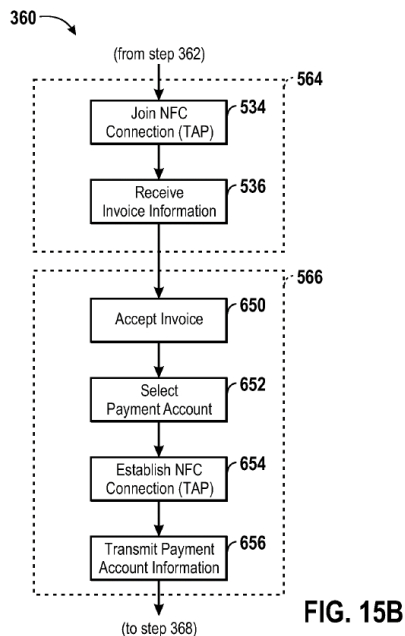
- 10. 1(i): transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction; and,**

¹⁰ The word "of" was deleted in a May 10, 2022 Certificate of Correction.

Lin teaches transmitting “payment account information 96 may similarly be transmitted from the payor device 92 to the payee device 10 by way of the previously established NFC connection through each device’s respective NFC interface 60[.]” *Lin*, 32:1-4; *see also* Claim 1(c). Specifically, Lin’s electronic device 92 transmits the payment account information to a payee device 10 (*a recipient reader*) via the NFC interface to the payee device’s NFC reader (*the recipient NFC reader*). *Lin* at 31:29-32:6, 59:22-60:2, 55:17-25, 77:1-8, Fig. 11B, FIG. 14I.



Lin at Fig. 14I (annotated).



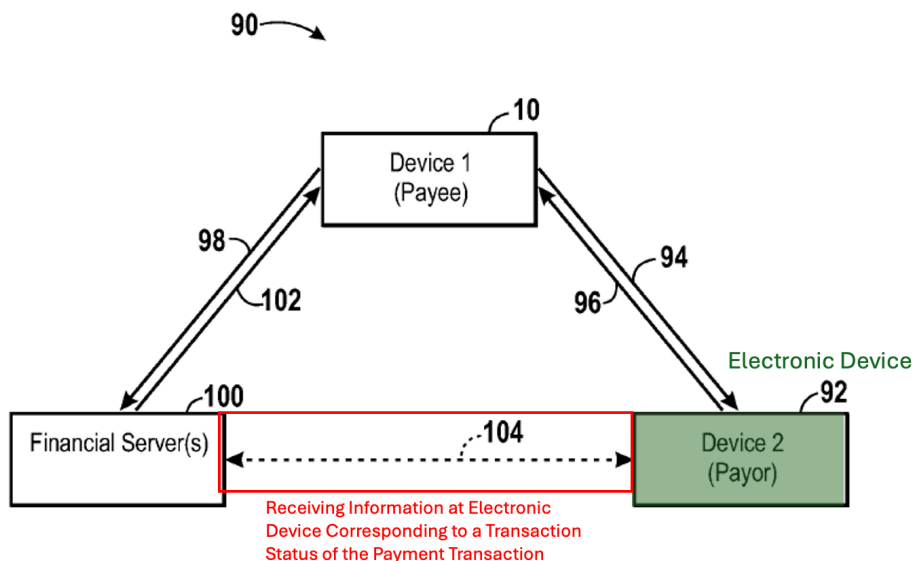
Lin at Fig. 15B.

The payee device subsequently transmits the transaction information “to one or more financial servers 100 for verification of the account information and the subsequent authorization and processing of the requested payment.” *Id.* at 32:20-27; *see also id.* at 53:5-23, 54:26-55:6, 60:6-12, 60:24-61:30, 79:24-80:3, 80:25-82:17, Figs. 11A, 15B.

As discussed above, the combination of Lin-Smith-Varadarajan teaches said complete device payment information. *See* Claim 1(h); *Dec.*, ¶¶147-149. Thus, the Lin-Smith-Varadarajan combination also teaches transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction for the same reasons. *Dec.*, ¶¶147-149.

- 11. 1(j): receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the [1]¹¹ complete device payment information by a payment processor authority and a payment issuer authority; and,**

Lin teaches that the electronic device receives “a confirmation message in the form of an electronic receipt, represented herein by reference numeral 104 to the payor device 92 if the transaction is processed successfully.” *Lin*, 35:24-28. The payment receipt “may be transmitted to the payor by the payee, either directly via the payor device 10, or indirectly via one of the financial servers[.]” *Id.*, 55:1-6; *see also id.*, 35:24-30, 55:29-56:5, 61:23-30, 83:19-27, Figs. 11B, 12A, 15A, 16A.



Lin at Fig. 4 (annotated).

¹¹ The word “transmitted” was deleted in a May 10, 2022 Certificate of Correction.

“The electronic receipt 104 may serve as acknowledgment that the requested payment has been satisfied by the payor and received by the payee.” *Id.* at 35:28-30. Thus, the confirmation message is information ... corresponding to a transaction status of the payment transaction.

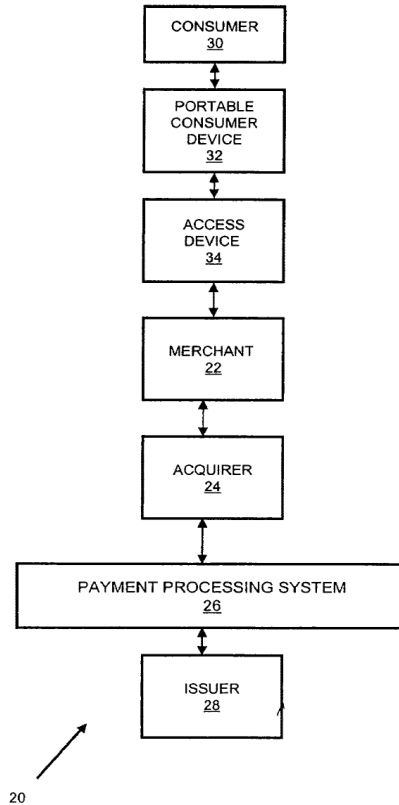
The validation of the payment information is performed by “financial servers 100[,]” which in one embodiment include a credit card verification server “which maintains the payor’s selected credit card account, such as American Express® or MasterCard®.” *Id.*, 33:8-34:24; *see also id.*, 53:15-23, 60:6-61:4, 61:9-30, Figs. 11A, 12A. The credit card verification server “verif[ies] whether the credit card account information ... corresponds to a valid credit card account belonging to the specified payor” and whether the line of credit has sufficient funds. *Id.*, 34:1-10. A POSITA would understand that such a credit card verification server, e.g., operated by MasterCard, is a payment processor authority, because it validates the credit card account, and a payment issuer authority, because it is authorizes issuance of the card. *Dec.*, ¶152.

Alternatively, and to the extent Patent Owner argues that Lin’s verification server does not teach a payment processor authority and a payment issuer authority, it would have been obvious to use these components in Lin’s financial servers based on the teachings of Hammad. *Dec.*, ¶153.

a) Hammad’s Teachings

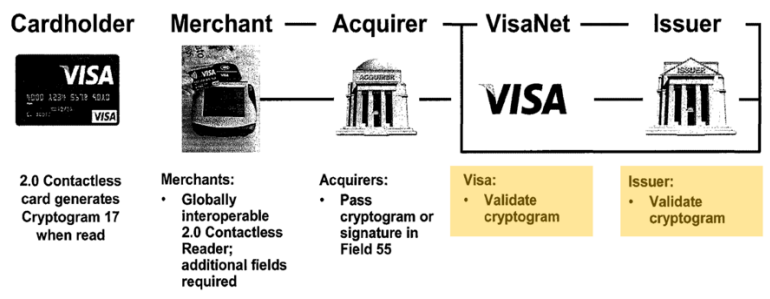
Hammad describes generating a dynamically generated card verification value (“dCVV”) using an application on a mobile device for use in a mobile payment transaction, including contactless transactions. *Hammad*, 2:65-3:11, 3:51-4:6. The dCVV is embedded in payment data that is sent to a service provider for validation via a payment network. *Id.*, 7:43-46, 7:55-61. A service provider is defined as a “payment processing organization or an issuer of the portable consumer device.” *Id.*, 2:18-20. The service provider, which is the payment processor or issuer, validates the payment data, including the dCVV. *Id.*, 2:18-20, 7:29-8:44.

Hammad ’089 Provisional describes a common architecture for processing payments involving a credit card that includes a merchant, acquirer, payment processing system (a payment processor authority), and issuer of the portable consumer device (a payment issuer authority), among other components. *Hammad ’089 Provisional (EX1011)*, [0012]-[0013].



Hammad '089 Provisional, Fig. 1.

The payment processing system is able to “process credit card transactions” and forward authorization requests to the issuer for authorization. *Id.*, [0016], [0021]-[0022]. Hammad '089 Provisional further describes that the payment processing system and issuer “validate cryptogram[,]” i.e., the DCV/dCVV.



Hammad '089 Provisional, p. 78. Hammad teaches, and a POSITA would have understood, that some entities, Discover and American Express, perform the functions of payment processor and issuer. *Id.*, [0025]; *Dec.*, ¶156.

b) Motivation to Combine

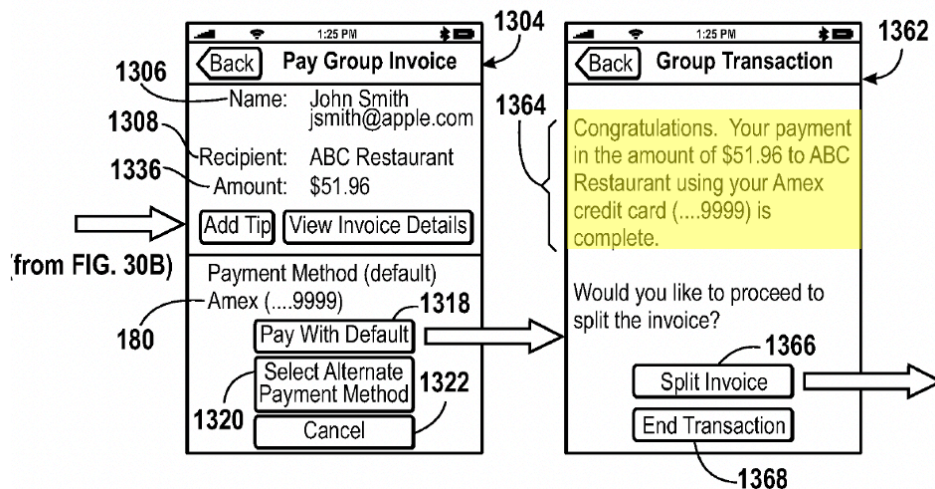
Based on the teachings of Hammad and Hammad '089 Provisional, it would have been obvious, and a POSITA would have been motivated to implement the Lin-Smith-Hammad-Varadarajan device with the payment processing architecture, including a payment processing and issuer system, as described in Hammad. *Dec.*, ¶157. A POSITA would have recognized that the payment processing system and issuer are similar to Lin's one or more financial servers. *Id.* A POSITA would have understood that a payment processing server and issuer, as described in Hammad, were commonly used to process authorization requests, and we often the same entity. *Id.* Thus, it would have been obvious to implement the known elements of Hammad's payment processing and issuer server in Lin's financial servers according to known methods to process a payment transaction. *Id.* Given the ubiquity of separate payment processing and issuer servers, there would have been a reasonable expectation of success. *Id.*

12. 1(k): visually conveying the transaction payment authorization status via a user-interface displayed on said display.

As discussed in Claim 1(j), Lin teaches that the electronic device 92 receives “a confirmation message in the form of an electronic receipt, represented herein by

reference numeral 104, to the payor device 92 if the transaction is processed successfully.” *Lin*, 35:24-28, Fig. 4; *see also* Claim 1(j). *Lin* further teaches that “a payment receipt may be transmitted to the payor by the payee ... directly via the payor device[.]” *Id.*, 55:1-3. A POSITA would have understood that the confirmation message/payment receipt received by the payor would be displayed on the user-interface. *Dec.*, ¶158.

Alternatively, this limitation is rendered obvious by *Lin*. *Lin* teaches another embodiment where “if the primary transaction 1172 is authorized by the financial servers 100” the electronic device displays a screen including “the notification message 1364 indicating to the initiator that the group invoice 180 has been paid using the selected default payment account 180.” *Lin*, 131:29-132:2.



Lin. Fig. 30C (annotated excerpt).

Based on this express teaching, it would have been obvious, and a POSITA would have been motivated to configure *Lin*’s electronic device to visually convey

the confirmation message 104 (*transaction payment authorization status*) *via a user-interface displayed on said display* for every transaction completed by the device. *Dec.*, ¶160. It was well known to POSITAs that users expected feedback to let them know when a transaction was successfully completed. *Id.* Visual feedback was a well-known and reliable way to provide this feedback to users. *Id.* Indeed, Lin already teaches providing the payor device with a confirmation message. *Id.* Thus, there would have been a reasonable expectation of success configuring Lin's device to generate a screen displaying a notification message to visually convey whether a transaction was authorized or not. *Id.*

B. Claim 2

- 1. 2: The method of claim 1, further comprising receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.**

Lin teaches that “the payee device 10 may also transmit a confirmation message [104] in the form of an electronic receipt [*confirmation*] ... to the payor device 92 if the transaction is processed successfully.” *Lin*, 35:24-30, Fig. 4; *see also id.*, 54:26-55:3, 56:2-5, 85:7-19, Figs. 11B, 16A; *see also*, Claim 1(j).

As discussed above, the payor device (*electronic device*) and the payee device (*NFC payment reader facility*) communicate via *said NFC interface*. *See* Claim 1(c); *see also Lin*, 20:4-9, 62:4-8. The transaction processed successfully if the credit card verification server “determines that the specified credit card account is valid and is

authorized to make the requested payment[.]” *Lin*, 34:1-10, 62:9-18, Figs. 4, 12A; *see also* Claim 1(i). In the Lin-Smith-Varadarajan-Hammad combination, the payment information that is authorized by the server is said complete device payment information. *See* Claim 1(h). Thus, the Lin-Smith-Varadarajan-Hammad combination also teaches receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.

C. Claim 3

- 1. 3: The method of claim 1, further comprising receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device.**

Lin teaches that the “financial servers 100 ... transmit a confirmation message [104] in the form of an electronic receipt ... to the payor device 92 if the transaction is processed successfully.” *Lin*, 35:24-30, 55:4-6, Fig. 4 (depicting receipt of confirmation message 104 from servers 100). As discussed in Claim 2, the payor receives the confirmation message over an NFC interface.

In addition to the NFC interface, Lin’s device also includes “a plurality of communication interfaces 56[.]” *Lin* at 20:23-30; 14:31-15:7.

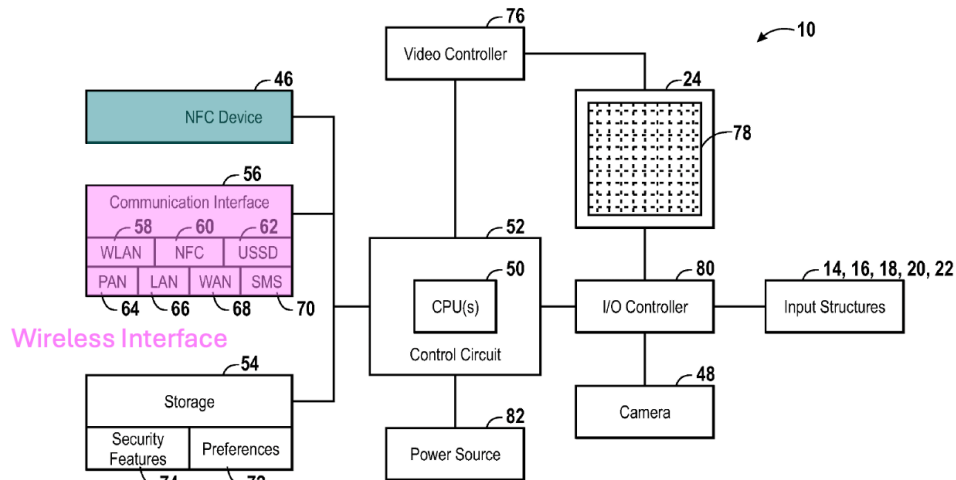


FIG. 3

Lin, Fig. 3 (annotated).

Thus, Lin teaches receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least ... NFC interface. Dec., ¶165

Lin's communication interfaces 56 also include wireless interfaces including "a wireless LAN, such as an IEEE 802.11 x wireless network" and "a cellular data network, such as the Enhanced Data rates for GSM Evolution (EDGE) network or the 3G network (e.g., based on the IMT-2000 standard)." Lin, 22:21-23:30. Lin teaches that a payment receipt can be sent by the financial server to the payor device over these network connections "established by way of a common networking interface available on the ... payor device[.]" Lin, 61:30-62:4, Figs. 4, 11A, 12A. As discussed above, Lin's financial servers including a credit card verification server, which a POSITA would understand to include a payment processing authority. See

Claim 1(j). It would have been obvious for the confirmation message 104 to be received from the financial server (payment processing authority) via a wireless interface of the payor device. *Dec.*, ¶166.

Alternatively, it would have been obvious for Lin's financial servers to utilize Hammad's payment processing system (a payment processing authority). *See* Claim 1(j). For the same reasons, it would have been obvious to configure Lin's payor device 92 to receive the confirmation message indicating that the transaction has been processed successfully (said confirmation result of said complete device payment information authentication status) from Hammad's payment processing system. *Id.*; *Dec.*, ¶167.

D. Claim 4

- 1. 4(a): The method of claim 3, wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment transactions performed by said device, in place of said selected issuer-payment information; and,**

For the reasons discussed in Claim 1(f), it would have been obvious to configure Lin's electronic device to generate a DCV (device-specific limited-use payment information) as taught by Varadarajan. As discussed, the DCV is used to replace issuer provided information, such as the "a CVC, CVV, CSC, PAN, account number, partial PAN and a portion of an account number[.]" *Id.*; *see also*, *Varadarajan*, [0012]-[0013]. Varadarajan further teaches the verification values,

such as the CVC, CVV, and CSC values are limited-in-use to specific issuer payment methods. *Varadarajan*, [0007].

When using the DCV generator, “the DCV application ... generate[s] a user device identifier.” *Varadarajan (EX1006)*, [0054]. There is a DCV generator for each card, e.g., selected issuer payment method. *Varadarajan (EX1006)*, [0052] (“[T]he DCV application can store DCV generators for multiple credit cards, debit cards, other DCV authorized payment or transaction cards, and for cards from different issuers or providers, on a single user device.”). A POSITA would have understood, therefore, that in the DCV generation process the mobile device utilizes a unique device [e.g., device identifier] generated information. *Dec.*, ¶168. A POSITA would have been motivated to the use a device identifier in the DCV generation process to “further increase user security ... by detecting whether the application has been ported to another (unauthorized) device by an attacker.” *Varadarajan (EX1006)*, [0052] [0054]; *Dec.*, ¶168.

Thus, for example, it would have been obvious to configure Lin’s device to dynamically generate the DCV to replace a CVV (said selected issuer-payment information). *Dec.*, ¶169.

Thus, the combination of Lin and Varadarajan also teaches wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment

transactions performed by said device, in place of said selected issuer-payment information. See Claim 1(f).

2. ***4(b): wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.***

Varadarajan teaches that the proper verification value must be included in the payment information in order to complete a card-based transaction. *Varadarajan* at [0003], [0024], [0043]. Specifically, if the device-generated DCV (device generated limited-use information) does not match the authority-generated DCV, the transaction will not be authorized (device account information will be rejected as invalid).

Hammad teaches that if the service provider generated dCVV does not match the dCVV provided by the mobile device (device generated limited-use information), the transaction is terminated (device account information will be rejected as invalid). *Hammad*, 3:36-40, 8:47-50, Fig. 6.

Thus, it would have been obvious that when modifying Lin-Smith-Varadarajan-Hammad to include generation of DCV/dCVVs, Smith's PPAN (device account information) would be rejected if the DCV/dCVV generated by the device does not match the authority-generated DCV/dCVV (device account information will be rejected as invalid). *Dec.*, ¶172.

E. Claim 5

- 1. 5(a): The method of claim 3, wherein the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information; and,**

As discussed above, Varadarajan teaches generating a DCV (limited-used payment information) for use in a financial transaction. *See* Claim 1(f); *Varadarajan*, [0011], [0015], [0020], Fig. 4. Varadarajan teaches that the DCV generator includes a “device identifier” (device-unique information) or PIN (payment processing authority recognizable information) that identifies the user device conducting a transaction or requesting a DCV. *Id.*, [0053]. In addition to the device information, account number, and CVV, the DCV generator can also use a “data element[,]” e.g., a string of alphanumeric characters representing a “challenge[,]” or transaction related information, to generate a DCV which “authenticate[s] the user, user device ... or transaction to the provisioning server.” *Id.*, [0055].

a) Hammad’s Teachings

Hammad similarly teaches generating a dynamically generated card verification value (“dCVV”) using an application on a mobile device for use in a mobile payment transaction. *Hammad*, 2:65-3:11, 3:51-4:6. The dCVV 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 and/or ... the consumer generally.” *Id.*, 4:21-56; *see also* 4:62-7:5, Figs. 1-3. 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 combining this information with multiple encryption keys, including a master derivation key, to the dynamic and static data elements, resulting in a 3-digit dCVV. *Id.*, 5:34-6:39, Figs. 1-3. The master derivation key is provided by the service provider and used by the consumer device to derive additional keys and generate the dCVV. *Id.*, 5:38-57, Fig. 2.

A dCVV is generated for each transaction and included with other payment data. *Id.*, 4:61-65; *see also id.*, 4:61-6:34. The dCVV is embedded into the payment data, which includes the account number, service code, PVKI, and/or PIN verification data, and transmitted to the point of sale terminal and then to the service provider. *Id.*, 6:40-42, 6:49-7:28, 7:55-61, Figs. 4-5. The service provider uses the dCVV to determine the authenticity of the payment service. *Id.*, 7:29-46, 7:61-8:50, Fig. 6.

b) Motivation to Combine

Based on the teachings of Hammad, it would have been obvious, and a POSITA would have been motivated to include dynamic and static data elements, as taught by Hammad, in the DCV generation process as implemented in Lin-Smith-Varadarajan. *Dec.*, ¶160. For example, Hammad teaches generating a dCVV from “at least three or four” dynamic data elements and static data elements, which makes it “highly unlikely that a skimmer can determine a dCVV.” *Hammad*, 4:46-51. These data elements include an ATC (transaction sequence counter); service code, expiration date, or PIN verification data (payment processing authority recognizable information); information relating to a “portable consumer device” (device-unique information); and an account number associated with a portable consumer device, which are combined using a master derivation key. *Id.*, 4:21-5:5, 5:38-58.

Similarly, Varadarajan teaches combining a unique device identifier in its DCV generator (device-unique information) and “challenge” information from the service provider (payment processing authority recognizable information), among other information, to generate a DCV such that each DCV is “identifiable to the user device.” *Varadarajan*, [0053], [0055]. Varadarajan recognizes that it may be helpful to include additional data elements. *Id.*, [0055]. A DCV is generated using a DCV key, which is generated by the issuer by combining a card verification key with the user’s account number and service code. *Id.*, [0050].

A POSITA would have found it obvious to include this information in addition to Smith's e-wallet number (*device account number*), in the generation of a DCV. *Dec.*, ¶178. Indeed, Hammad teaches including at least three or four dynamic data elements and static data elements, including an account number, in the generation of a dCVV. *Id.* A POSITA would have recognized that including more data elements in generation of the DCV would decrease the likelihood that, even if the payment data were intercepted, that the DCV could be regenerated. *Id.* Therefore, a POSITA would have been motivated to include more data elements in generating a DCV in Lin-Smith-Varadarajan, as taught by Hammad. *Id.* Given Hammad's teachings regarding how to generate such a dynamic verification value, and that a dCVV can be used in a contactless transaction (like Lin, Smith, and Varadarajan), a POSITA would have had a reasonable expectation of success. *Dec.*, ¶¶178-179. A POSITA would have further recognized that modifications to Lin-Smith-Varadarajan-Hammad would be minimal as it would simply require additional inputs to Varadarajan's DCV generator, in addition to the PPAN and CVV. *Dec.*, ¶179. This modification of known techniques that would have yielded the predictable result of increasing security of the transaction. *Id.*

2. ***5(b): wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction; and,***

Hammad teaches generating a dCVV “for each transaction and for utilizing such value to verify that the payment service is authentic[.]” *Hammad*, 2:65-3:2; *see also id.*, 4:61-65. The dCVV is generated using at least two dynamic data elements that “change with each transaction[.]” *Id.*, 4:40-42. Specifically, because the dCVV is generated from the ATC, which will change with each transaction, the dCVV will also change. *Id.*, 4:22-33, 4:63-5:5; *Dec.*, ¶180.

As implemented in Lin-Smith-Varadarajan-Hammad, the DCV/dCVV is used to authorize a payment for the single transaction (*singular counted transaction*) for the selected payment method by the device. *Id.*

3. ***5(c): wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device; and,***

As discussed in Claim 1(j), Varadarajan teaches that an authenticating server (*payment processing authority*) “independently generate[s] one or more DCVs” (i.e., “verifiable dynamic CVVs”) “with an equivalent method” to the user device. *Varadarajan*, [0045]; *id.*, [0033], [0056]. The authenticating server “regenerates a DCV independently and compares it with the user provided DCV for validity[.]” *Varadarajan*, [0056]. If the device-generated and authenticating server-generated DCV match, the DCV is authenticated and the transaction is authorized. *Id.*, [0045], [0056], Fig. 4.

Hammad similarly teaches that a service provider (payment processing authority) can “independently re-generate the dCVV for the given transaction” utilizing an “analogous process as described above” for the consumer device. *Hammad*, 8:37-41. If the dCVVs match, the service provider deems the payment application to be authentic and the transaction is approved. *Id.*, 8:41-44, Fig. 6.

A POSITA would understand that in order to regenerate a DCV/dCVV independently and authorize a transaction, an authenticating server or service provider would need to use the same method and information elements used by the mobile device (comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device). *Dec.*, ¶184; Claim 5(a); see also Claim 5(f).

It would have been obvious to modify the Lin-Smith system with the teachings of Varadarajan and Hammad for the same reasons discussed in Claims 1(f), 1(j), and 5(a). *Dec.*, ¶185.

4. ***5(d): a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number; and,***

Varadarajan teaches that an authenticating server “independently generate[s] one or more DCVs” (i.e., “verifiable dynamic CVVs”) “with an equivalent method” to the user device. *Varadarajan*, [0045]; *see also*, [0033], [0056].

Hammad similarly teaches that “the service provider computer can independently re-generate the dCVV for the given transaction 645 utilizing a similar or analogous process” as described for the user device. *Hammad*, 8:37-41.

Hammad teaches that the dCVV can be generated from an ATC (device transaction sequence counter count), service code (issuer payment information), and information about the user (device user information). *See Hammad*, 4:21-60, 4:61-7:5, Fig. 1; *see also* Claims 1(j), 5(a). Hammad further teaches that the service provider compares a received ATC with “the corresponding ATC stored on the service provider computer” (expected device transaction sequence counter count). *Hammad*, 8:2-5, 8:41-47. Hammad also teaches that the service provider may determine if the other data elements match data elements at the service provider. *Hammad*, 8:9-11; *see also*, 9:23-27.

Smith teaches that the PPAN is stored at the financial institution server along with the actual account number. *Smith*, [0014]-[0016], [0034]-[0037], [0039]-[0040], Figs. 1-3, 5-6.

Thus, a POSITA would understand that in the proposed combination, the payment processing authority stores the ATC (device transaction sequence counter

count), wallet account number (*device account number*), actual account information (*expected issuer payment information*), and user information (*expected device user information*) in order to independently generate the DCV/dCVV during the authorization process. *Dec.*, ¶189. Further, a POSITA would understand that this information is, at a minimum, transitorily stored at the payment processing authority during the independent DCV/dCVV generation process. *Id.*

5. 5(e): an adjusting of said transaction sequence counter count on a per transaction basis; and,

Hammad teaches that the consumer device maintains an ATC that is initially set by the service provider and that can be “incremented with each transaction.” *Hammad*, 4:23-26. The service provider will then adjust its ATC with that received from the consumer device after the dCVV is authenticated. *Id.*, 8:41-47.

Thus, in the proposed combination, a POSITA would understand that ATC counter in the user device and at the payment processing authority are adjusted on a per-transaction basis. *Dec.*, ¶191. The use of ATC counters in connection with payment transactions was prevalent at the time and a POSITA would have been familiar with using such counter in connection with mobile payment transactions. *Id.* Thus, a POSITA would have recognized that implementing transaction counters in Lin-Smith-Hammad-Varadarajan required only basic software modifications and routine skill. *Id.* This modification would have been a combination of known

elements that would yield predictable results of increased security. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007); *Dec.*, ¶191.

6. ***5(f): an authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching.***

Varadarajan teaches that if the “user inputted DCVs are matched to verifiable DCVs, the inputted DCVs are authenticated to the transaction server[.]” *Varadarajan*, [0045]; *see also*, [0033], [0056]. If the device-generated and authenticating server-generated DCV match, the DCV is authenticated and the transaction is authorized. *Id.*, [0033], [0045], [0056], Fig. 4.

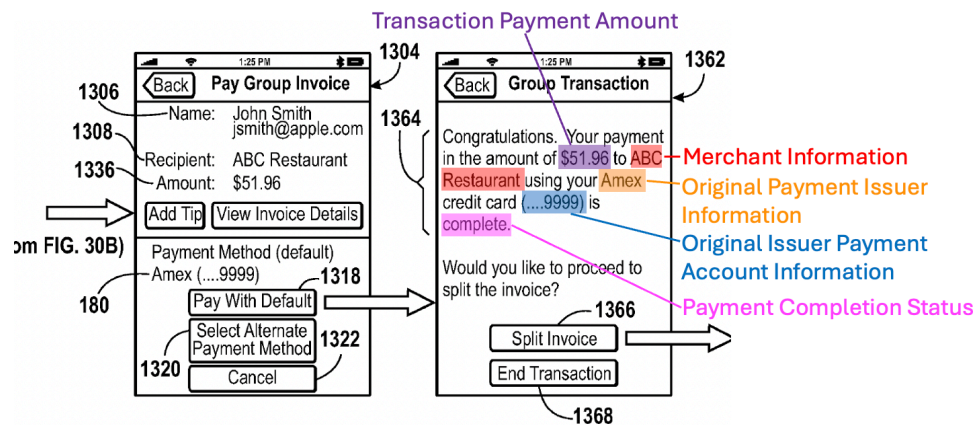
Hammad teaches that the service provider authorizes the payment transaction if the “generated dCVV matches the dCVV received from” the consumer device. *Hammad*, 8:41-44; *see also id.*, 2:36-39, 8:21-23. If the dCVVs match, “the service provider deems the payment application to be authentic” and the transaction is approved. *Id.*, 8:41-44, Fig. 6 (steps 650, 655).

Thus, a POSITA would understand that in Lin-Smith-Hammad-Varadarajan, the payment processing authority would authorize a transaction only if the device-generated and authority-generated DCV/dCVVs (limited-use payment transaction information) match. *Dec.*, ¶194.

F. Claim 7

1. **7:** *The method of claim 3, wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including: ... a transaction payment amount, ... a merchant information, an original issuer payment account information, an original payment issuer information, ... [and] a payment completion status.*

For the reasons described above, Lin teaches, or alternatively, renders obvious, visually conveying the received confirmation message in the form of an electronic receipt, such as shown in Figure 30C. *See* Claim 1(k). As shown below, the electronic receipt visually conveyed includes a transaction payment amount, a merchant information, an original issuer payment account information, an original payment issuer information, and a payment completion status.



Lin, Fig. 30C (annotated excerpt); *see also id.*, 131:29-132:2.

G. Claim 8

1. **8(a):** *The method of claim 1, wherein the generating the limited-use payment information is comprising: a device-specific account number; and,*

2. 8(b): a device-internal transaction sequence counter count; and,

As discussed in Claim 5(a), the Lin-Smith-Varadarajan-Hammad combination teaches generating limited-use payment information uses an e-wallet number (device-specific account number) and an ATC (device-internal transaction sequence counter).

3. 8(c): an information unique to the user and device which does not pass in the transaction; and,

The combination of Lin-Smith-Varadarajan-Hammad teaches, or renders obvious, generating the limited-use payment information unique to the user and device which does not pass in the transaction.

As discussed in Claim 1(f), Varadarajan teaches using a DCV generator to generate the DCV using a DCV key. *Varadarajan*, [0015], [0034] [0050]. The DCV key is information unique to a user because it is generated from user's account number, expiration date, and service code (information unique to a user) and the DCV generator uses a device identifier (unique to the user and device) to generate a DCV that is "identifiable to the user device ... requesting a DCV." *Id.*, [0049], [0053]. This information does not pass in the transaction. *Dec.*, ¶198.

4. 8(d): at least one payment authority-supplied information which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements, and

Varadarajan teaches that a DCV can be generated from a security challenge “provided by” the authentication server (payment authority). . *Varadarajan*, [0055]. In the Lin-Smith-Varadarajan-Hammad combination, when a DCV/dCVV is generated from the security challenge (payment authority-supplied information), among other information, the security challenge does not pass in the transaction because it is received prior to any transaction being initiated (and outside the context of a transaction because it is a different interface) and would be hashed into the DCV during the DCV generation process. In other words, only the DCV passes during a specific transaction, not the security challenge or response to the security challenge itself. *Dec.*, ¶199.

Additionally, in the combination, a POSITA would have found it obvious to use the actual account number or CVV in generating a DCV/dCVV. *Dec.*, ¶200. Hammad teaches using static data elements that “do not change from transaction to transaction,” such as the account number, to generate a dCVV. *Hammad (EX1007)*, 4:54-58. It would have been obvious to a POSITA use the actual account number or CVV (both static data elements that do not change between transactions) in generating the dCVV for the same reasons detailed in Claim 5(a). *Id.* This would have further secured the transaction by allowing the validating authorities, which have knowledge of the actual account number and CVV, to determine whether a valid account number and/or CVV are used in the transaction. In the combination,

the actual account number or CVV would not pass in the transaction, only the PPAN and DCV/dCVV passes with other payment data. *Id.*

The complete device payment information (e.g., DCV/dCVV and other payment data) is only valid for payment if the numbers used to generate the DCV/dCVV comprise the same data as generated by the processing payment authority. *See* Claims 5(a), (c), (f); *Dec.*, ¶201.

5. ***8(e): wherein said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information.***

The generating of a DCV/dCVV in the Lin-Smith-Varadarajan-Hammad combination is limited in scope of use to the user-selected payment information for a single transaction by that device. *See* Claims 1(d)-(e); *Dec.*, ¶202. For example, because the ATC is used, it is limited to one transaction. *See* Claim 5(a)-(b); *Dec.*, ¶202. Similarly, because the selected account number is used, it is for the selected user payment method. *See* Claim 1(d); *Dec.*, ¶202.

As discussed in Claims 5(a) and 8(a)-(c), the combining includes an ATC (transaction-specific sequence count), device identifier or wallet account number (device-specific information), user name, address or birthday (user-specific information), and security challenge (authority-specific information). *Dec.*, ¶203. A

POSITA would have found it obvious, and been motivated, to use additional dynamic or static data elements to generate a DCV/dCVV for same reasons discussed in Claim 5(a). *Id.*

H. Claim 9

1. ***9: The method of claim 8, wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number, capable of passing in at least a portion of the device transaction payment information.***

Varadarajan teaches that the DCV, when used to replace the CVV, is a three-digit number. *Varadarajan*, [0021]. The DCV is generated using an ARQC generating algorithm in compliance with EMV standard protocol. *Id.*, [0051]. A POSITA would understand that these algorithms generate cryptograms and that a DCV/dCVV are a cryptogram. *Dec.*, ¶204. The DCV/dCVV passes along with any other payment data to the authenticating server. *Varadarajan*, [0011], [0027], [0045], [0056]; *Dec.*, ¶24.

I. Claim 10

1. ***10: The method of claim 9, wherein the generating the limited-use payment information further utilizes a secure combination with a device key, and a payment issuer secret.***

Varadarajan teaches using a DCV key (device key) and a data element such as a server challenge (payment issuer secret) to generate a DCV. *Varadarajan*, [0055]. A POSITA would have found it obvious to combine this information, in addition to that described in Claims 5(a) and 8(a)-(c), (e), in generating the DCV/dCVV

(limited-use payment information) to further increase the security of the transaction.

Dec., ¶205; see also Claims 5(a) and 8(a)-(c), (e).

J. Claim 11

1. *11(a): The method of claim 1, wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of:*
2. *11(b) a device payment transaction sequence counter count, and*

See Claim 5(a).

3. *11(c): at least one of a set comprising:
a device-specific internal information associated with said device and also known to a payment processing authority; and,
at least one payment processing authority-specific information provided by a payment processing authority; and,
a payment issuer specific information provided by a payment issuer.*

See Claims 5(a), (d), 8(e), 10 (describing combining service code, expiration date, service code, PIN verification data, server challenge (payment processing authority recognizable information), DCV key, and wallet account number (payment issuer specific information) in generating a DCV/dCVV).

K. Claim 12

1. *12: The method of claim 1, wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information.*

As described in Claim 5, Hammad teaches generating a dCVV using various dynamic data elements, including a “terminal ID” and “a randomly generated number from a terminal” (*NFC facility provided information*). *Hammad*, 4:37-40. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction and tie the DCV/dCVV to the NFC reader. *Dec.*, ¶208; *see also* Claim 5(a).

L. Claim 13

- 1. 13: The method of claim 1, wherein the generating the limited-use payment information utilizes a merchant identifying information.**

Hammad teaches generating a dCVV using various dynamic data, including a “merchant ID” (*merchant identifying information*). *Hammad*, 4:37-40. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction. *Dec.*, ¶209; *see also* Claim 5(a).

M. Claim 14

- 1. 14: The method of claim 1, wherein the generating the limited-use payment information utilizes a transaction facility information.**

As discussed in Claim 13, Hammad teaches and a POSITA would have found it obvious to include a merchant ID (*transaction facility information*) as a data

element in generating the limited-use information to further increase the security of the transaction. *Dec.*, ¶210; *see also* Claim 5(a).

N. Claim 15

- 1. 15: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment amount.**

Varadarajan teaches generating the DCV from “total purchase or payment amount[.]” *Varadarajan*, [0055]. Hammad teaches generating a dCVV using various dynamic data, including a “current transaction amount.” *Hammad*, 4:37-41. A POSITA would have found it obvious to include payment amount as additional data elements in generating the limited-use information to further increase the security of the transaction. *Dec.*, ¶211; *see also* Claim 5(a).

O. Claim 16

- 1. 16: The method of claim 1, wherein the generating the limited-use payment information utilizes a payment facility type.**

Varadarajan teaches that the first six-digits of a PAN are an issuer identification number (payment facility type). *Varadarajan*, [0021]. Thus, when a DCV is generated from the entire PAN, it would use transaction facility information. *Dec.*, ¶212. Hammad also teaches generating a dCVV using various dynamic data, including a “terminal ID” (payment facility type). *Hammad*, 4:37-40. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction. *Dec.*, ¶212; *see also* Claim 5(a).

P. Claim 17

- 1. 17: The method of claim 1, wherein the generating the limited-use payment information utilizes an online transaction information.**

Varadarajan teaches that the data element used to generate the DCV can be a “payment amount[.]” [0055]. Varadarajan further teaches that its system can generate DCVs in card-not-present transactions, including “online transactions.” [0010], [0021]-[0022], [0029], [0042], [0045], Fig. 1.

A POSITA would understand the payment amount for an online transaction is online transaction information. Dec., ¶214. A POSITA would have found it obvious to include such additional data elements in generating the limited-use information to further increase the security of the transaction. Dec., ¶214; see also Claim 5(a).

Q. Claim 18

- 1. 18(a): The method of claim 1, further comprising:

dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number; and**

As discussed in Claim 5(a) and 10, Lin-Smith-Varadarajan-Hammad render obvious generating a DCV/dCVV by cryptographically combining an ATC (transaction sequence counter count), a wallet account number (device account

number) and a server-provided challenge or master derivation key (payment processing authority secrets). A POSITA would understand that a DCV/dCVV is a cryptogram number. *See* Claim 9; *Dec.*, ¶215. The DCV is used in place of a CVV (card validation value) that originated from the issuer. *Dec.*, ¶215.

2. ***18(b): wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number, via the incrementing of said transaction sequence counter count on a per-transaction basis, and using said updated transaction sequence counter count in said generation of said cryptogram; and,***

As discussed in Claim 5(b) and 8(e), the DCV is a one-time CVV (one-time limited-use card validation value number). *Varadarajan*, [0020], [0023], [0045], [0047]; *Dec.*, ¶216. Hammad further teaches that an ATC is incremented on a per-transaction basis and the updated count is used in generating the dCVV. *Hammad*, 4:22-31. The current value of the ATC, incremented from the previous transaction, is used in generating the dCVV. *Id.*, 6:61-8:34.

3. ***18(c): wherein said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device.***

The DCV/dCVV is used in place of the CVV (issuer supplied card validation value number) in performing the transaction payment by the device. *See* Claims 1(f), 18(a).

**VI. GROUND 2: CLAIM 6 IS OBVIOUS OVER LIN, SMITH,
VARADARAJAN, HAMMAD AND KRANZLEY**

A. Claim 6

- 1. 6(a): The method of claim 3, wherein the generating the limited-use payment information further utilizes a secure combination of said information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information; and,**

As discussed in Claim 5(a) and 8(d), the generating of a DCV/dCVV (limited-use payment information) in Lin-Smith-Varadarajan-Hammad utilizes a secure combination of said information with Smith's PPAN (device account number), Hammad's ATC (a device sequence counter count), Varadarajan's DCV generator (device-specific information), and DCV key or security challenge (payment processing authority specific information). *Dec.*, ¶219.

- 2. 6(b): a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority; and,**

As discussed in Claim 5(c), the payment processing authority performs the same combination of the same information to verify the DCV. *Dec.*, ¶220.

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 financial institution server. *Smith*, [0047], [0050], [0079]-[0080], Figs. 1-3.

Varadarajan teaches that the authenticating server 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. *See* Claim 5(c). A POSITA would have understood that the user account information used to generate the DCV key that is used to generate the DCV generator would have been stored at the authenticating server. *Dec.*, ¶222; *see also Varadarajan*, [0043] (“The authenticating server 150 uses information specific to the user’s DCV generator 100 provided by the provisioning server 155 to independently generate DCVs for that user’s credit/debit card account, for the purpose of verifying the inputted DCVs as authenticated DCV inputs for that user’s credit/debit card.”). Thus, a POSITA would have understood, or found it obvious, to store at the authenticating server the information required to independently generate a DCV. *Dec.*, ¶222.

3. ***6(c): a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid; and,***

As discussed in Claims 5(c) and (f), Varadarajan’s authenticating server and Hammad’s payment processing authority validates a payment by determining whether the device generated DCV/dCVV matches the authenticating server DCV/dCVV.

4. ***6(d): a conveying of said validation result as a declining or accepting of said transaction payment; and,***

As discussed in Claim 2, Lin teaches transmitting a confirmation message in the form of a receipt if the transaction is processed successfully (*accepting of said*

transaction payment). Specifically, the credit card verification server “determines that the specified credit card account is valid and is authorized to make the requested payment[.]” *Lin*, 34:1-10, 62:9-18, Figs. 4, 12A. *Lin* also teaches that if the payment transaction is not authorized (declining ... of said transaction payment), the payor may be notified to select a different payment option that has sufficient funds. *Lin*, 54:6-11, 80:30-81:5, Figs. 12A-B, 14J; *see also* Claims 2, 4. As discussed in Claim 1(k), it would have been obvious and a POSITA would have been motivated to configure *Lin*’s device to convey these results to the user device. *Dec.*, ¶224.

5. 6(e): upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction.

As discussed in Claim 1(i), *Hammad* teaches a system including a service provider, such as a payment processing system or issuer, that validates a dCVV. In the case of only a payment processing system validating a dCVV, a POSITA would understand that the payment data, including the original account number, would still be sent to the issuer to determine whether the account has sufficient funds (settlement of said transaction). *Dec.*, ¶225.

To the extent Patent Owner contends *Hammad* does not teach or render obvious that original payment information is sent to an issuer upon validation of a dCVV and other payment information by a payment processing authority, it would have been obvious to do so in view of *Kranzley*. *Dec.*, ¶226-230.

a) Kranzley's Teachings

Like Lin, Smith, Varadarajan, and Hammad, Kranzley teaches a mobile device having a payment application thereon for conducting payment transactions. *Kranzley*, [0019]. Similar to Varadarajan and Hammad, the mobile device generates a dynamic code or other dynamic variable that is sent, along with other payment information, to a payment processing system for validation. *Id.*, [0023]-[0027], [0030], [0035], Figs. 3, 6. In certain instances, the mobile device sends a static VPAN, i.e., account number different than the actual account number (similar to Smith's wallet account number), and an expiration date for the static VPAN and dynamic code (used in place of a CVV) to a payment provider to confirm validity of the dynamic code and determine an actual account number associated with the static VPAN. *Id.*, [0035]-[0037], [0041]-[0042], [0044]-[0045], Figs. 1B, 3, 5-6. Once confirmed, the payment provider sends the actual PAN to the issuer for authorization, including determining whether the account has sufficient funds (settlement of said transaction). *Id.*, [0037], [0048].

b) Motivation to Combine

Based on the teachings of Kranzley, it would have been obvious, and a POSITA would have been motivated to include Kranzley's payment processing authority to validate dynamic payment data and subsequently sending original account information to an issuer for authorization. *Dec.*, ¶227. Per Kranzley, having

the payment provider, and not the issuer, check the dynamic code allows for new validation processes (including generating and tracking VPANs) to be implemented or deployed without having to update issuer systems. *Kranzley*, [0049]; *Id.*

Lin, Varadarajan, and Hammad already teach using multiple financial servers (e.g., transaction server, authenticating servers, payment processing and issuer systems) in authorizing a payment. A POSITA would have been motivated to configure the Lin-Smith-Varadarajan-Hammad to use these servers, such as payment processor and issuer, in the way and for the same reasons expressly taught by *Kranzley*. *Dec.*, ¶228. Specifically, it would allow for Smith's wallet account numbers to be generated and tracked by the payment processing authority. *Id.* This would free up resources at the issuer and also not require updates to the issuer when changes were made to the generation of and distribution of PPANs, in the combination, as taught by *Kranzley*. *Id.*

A POSITA would recognize that modifying Lin-Smith-Varadarajan-Hammad in this way would only require basic software modifications and routine skill as the system already includes a payment processing and issuer authority to validate the DCV/dCVV (limited-use payment information). *Dec.*, ¶229. Thus, the payment processing system would simply send the actual account number, among other information, to the issuer for authorization, while retaining the additional benefits taught by *Kranzley*. *Id.*

Because the components and functionalities are largely the same, there would have been a reasonable expectation of success configuring Lin's financial servers to include a payment processing system and issuer system in this way. *Dec.*, ¶230; *see also* Claim 1(j). This would have been a combination of known elements that would yield the predictable result of a secure payment in the existing payment processing architecture. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007); *Dec.*, ¶230.

VII. DISCRETIONARY CONSIDERATIONS

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

I. 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

II. 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.

B. 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.

C. 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	WIPO Pub. No. 2010/039337 to Lin et al. (“Lin”)
Exhibit 1005	U.S. Pub. No. 2010/00125508 (“Smith”)
Exhibit 1006	U.S. Pub. No. 2011/0184867 to Varadarajan (“Varadarajan”)
Exhibit 1007	U.S. Patent No. 7,740,168 to Hammad et al. (“Hammad”)
Exhibit 1008	U.S. Pub. No. 2010/0125509 to Kranzley et al. (“Kranzley”)
Exhibit 1009	U.S. Provisional Application No. 60/884,089 (“Hammad ’089 Provisional”)
Exhibit 1010	Intentionally Left Blank
Exhibit 1011	Intentionally Left Blank
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) (“ <i>Smart</i> ”)
Exhibit 1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. (“ <i>Pitroda</i> ”)
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] (“ <i>MasterCard Mobile Partner</i> ”)
Exhibit 1029	U.S. Patent Publication No. 2013/0054474 to Yeager (“ <i>Yeager</i> ”)
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 (“ <i>EMVCo</i> ”)
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) (“ <i>PCI SSC</i> ”)
Exhibit 1032	<i>Alessandro Vizzarri et al., Security in Mobile Payments</i> (2013) (“ <i>Vizzarri</i> ”)
Exhibit 1033	U.S. Patent Publication No. 2008/00110983 to Ashfield (“ <i>Ashfield</i> ”)
Exhibit 1034	Intentionally Left Blank
Exhibit 1035	“Smart Card Technology: New Methods for Access Control” (“ <i>Smart Card Tech.</i> ”)
Exhibit 1036	U.S. Patent No. 5,528,222 (“ <i>Moskowitz</i> ”)
Exhibit 1037	“The Electronic Purse” (“ <i>Wenninger</i> ”)
Exhibit 1038	U.S. Patent 5,594,233 (“ <i>Kenneth</i> ”)
Exhibit 1039	U.S. Patent No. 7,004,385 (“ <i>Douglass</i> ”)
Exhibit 1040	U.S. Pub. No. 2007/0265984 (“ <i>Sanantha</i> ”)
Exhibit 1041	U.S. Pub. No. 2012/0197691 (“ <i>Grigg</i> ”)
Exhibit 1042	U.S. Patent Publication No. 2010/0125509 (“ <i>Kranzley</i> ”)
Exhibit 1043	U.S. Pub. No. 2011/0140841 (“ <i>Bona</i> ”)
Exhibit 1044	U.S. Pub. No. 2014/0019367 (“ <i>Khan</i> ”)
Exhibit 1045	U.S. Pub. No. 2013/0262317 (“ <i>Collinge</i> ”)

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”)

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 12,500 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

IPR2025-01149

U.S. Patent No. 11,176,538

(913) 777-5600 Telephone

(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER