

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARDWARE INC.,
Patent Owner

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

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE '538 PATENT CLAIMS.....	4
III. PETITIONER'S ALLEGED PRIOR ART	6
A. <i>Kalgi</i>	7
B. <i>Khan</i>	12
C. <i>Varadarajan</i>	12
D. <i>Smith</i>	16
E. Petitioner's Proposed Combinations	20
IV. CLAIM CONSTRUCTION	22
A. Petitioner Omits its Contradictory District-Court Indefiniteness Arguments that Certain Claim-Scope Allegedly Cannot be Ascertained	22
V. LEVEL OF ORDINARY SKILL IN THE ART	23
VI. ARGUMENT	24
A. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination For Ground 1 Includes "Generating At Least One Limited-Use Numbers At Said Electronic Device, And Using Said Limited-Use Number In Place of At Least A Portion of Selected Account Issuer Payment Information" of Limitation 19(e).	24
1. Petitioner Ignores the Disparate Teachings in <i>Kalgi</i> 's Disclosure and Fails To Show a Motivation to Modify, or a Reasonable Expectation of Success in Modifying, <i>Kalgi</i> Figure 1 with <i>Kalgi</i> Figures 9A-10B.	24
2. Petitioner and Its Expert Fail to Show a Motivation to Combine <i>Kalgi</i> and <i>Varadarajan</i>	33
B. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combinations for Grounds 3 and 7 Have A "Static Device Account Number [] of a Limited Scope of Valid Use to a Specific Device" of	

Claim 21 or a “Static Device-Specific Account Number . . . Limited in Use To the Device” of Limitation 27(b).....	40
1. Petitioner Fails to Show That <i>Smith</i> ’s PPAN is “For a Specific Device” or “Limited in Use To [A] Device”	41
2. Petitioner and Its Expert Fail to Show a Motivation to Combine <i>Kalgi</i> with <i>Smith</i> and with <i>Varadarajan</i>	53
C. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combinations for Ground 4 Includes “Generat[ing] A Device-Specific Limited-Use Payment Information” of Limitations 25(f), 25(g), and 25(h).	58
1. Petitioner Fails to Explain Why Its “Dynamic Partial PPAN” Is “Device-Specific.”	59
2. Petitioner Fails to Explain Why <i>Varadarajan</i> ’s DCV is “Device-Specific”	59
3. Petitioner and Its Expert Fail to Show A Motivation to Combine <i>Kalgi</i> , <i>Varadarajan</i> , and <i>Smith</i>	67
D. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combinations for Ground 4 Includes “A Statically Generated Portions Stored In A Memory of the Device” of Limitation 25(g) and 25(h).	68
E. Additional Reasons that Petitioner has Failed to Meet Its Burden.....	70
VII. CONCLUSION.....	71

TABLE OF AUTHORITIES

Page(s)

Cases

<i>ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.</i> , 694 F.3d 1321 (Fed. Cir. 2012)	33, 37, 54, 56
<i>Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.</i> , 776 F.2d 281 (Fed. Cir. 1985)	33
<i>AT&T Servs. Inc. v. Innovative Sonic Ltd.</i> , IPR2024-01143, Paper 15 (PTAB Feb. 11, 2025).....	32, 37, 54
<i>Microchip Tech. Inc. v. Aptiv Techs. AG</i> , IPR2024-00558, Paper 12 (PTAB Oct. 7, 2024).....	23
<i>NearMap US, Inc. v. Pictometry Int'l Corp.</i> , IPR2024-00729, Paper 9 (PTAB Oct. 10, 2024).....	38, 55, 56
<i>Precision Cancer Techs. Inc. v. Oncoustics Inc.</i> , IPR2025-00242, Paper 7 (PTAB June 3, 2025)	32, 37, 54, 60
<i>Upjohn Co. v. Mova Pharm. Corp.</i> , 225 F.3d 1306 (Fed. Cir. 2000)	33, 37, 54, 56
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022).....	32, 37, 54, 60

Regulations

37 C.F.R. § 11.18	23
37 C.F.R. § 42.6(a)(3)	38
37 C.F.R. § 42.11	23
37 C.F.R. § 42.12(b)	23

PATENT OWNER’S EXHIBIT LIST

No.	Exhibit Description
2001	Memorandum for Interim Processes for PTAB Workload Management, dated March 26, 2025
2002	Interim Director Discretionary Process <i>available at</i> https://www.uspto.gov/patents/ptab/interim-director-discretionary-process
2003	Agreed Scheduling Order in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. May 20, 2025)
2004	Standing Order Governing Proceedings (OGP)—Patent Cases for cases before Judge Albright (dated Mar. 5, 2025)
2005	Docket Navigator Time to Trial Statistics for Patent Cases before Judge Albright
2006	Judges’ Directory and Biographies for the U.S. District Court for the Western District of Texas, <i>available at</i> https://www.txwd.uscourts.gov/judges-information/judges-directory-biographies/
2007	Complaint in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Nov. 4, 2024)
2008	First Agreed Scheduling Order in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2009	Complaint in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2010	Invalidity Contentions Cover Pleading in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Apr. 7, 2025)
2011	Defendants’ Notice of Subpoena to Apple, Inc. in <i>CardWare Inc. v. Samsung Elecs. Co., Ltd.</i> , No. 2:22-cv-00141-JRG-RSP (E.D. Tex. Dec. 9, 2022)
2012	Apple Inc.’s Response and Objections to Defendants’ Subpoena in <i>CardWare Inc. v. Samsung Elecs. Co., Ltd.</i> , No. 2:22-cv-00141-JRG-RSP (E.D. Tex. Dec. 23, 2022)
2013	Letter from CardWare, Inc. to Apple Inc. dated October 10, 2023 “RE: Patent Portfolio of CardWare Inc.”
2014	Proof of Delivery to Apple Inc. dated October 11, 2023, for Letter from CardWare, Inc. to Apple Inc. dated October 10, 2023 “RE: Patent Portfolio of CardWare Inc.”
2015	Docket Navigator Time to Trial Statistics for Patent Cases in the Western District of Texas

No.	Exhibit Description
2016	Apple’s Opening Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. May 27, 2025)
2017	CardWare’s Responsive Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. June 17, 2025)
2018	Apple’s Reply Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. July 1, 2025)
2019	CardWare’s Sur-Reply Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. July 17, 2025)
2020	Joint Claim Construction Statement in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. July 18, 2025)
2021	Comparison Chart for References Relied Upon in Apple’s Invalidity Contentions in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex.)
2022	Excerpts from Defendant Google LLC’s Invalidity Contentions in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Apr. 3, 2025)
2023	Excerpts from Exhibits to Apple’s Invalidity Contentions in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Apr. 7, 2025)
2024	Claim Construction Order in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Aug. 29, 2025)

I. INTRODUCTION

On June 24, 2025, Apple Inc. (“Apple” or “Petitioner”) filed a Petition requesting *inter partes review* of claims 19-30 (“Challenged Claims”) of U.S. Patent No. 11,176,538 (“the ’538 Patent”) (EX1001), entirely on obviousness grounds. Paper 1 (“Petition” or “Pet.”). On July 15, 2025, the Board issued a Notice of Filing Date Accorded for the Petition and set the time for filing Patent Owner’s preliminary response. Paper 6.

The Board should deny institution because Petitioner fails to meet its burden of demonstrating that its prior art references render obvious any of the Challenged Claims, which generally relate to methods and systems for reducing the risk of fraud in connection with completing payment transactions. Petitioner’s arguments suffer from three main flaws—which together are dispositive of all Challenged Claims.

First, in **Ground 1** (in reference to independent claim 19), Petitioner fails to show a motivation to modify, or a reasonable expectation of success in modifying, two separate embodiments of *Kalgi* and then further modifying them with the DCV of *Varadarajan*, to disclose “generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information” of limitation 19(e). Specifically, Petitioner relies on the E-Wallet Checkout (“E-Wallet”) Embodiment of *Kalgi* (see Figures 1-6) which does *not* send a user’s payment information to a merchant to

complete a transaction for the elements “receiving an...input signal corresponding to a request for payment of an online payment transaction by said electronic device” of limitation 19(a) and “receiving, from a valid device user, a payment selection and authorization approval input on the electronic device” of limitation 19(d). But, Petitioner relies on a separate Purchase Transaction Authorization (“PTA”) Embodiment of *Kalgi* (see Figures 9A-10B), which *does*, for limitation 19(e). Yet, Petitioner does not explain why, or how, a POSITA would modify the E-Wallet Embodiment with the less secure PTA Embodiment, or how a POSITA would further modify their combination with *Varadarajan*’s DCV.

Second, in **Grounds 3 and 7** (which challenges dependent claims 21 and 27), Petitioner fails to show that its proposed obviousness combination includes a “static device account number [] of a limited scope of valid use to a specific device” of claim 21 and a “static device-specific account number ... limited in use to the device” of limitation 27(b). Petitioner relies on *Smith*’s “PPAN” as disclosing this limitation, but *Smith* merely teaches that the PPAN is mapped to a user’s account. This says nothing about whether it is “device-specific.” For example, *Smith* does not say that its PPAN is limited to a particular device (*e.g.*, it could be used with multiple devices at the same time), and *Smith* does not say what happens if a user gets a new device (*e.g.*, the PPAN could be re-used on the new device). Indeed, *Smith* specifically states that “multiple NFC-enabled handsets may be managed for a single

account.” EX1008, [0029]. Petitioner makes no further obviousness argument based on *Smith* and these limitations. *See* Pet., 36-41, 72.

Third, in **Ground 4** (which challenges independent claim 25), Petitioner also fails to show that its proposed obviousness combination includes to “generate a device-specific limited-use payment information” of limitations 25(f), 25(g), and 25(h). Petitioner relies on “a dynamic partial PPAN”—which is a combination of *Smith*’s purportedly device-specific PPAN partially replaced by *Varadarajan*’s “DCV” (purportedly the dynamically generated portion) as disclosing this limitation, but, as discussed above in reference to Grounds 3 and 7, *Smith*’s PPAN is not device specific. *See* Pet., 50. “Additionally, or alternatively,” Petitioner relies on *Varadarajan*’s “DCV” as disclosing this limitation, asserting that “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.” *See* Pet., 50. However, *Varadarajan* does not teach that the “device derived identification parameter” is used to generate the DCV, instead, it is used as a layer of security to limit access to the DCV generating application (like an authenticator app) that hosts the DCV generator.

The same problems exist with the remaining **Grounds 2, 5, and 6** (challenging dependent claims 20, 22, 23, 26, 28-30), at least because Petitioner relies on some of the same combinations of references and disclosure as the above

Grounds, plus additional references (*Khan, Hammad, Bauer, and Kranzley*) addressing additional limitations in such dependent claims.

For these reasons, and those explained below, the Board should therefore decline to institute.

II. THE '538 PATENT CLAIMS

When David Wyatt conceived of the invention claimed in the '538 Patent over a decade ago, there were “several different types of credit cards available in the marketplace.” EX1001, 1:32-33.

As the patent explains:

A first type of credit card is a conventional, standard piece of plastic with a magnetic strip, which is readily available and in wide commercial use. The advantage of this first type of credit card is that a large portion of the infrastructure for credit card transactions is built around this type of card, and consequently such a card works in a wide array of vendors' credit card machines, automated teller machines (ATMs), and other devices that support the present credit card and banking infrastructure.

EX1001, 1:33-41.

The claims of the '538 Patent generally relate to systems and methods for reducing fraud during payment transactions. Independent claim 19—one of the challenged independent claims—is illustrative and is directed to a method of

performing an online payment transaction via a wireless interface of an electronic device. EX1001, 22:62-23:34 (claim 19). The method of claim 19 involves receiving a request for a transaction payment at an electronic device via a wireless interface. EX1001, 22:64-67. A touch-screen display user-interface of the electronic device then displays the payment request, and, upon an authorizing of a valid device user, at least one user-selectable payment account option and a request for user approval of payment. EX1001, 23:1-7. The method further “generat[es] at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information” and “combining said at least one limited-use numbers, with said selected account information, to form a complete payment information.” EX1001, 23:11-18. This complete payment information is transmitted over a wireless interface of the electronic device to complete the online payment transaction. *See* EX1001, 23:33.

Claim 25—the other challenged independent claim—claims a non-transitory, computer-readable medium storing computer executable instructions for similarly performing an online payment transaction. EX1001, 24:49-25:15. In particular, the instructions cause one or more processors to “generate a device-specific limited-use payment information for use in place of at least a portion of said selected issuer payment account information on the device” and “form a complete combined device payment information from a dynamically generated portion and a statically

generation portions stored in a memory of the device.” EX1001, 24:66-25:6.

The various cryptographic techniques of the '538 Patent drastically improve security vis-à-vis prior art while maintaining convenience and flexibility by allowing selection and use of different payment accounts.

III. PETITIONER’S ALLEGED PRIOR ART

Petitioner relies upon seven references in its Grounds (*Kalgi*, *Khan*, *Varadarajan*, *Hammad*, *Smith*, *Bauer*, and *Kranzley*). In Ground 1, Petitioner presents the combination of *Kalgi*, *Khan*, and *Varadarajan* to challenge independent claim 19 and dependent claim 24. In Ground 2, Petitioner adds a fourth reference (*Hammad*) to Ground 1’s combination to challenge dependent claims 20 and 22. In Ground 3, Petitioner adds a fourth reference (*Smith*) to Ground 1’s combination to challenge dependent claim 21. In Ground 4, Petitioner presents the combination of *Kalgi*, *Varadarajan*, and *Smith* to challenge independent claim 25. In Ground 5, Petitioner adds a fourth and fifth reference (*Hammad* and *Smith*) to Ground 1’s combination to challenge dependent claim 23, and a fourth and fifth reference (*Khan* and *Hammad*) to Ground 4’s combination to challenge dependent claims 28 to 30. In Ground 6, Petitioner adds a fourth and fifth reference (*Hammad* and *Bauer*) to Ground 4’s combination to challenge dependent claim 26. In Ground 7, Petitioner adds a fourth and fifth reference (*Hammad* and *Kranzley*) to Ground 4’s combination to challenge dependent claim 27.

Patent Owner provides an overview of the relevant references, for purposes of this Preliminary Response, in this Section III. Patent Owner then explains in the following sections how Petitioner's Grounds using such references fail to demonstrate a reasonable likelihood of success that any Challenged Claim is obvious.

A. *Kalgi*

International Publication No. WO2013/0013499 ("*Kalgi*") is directed to "electronic purchase transactions," specifically "electronic wallet checkout platform apparatuses, methods and systems ('EWCP') that "transform customer purchase requests triggering electronic wallet applications, via EWCP components, into electronic purchase confirmation and receipts." EX1004, Abstract, [0003], [0027].

Kalgi explains:

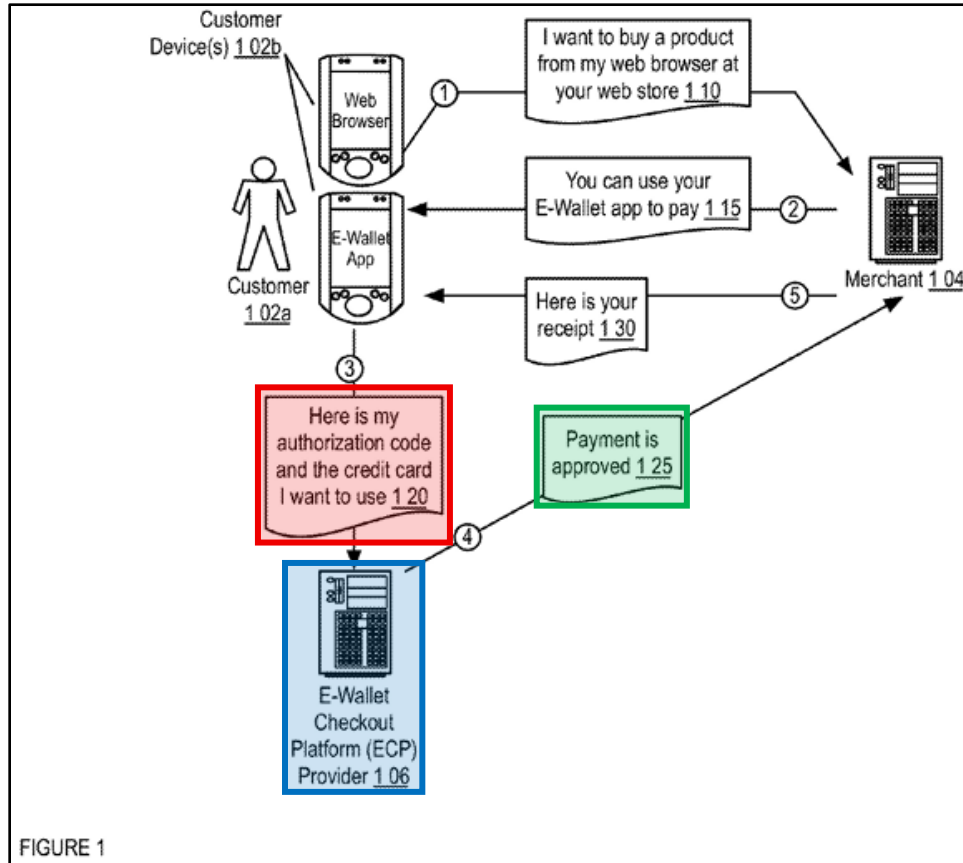
A consumer who wants to purchase a product and/or a service from a merchant may go to the merchant's website to engage in a purchase transaction. For example, this may involve using the merchant's website *to provide personal information, such as credit card billing address and credit card information, to the merchant* to facilitate the purchase transaction. *Such online shopping experience may be fraught with security risks and usability problems. The customer's data may be exposed or misused by the merchant during the checkout and/or payment flow. If the merchant stores the customer's personal information, this*

information may be also vulnerable to security breaches that may happen long after the customer engaged in a purchase transaction The EWCP externalizes the checkout and/or payment flow from the web based, merchant driven model. Using the EWCP, the customer may engage in a purchase transaction via a secure platform that may provide a consistent user experience across merchant websites.

EX1004, [0027] (emphases added).

Kalgi, in reference to Figure 1, reproduced below, describes an embodiment in which a customer 102a makes a purchase on a webpage that supports an EWCP-supported protocol, using an E-Wallet app installed on their consumer device 102b that is compatible with the EWCP. EX1004, [0028]-[0029]; *see* EX1004, [0006]-[0011]; *see* EX1004, [0029] (“The EWCP may detect that the merchant uses an EWCP-supported protocol (e.g., via a mobile EWCP application described in more detail in FIG. 2), and may prompt the customer to use an EWCP electronic wallet (hereinafter ‘E-Wallet’ or ‘wallet application’) to facilitate payment.”). “Using the E-Wallet may facilitate payment for [an] item without revealing the customer’s personal information to the merchant.” EX1004, [0029] (emphasis added). Specifically, when a customer requests to check out on a webpage using an EWCP-supported protocol, they are prompted to use an E-Wallet. The customer uses the E-Wallet to provide “authentication and/or authorization information to use the E-

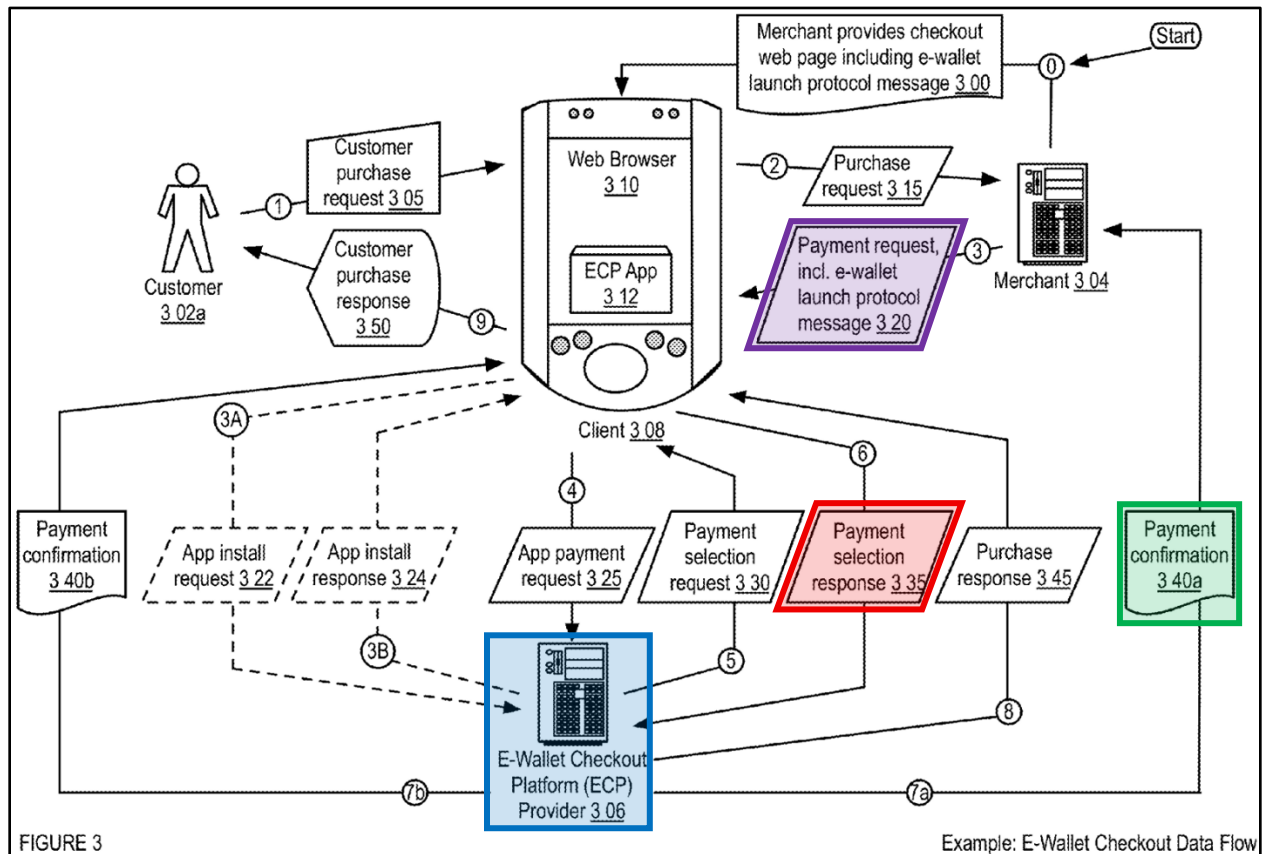
Wallet” and “a selection of a payment method (e.g., a specific credit card) 120” (**red**) to an intermediary, the EWCP provider 106 (**blue**), which verifies the information, “calculate[s] the total amount due from the customer, collect[s] the total amount due and provide[s] appropriate payment (e.g., total amount due minus fees) to the merchant[,]” and “provide[s] a confirmation to the merchant that payment information was obtained 125” (**green**). EX1004, [0029]-[0030], FIG. 1 (annotated); *see also* EX1004, [0047]-[0061]; FIGs. 4-6.



EX1004, FIG. 1.

Kalgi, in reference to Figure 3, further explains that, in response to a customer purchase request sent to the merchant via the E-Wallet, “[t]he merchant may respond

with a payment request 320 [(purple) that] may prompt the customer to provide payment information to pay for the item” that prompts the E-Wallet to launch or to prompt the customer to install the E-Wallet. *See* EX1004 [0039]-[0043], FIG. 3; *see also* EX1004, [0047]-[0061]; FIGs. 4-6. The rest of the process of Figure 3 follows Figure 1 and its accompanying description. *See* EX1004, [0043]-[0046].



EX1004, FIG. 3.

Kalgi, in reference to Figure 9A, reproduced below, depicts a separate embodiment in which a Purchase Transaction Authorization (“PTA”) component of the EWCP which “transform[s] a user virtual wallet access input ... into a purchase transaction receipt notification.” *See* EX1004, [0067]-[0092], FIGs. 9A-10B; *see*

also EX1004, [0185], FIG. 20. *Kalgi* explains in reference to Figures 9A-10B that a transaction authorization input 914 (**orange**) including customer's credit card information is not only directly transmitted to the merchant (risking interception) but also stored on a merchant's databases and used in search queries (risking disclosure as a result of merchant-side security breaches). *See* EX1004, [0027], [0068]-[0072], *see also* EX1004, [0143], FIG. 19A ("[I]n the example illustration in FIG. 19A, the user has selected the name 1911 a, *account number 1912 a, security code 1913 a,* merchant account ID 1918 a and rewards account ID 1919 a *as the fields to be sent* as part of the notification to process the purchase transaction.") (emphases added).

EX1004, FIG. 9A.

B. *Khan*

U.S. Patent App. Pub. No. 2014/0019367 (“*Khan*”) discloses “[a] commercial transaction method[,]” “for conducting a wireless commercial transaction that is both user friendly and secure.” EX1005, Abstract, [0002], [0005]. Specifically, *Khan* discloses a method in which “a portable device can make purchases by using near field communications (NFC) to establish a secure link with a point of sale (POS) device connected to a backend system that is configured to execute commercial transactions.” EX1005, [0006]. “Th[e] secure link can be established by positioning the portable device to be within close proximity of the point of sale device. Increased mobility is provided to users of the portable device making purchases by establishing a second secure link that uses a different protocol, such as WIFI or Bluetooth, that has more desirable characteristics for maintaining the link over time than NFC.” EX1005, [0006].

C. *Varadarajan*

U.S. Patent App. Pub. No. 2011/0184867 (“*Varadarajan*”) discloses “[a] method and system ... for generating a dynamic card value (DCV) from a mobile user device for use in a transaction between a user cardholder and a transaction provider.” EX1006, Abstract. “The DCV may be configured for use as a card verification value (CVV), also known as a card security code (CSC), a primary account number (PAN), or a portion of a PAN.” EX1006, Abstract; [0012]-[0013].

More than one type of DCV may be provided for the same transaction, like “both a dynamic PAN and a dynamic CVV.” EX1006, [0022].

The DCV addresses “security vulnerabilities” associated with “[c]ard based transactions,” such as: (1) use of “skimmer[s]” in in-person, “card present,” transactions, where the fixed PAN and CVV1 encoded on a payment card’s magnetic stripe is intercepted and used to create a counterfeit card; (2) “phishing” in on-line or over-the-phone, “card not present,” transactions, where a customer is tricked into providing their card’s embossed PAN and CVV2 printed on the back of the card; (3) weaknesses in a receiving merchant’s document security system; or (4) viruses or screen wipers on a user’s device that record static payment information as it is entered. *See* EX1006, [0003]-[0010].

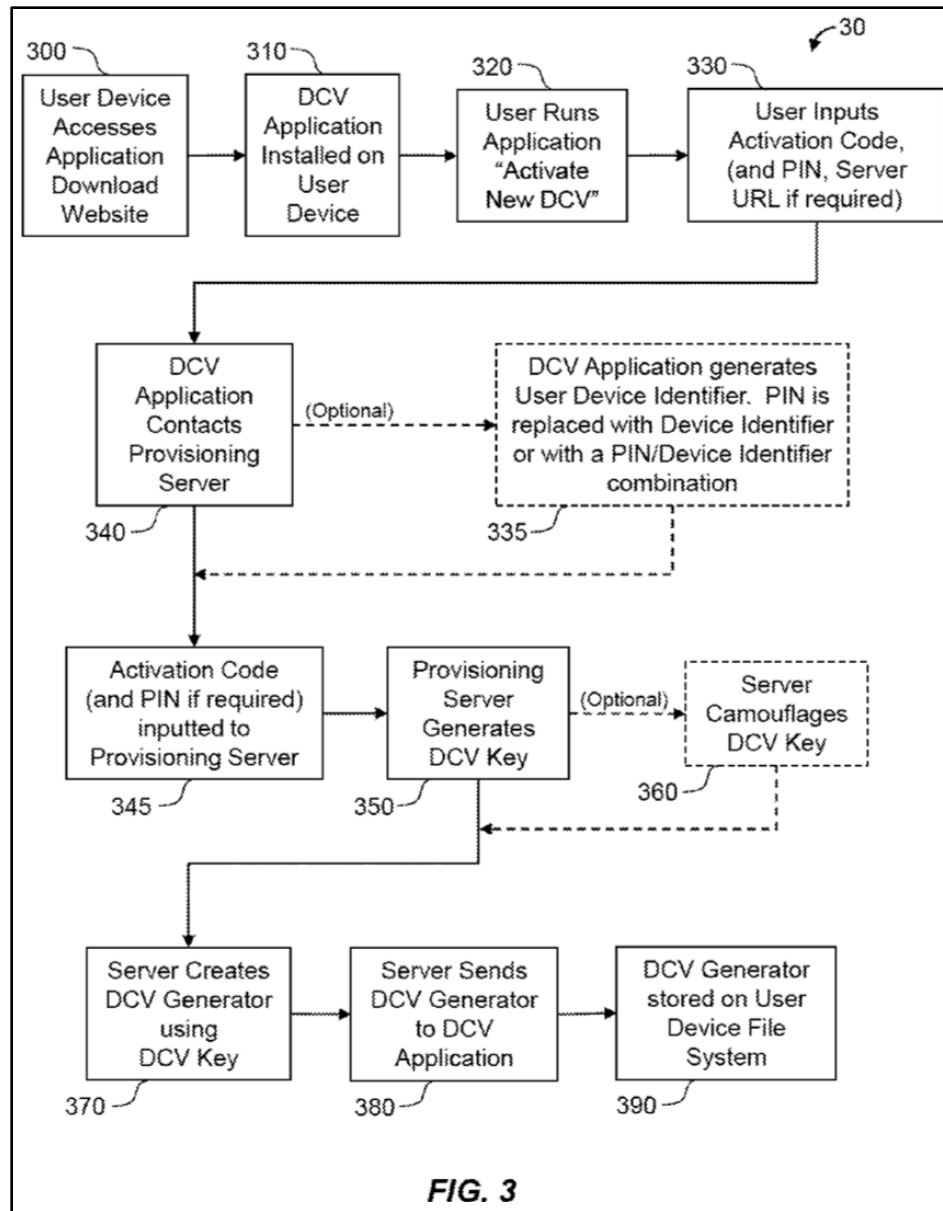
Varadarajan explains, in reference to Figure 3 below, the process of preparing a user’s mobile device to generate a DCV as follows.

1. At steps 300 and 310, the user downloads and installs a DCV application to their mobile device.
2. At step 320, the user requests a DCV on the DCV application. As a security measure, the user may be required to enter a PIN (*e.g.*, CVV2 or other static PIN). As shown at step 335, as a further security measure, the PIN may be combined with or replaced by a device-generated PIN (a.k.a. “device derived identification parameter” or “device identifier”)

that uniquely associates the DCV application to the user's device.

3. At steps 340 and 345, the DCV application contacts the provisioning server of a card issuing entity—such as a bank, financial institution, retailer, merchant, or other payment services provider—and provides the PIN, device identifier, or PIN and device identifier.
4. At steps 350 and 370, the provisioning server generates a DCV generation key (a.k.a. “DCV key”) and creates a DCV generator.
5. At steps 380 and 390, the provisioning server sends the DCV generator to the user's device hosting the DCV application, where it is stored.

See EX1006, FIG. 3, [0024]-[0026], [0029], [0048]-[0051].



EX1006, FIG. 3.

Varadarajan explains that the DCV generator may use an algorithm and a DCV generation key (or DCV key) to generate the DCV. EX1006, [0034]. The algorithm may be “a standardized DCV generating algorithm, such as HOTP, EMV/CAP, or other OATH-approved standard, or may be another or customized DCV generating algorithm.” EX1006, [0034]. The DCV key may be “generated by

applying a card verification key (CVK) to the user's account number and related account information, such as the card expiration date and service code," resulting in a DCV key that "specific to the user's account." EX1006, [0050]. The DCV generator may also use a security challenge, transaction information, or transaction amount to generate the DCV. EX1006, [0055].

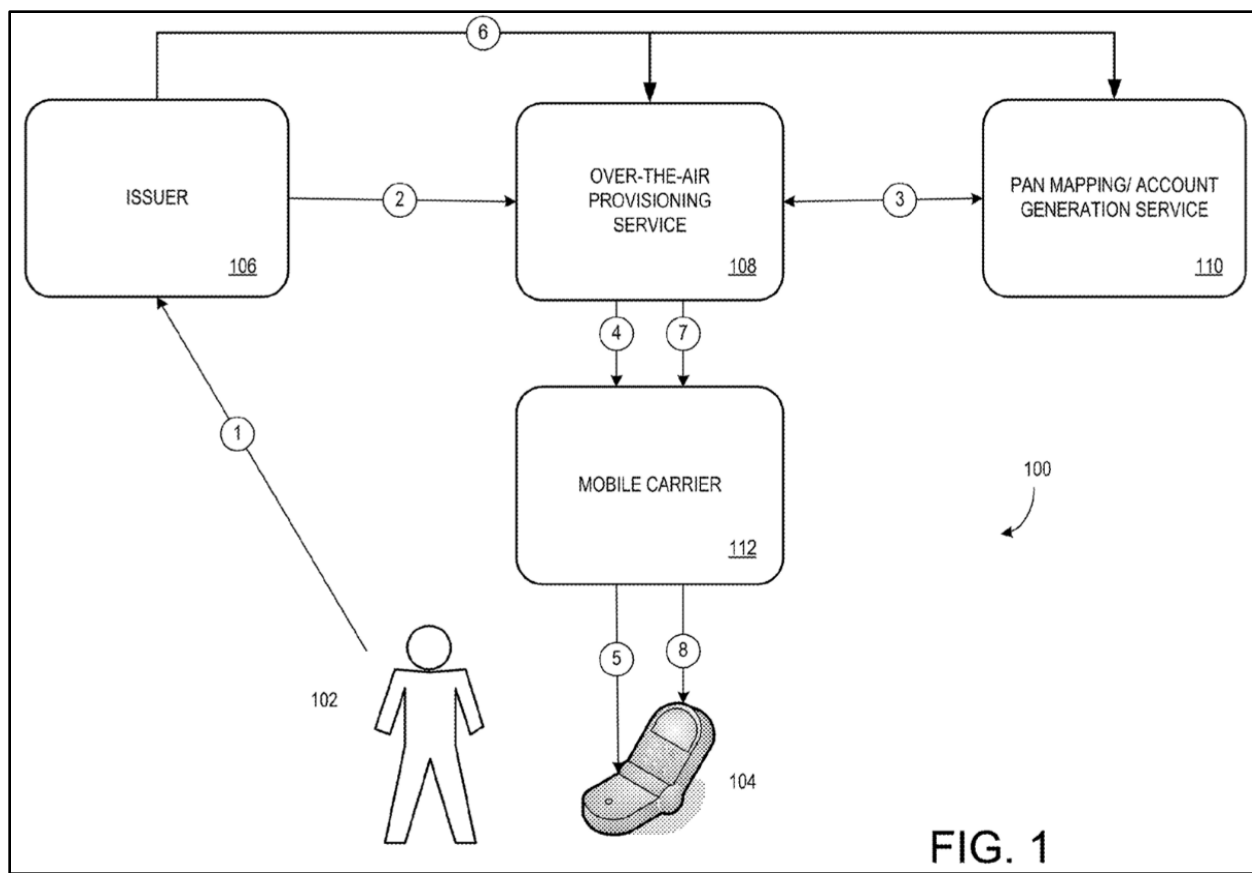
Varadarajan explains that, when a user requests a DCV using the DCV application on their mobile device, the same device identifier used to initially request a DCV generator may be used as a security measure. EX1006, [0054]. Specifically, if the DCV application is "ported" to another device and used without authorization by an attacker, "[t]he other (unauthorized) device will generate an invalid device identifier which may prompt the DCV generator to display a DCV which would be recognizable as an alert code by the authenticating server." EX1006, [0054]. "Upon recognizing the alert DCV, the authenticating server may decline the transaction, notify the user and/or card-issuing entity and/or store the DCV for detection of a second intrusion attempt by the non-user device attempting to execute the DCV generating application." EX1006, [0054].

D. *Smith*

U.S. Patent App. Pub. No. 2010/0125508 ("*Smith*") is directed to methods for automatically assigning a "temporary payment account number ('PAN')" to a consumer's request for a new payment account, which "allow[s] the account holder

to access the account during a time period in which the issuer systems are updated to include the actual payment account number (or ‘actual PAN’).” EX1008, [0012]; EX1008, Abstract.

As *Smith* explains, when a consumer uses a payment application on their mobile device to activate a payment account, “there may be a delay between [the] request ... and the time at which an issuer can establish an actual account in response to that request,” which delay “may be frustrating to a consumer who want to use his or her mobile device to complete a purchase transaction.” EX1008, [0002]. It is therefore “desirable to allow consumers to activate such a payment application on a consumer’s mobile phone and then instantly, that is to say within a relatively brief period of time, use the mobile phone in a payment transaction.” EX1008, [0003].



EX1008, FIG. 1.

Smith explains, in reference to Figure 1 above, the following transactions involved in its method for issuing a payment account over a mobile network:

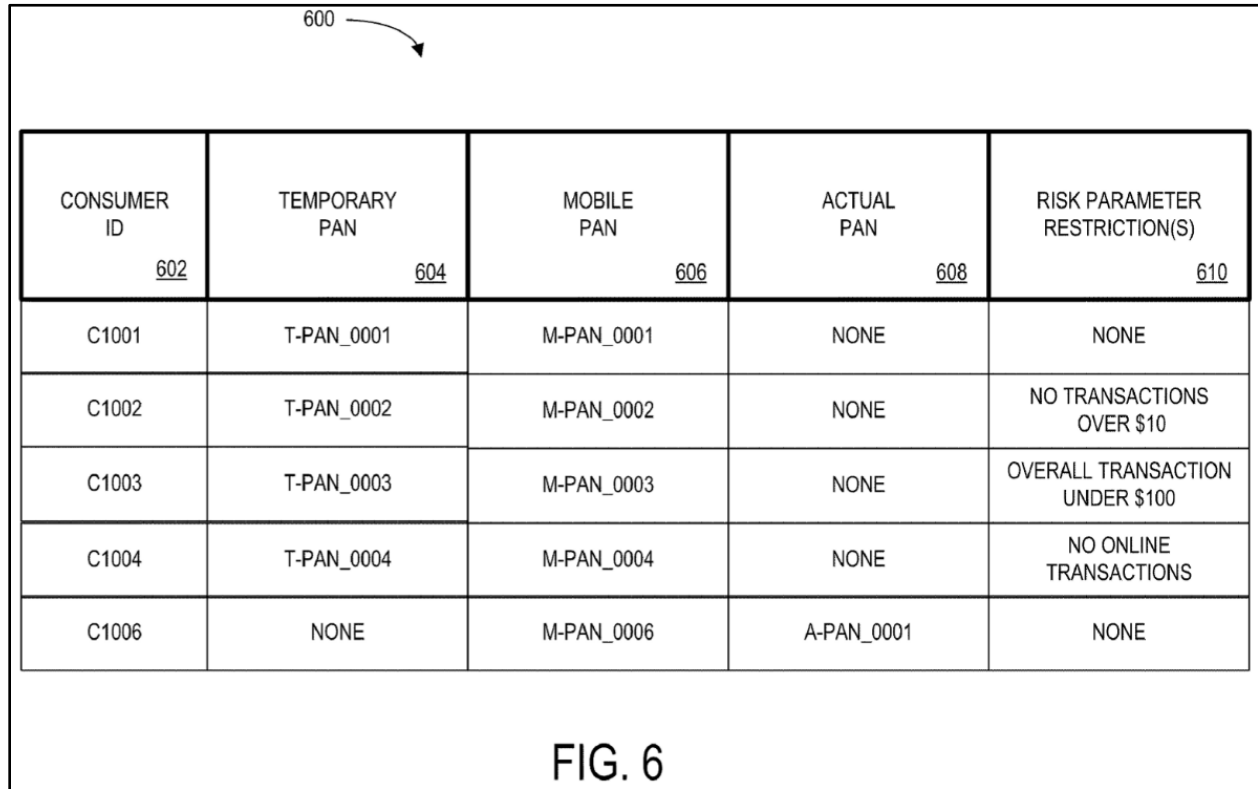
1. Transaction 1: A customer 102 enters account registration data and requests an issuer 106 issue a payment account using their mobile device 104.
2. Transaction 2: The issuer 106 assigns a temporary PAN to the customer's account registration data and transmits the temporary PAN to an over-the-air ("OTA") provisioning service 108 with a request to

install a payment application and account information on the customer's mobile device 104.

3. Transaction 3: The OTA provisioning service 108 forwards the temporary PAN to a PAN mapping service 110, which assigns a PayPass PAN ("PPAN") to the payment application destined for the mobile device 104 and maps the PPAN to the temporary PAN. The PAN mapping service sends the PPAN back to the OTA provisioning service 108.
4. Transaction 4: The OTA provisioning service 108 delivers a software package with a payment application and the PPAN to the mobile carrier 112 network associated with the mobile device 104.
5. Transaction 5: The mobile carrier 112 pushes the software package to the mobile device 104, during which process the customer 102 enters a verification code to confirm their identity and authorize installation of the software package.
6. Transactions 6-8. Once the issuer 106 issues an actual PAN for the account of the customer 102, it sends a request message to the PAN mapping service 110 to replace the temporary PAN with the actual PAN in its mapping database.

EX1008, [0013]-[0019]; *see also* EX1008, FIGs. 3 & 4, [0025]-[0032].

Smith further explains that the primary account number database 600 of Figure 6 below has “entries associated with consumers how [*sic*: who] have requested to use a mobile device to complete purchase transactions.” EX1008, [0039].



The diagram shows a large rectangular box labeled '600' at the top left with an arrow pointing to a table. The table has five columns and six rows. The columns are labeled: CONSUMER ID (602), TEMPORARY PAN (604), MOBILE PAN (606), ACTUAL PAN (608), and RISK PARAMETER RESTRICTION(S) (610). The rows contain data for consumers C1001, C1002, C1003, C1004, and C1006. The last row for C1006 has a blank cell in the TEMPORARY PAN column and 'A-PAN_0001' in the ACTUAL PAN column.

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

EX1008, FIG. 6.

E. Petitioner’s Proposed Combinations

Petitioner’s proposed obviousness combination for Grounds 1, 2, 3, and 5 is based on a combination of *Kalgi*, *Khan*, and *Varadarajan* (additionally with *Hammad* in Ground 2, *Smith* in Ground 3, and *Hammad* and *Smith* in Ground 5).

Relevant to this Preliminary Response and as further discussed below, as best that Patent Owner can discern, for Grounds 1, 2, 3, and 5 Petitioner proposes that *Kalgi* is the primary reference, including its electronic wallet checkout platform

apparatuses, methods, and systems. Petitioner then appears to propose that it would have been obvious to “incorporate a wireless interface, such as Khan’s WIFI interface, so that the mobile device receives a payment request wirelessly.” Pet., 16-17. Petitioner further appears to propose that it would have been obvious to further add the DCV disclosure of *Varadarajan*, specifically to “configure Kalgi’s device processor to dynamically generate a DCV or PAN to be used in place of at least a portion of the selected issuer payment account information responsive to receiving a valid user transaction payment approval.” Pet., 24-26. From there, for Ground 3, Petitioner further appears to propose that a POSITA would add to the *Kalgi-Khan-Varadarajan* combination the PPAN disclosure of *Smith*: “A POSITA would have found it obvious and been motivated to use Smith’s PPAN in place of Kalgi’s account number” and “[a] POSITA would have further found it obvious and been motivated to use the PPAN to generate a dynamic partial PPAN, as taught by Varadarajan” to “generate a dynamic CVV and dynamic partial PPAN (DCV + portion of the PPAN), which is of limited scope of valid use to the user’s specific device.” Pet., 39-41.

Petitioner’s proposed obviousness combinations for remaining Grounds 4, 6, and 7 are based on a combination of *Kalgi*, *Varadarajan*, and *Smith* (additionally with *Hammad* and *Bauer* in Ground 6, and *Hammad* and *Kranzley* in Ground 7).

Relevant to this POPR and as further discussed below, as best that Patent Owner can discern for Grounds 4, 6, and 7, Petitioner proposes that *Kalgi* is the primary reference, including its electronic wallet checkout platform apparatuses, methods, and systems. In Ground 4, Petitioner appears to propose to replace the payment information of *Kalgi* with the “dynamic partial PPAN” introduced in Ground 3 wherein “a DCV [(of Varadarajan) is] generated and used as part of a PPAN” of *Smith* or, alternatively with just *Varadarajan*’s DCV. Pet., 50-52.

IV. CLAIM CONSTRUCTION

A. Petitioner Omits its Contradictory District-Court Indefiniteness Arguments that Certain Claim-Scope Allegedly Cannot be Ascertained

In its Petition, Petitioner purports to apply “the plain and ordinary meaning of *all* claim terms as understood by a POSITA.” Pet., 5 (emphasis added). Its expert also purports to apply the plain and ordinary meaning. EX1003 ¶25.

However, Petitioner omits that—in district court using a different expert—Petitioner asserts challenged claim 27 is indefinite because a POSITA allegedly could not determine the scope of the limitation “said secrets”. EX2016, 26-29; EX2018, 15-16; EX2020, 3. The district court has now rejected Petitioner’s arguments (*see* EX2024, 3), but regardless, Petitioner’s positions are completely inconsistent and it will surely insist on preserving its indefiniteness positions for appeal (and it has not waived its right to do so).

Patent Owner respectfully submits that Petitioner should not be able to assert, on the one hand, that certain claimed scope cannot be ascertained and claims are indefinite in district court, and on the other hand, tell the Board that they are amenable to an obviousness challenge. Petitioner's failure to inform the Board about these material facts should be reason to deny the Petition as it believes that at least one challenged claim cannot actually be construed. Indeed, Petitioner is taking different positions concerning claims as the need suits. *See* 37 C.F.R. §11.18; (b)(1) (prohibiting "conceal[ment]" of material facts); 37 C.F.R. §42.11; 37 C.F.R. §42.12(b) (identifying available sanctions); *see also Microchip Tech. Inc. v. Aptiv Techs. AG*, IPR2024-00558, Paper 12, 10-12 (PTAB Oct. 7, 2024) (denying institution where Petitioner argued for indefiniteness in district court and refusing to "adopt the claim construction upon which the Petition relies because it is not persuasively argued or adequately supported by either party.").

V. LEVEL OF ORDINARY SKILL IN THE ART

For purposes of this Preliminary Response, Patent Owner does not challenge Petitioner's level of ordinary skill in the art.

VI. ARGUMENT

A. **Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination For Ground 1 Includes “Generating At Least One Limited-Use Numbers At Said Electronic Device, And Using Said Limited-Use Number In Place of At Least A Portion of Selected Account Issuer Payment Information” of Limitation 19(e).**

1. **Petitioner Ignores the Disparate Teachings in *Kalgi*’s Disclosure and Fails To Show a Motivation to Modify, or a Reasonable Expectation of Success in Modifying, *Kalgi* Figure 1 with *Kalgi* Figures 9A-10B.**

Petitioner and its expert assert, referencing *Kalgi* Figure 1, that “*Kalgi* teaches a user providing a credit card and authorization code to complete a purchase[.]” Pet., 21 (citing EX1004, [0029], [0059], FIG. 1). Petitioner and its expert then assert, referencing *Kalgi* Figures 9A-10B, that “*Kalgi* additionally teaches that its EWCP includes a User Purchase Checkout and Purchase Transaction Authorization component” wherein “a user may purchase a product from a merchant’s online site by communicating with the merchant’s PoS client or server” and that “[w]hen using the E-Wallet, the user provides payment information to the merchant, including an account number, account name, account address, CVV (static or dynamic), and other information, in a compatible data form.” Pet., 21-22 (citing EX1004, [0062], [0066], [0083], FIGs. 9A-10B, [0068]-[0069], [0084]).

This is a mischaracterization of *Kalgi* that conflates two separate embodiments for making payment transactions that use completely separate sets of components of the EWCP to transform received inputs into transaction-related

outputs: (1) a **E-Wallet Checkout (“E-Wallet”) Embodiment** depicted in Figures 1-6 using a dedicated E-Wallet and (2) a **Purchase Transaction Authorization (“PTA”) Embodiment** depicted in Figures 9A-10B that receives issued payment information from any user’s virtual wallet input and processes it for payment. *See* EX1004, FIGs. 1-6, 9A-10B; *see also* EX1004, [0185], FIG. 20.

In the **E-Wallet Embodiment**, a customer carries out payment transactions using a dedicated E-Wallet on their device that communicates with an EWCP provider. EX1004, [0029]. The EWCP provider acts as an intermediary between the user and a merchant, so that the transaction can be completed “*without* revealing the[ir] personal information to the merchant.” EX1004, [0029] (emphasis added). *Kalgi* provides examples of “personal information, such as credit card billing address and credit card information.” *See* EX1004, [0027].¹ Specifically, the customer

¹ Petitioner cites to *Kalgi*’s paragraph [0059], but that paragraph merely explains that, in an embodiment, the customer “may have to enter a payment method security code (e.g., a three digit security code on the back of a credit card) to use the[ir] selected payment method,” which is provided to the EWCP provider for verification, but it is *not* sent to the merchant, nor is it sufficient information to complete a transaction. *See* Pet., 21; EX1004, [0059], FIG. 5. The EWCP provider itself stores account information. *See* EX1004, [0060], [0181], FIGs. 5, 6, 20.

selects a payment method and provides an authentication to use the E-Wallet on their device, which selection and authentication are transmitted to the EWCP provider. *See* EX1004, [0029]-[0030], FIG. 1. The EWCP provider receives the selection and authentication information, verifies such information, processes the payment, and sends a payment confirmation to the merchant. *See* EX1004, [0029]-[0030], FIG. 1. *See also supra* Section III.A. The EWCP components used in this embodiment are the EWC, E-Wallet Checkout Payment Acquisition (“EWCPA”), and E-Wallet Checkout Payment Transaction (“EWCPT”). *See* EX1004, [0006]-[0011]; [0028]-[0062]; FIGs. 1-6.

Notably, Petitioner relies exclusively on this E-Wallet Embodiment for the element of limitation 19(a), “receiving an ... input signal corresponding to a request for payment of an online payment transaction by said electronic device,” and for the whole of limitation 19(d), “receiving, from a valid device user, a payment selection and authorization approval input on the electronic device.”² *See* Pet., 11-13 (citing

² Petitioner relies on a combination of *Kalgi* and *Khan* for limitation 19(a). *See* Pet., 11-17. Petitioner relies on *Khan* only for its “mobile device that communicates payment information via a wireless interface.” Pet., 15-16 (emphasis in original). Other than the disclosure discussed above, Petitioner also relies on *Kalgi*’s disclosure of an electronic device with a wireless interface. *See* Pet., 11-12, 14-15.

EX1004, [0039]-[0041], [0047]-[0048], [0051], FIGs. 3 & 5); Pet., 20-21 (citing EX1004, [0029], [0043], [0057], [0059], FIGs. 1, 3, & 5).³

In contrast, for limitation 19(e), Petitioner relies solely on the **PTA Embodiment** depicted in Figures 9A through 10B, wherein *Kalgi* discloses a customer providing issued payment information to directly to a merchant using a “user wallet device” with “virtual wallet features” or a “plastic card,” which the EWCP’s PTA component “transform[s] ... into a purchase transaction receipt notification.” See EX1004, [0067]-[0092], [0185], FIGs. 9A-10B, 20; *see also supra* Section III.A. For example, when a plastic card (*e.g.*, credit or debit card) is used, *Kalgi* discloses that the “PoS client may obtain, as transaction authorization input 914, track 1 data from the user’s plastic card ..., such as the example track 1 data provided below” (including personal information such as a credit card number):

%B123456789012345~PUBLIC/J.Q.^99011200000000000000**901*****?*

(wherein '123456789012345' is the card number of 'J.Q. Public' and has a CVV number of 901. '990112' is a service code, and *** represents decimal digits which change randomly each time the card is used.)

EX1004, [0068].

Kalgi further discloses that, “[i]n embodiments where the user utilizes a user wallet device, the user wallet device may provide *payment information to the PoS*

³ Petitioner also relies on *Kalgi*’s disclosure that “[t]he ‘user may provide a wallet access input ... into the user wallet device’ through a touchscreen interface.” Pet., 20.

client, formatted according to a data formatting protocol appropriate to the communication mechanism employed in communication between the user wallet device and the PoS client.” EX1004, [0069] (emphasis added). “An example listing of transaction authorization input 914, substantially in the form of XML-formatted data, is provided below:”

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

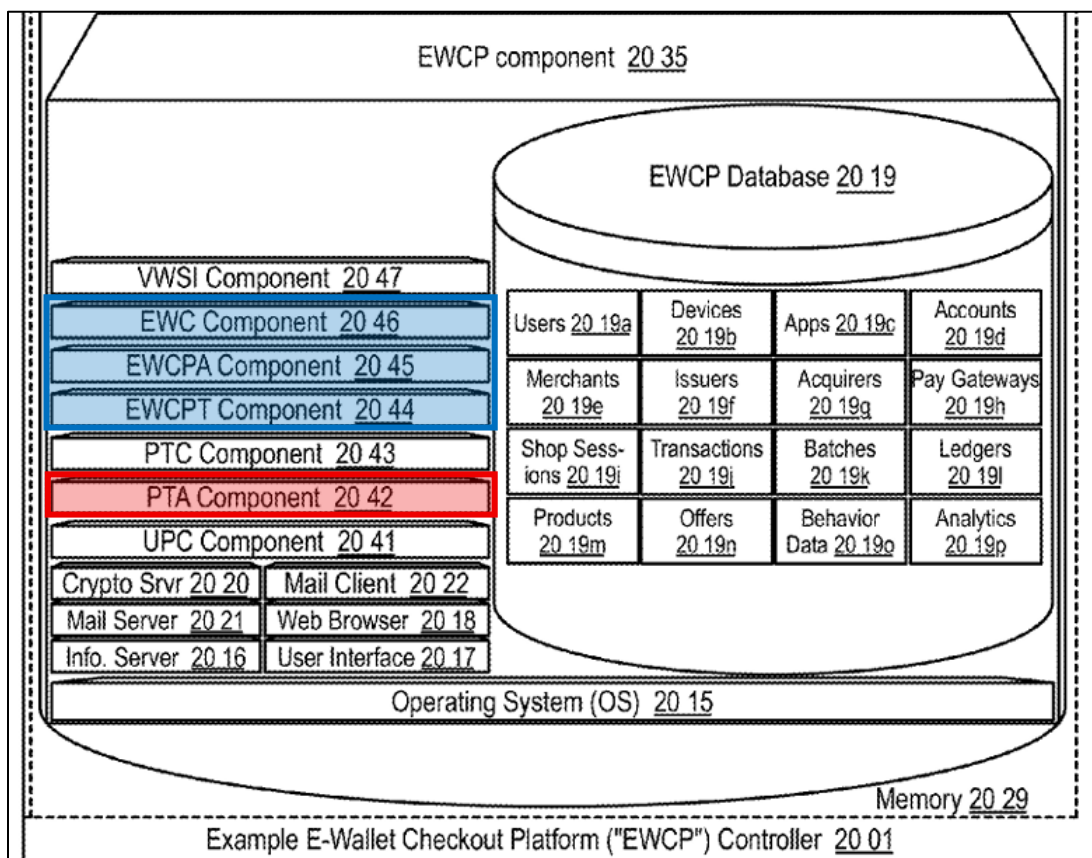
-continued

```
<cloak_flag>ON</cloak_flag>
<alert_rules>tar1 tar4 tar12</alert_rules>
<mode>Bluetooth</mode>
</account>
<account>
  <charge_priority>2</charge_priority>
  <charge_ratio>100%</charge_ratio>
  <account_number>345678901234567</account_number>
  <account_type>credit</account_type>
  <value_exchange_symbol>USD</value_exchange_symbol>
  <account_name>John Q. Public</account_name>
  <bill_add>987 Green St #456, Chicago, IL 94652</bill_add>
  <ship_add>987 Green St #456, Chicago, IL 94652</ship_add>
  <CVV_type>static<CVV_type>
  <CVV>173</CVV>
  <cloak_flag>ON</cloak_flag>
  <alert_rules>tar1 tar4 tar12</alert_rules>
  <mode>NFC</mode>
</account>
</payment_data>
<!--optional data-->
<timestamp>2011-02-22 15:22:43</timestamp>
<expiry_lapse>00:00:30</expiry_lapse>
<secure_key>0445329070598623487956543322</secure_key>
<alerts_track_flag>TRUE</alerts_track_flag>
<device_fingerprint>
  <device_IP>192.168.23.126</device_IP>
  <device_MAC>0123.4567.89ab</device_MAC>
  <device_serial>312456768798765432</device_serial>
  <device_ECID>00000AEB CDF12345</device_ECID>
  <device_identifier>jqp_air</device_identifier>
  <device_UDID>21343e34-14f4-8jn4-7yfe-124578632134</device_UDID>
  <device_browser>firefox 2.2</device_browser>
  <device_type>smartphone</device_type>
  <device_model>HTC Hero</device_model>
  <OS>Android 2.2</OS>
  <wallet_app_installed_flag>true</wallet_app_installed_flag>
</device_fingerprint>
</transaction_authorization_input>
```

EX1004, [0069]. *See also supra* Section III.A (further explaining same including transaction authorization input 914). *Kalgi* discloses that a “PoS client may generate a card authorization request, e.g., 915, using the obtained transaction authorization

input from the user wallet device,” but the resulting generated card authorization request 916 is provided to the merchant server, not to the user’s electronic device, as required by limitation 19(a), *“receiving an ... input signal corresponding to a request for payment of an online payment transaction by said electronic device.”* See EX1004, [0070]-[0071]; Pet., 11-13 (citing EX1004, [0039]-[0041], [0047]-[0048], [0051], FIGs. 3 & 5).

The components of the EWCP used for in the E-Wallet Embodiment are depicted **red** in Figure 20 below, while the components involved in the PTA Embodiment are depicted in **blue**. See EX1004, [0185], FIG. 20.



EX1004, FIG. 20 (excerpted and annotated).

Petitioner's flaw is that it fails to appreciate—let alone address—that incompatibility of these separate embodiments, where one embodiment does not transmit personal information to perform a payment transaction (E-Wallet Embodiment) but the other embodiment does (PTA Embodiment). Petitioner does not explain why a POSITA implementing the E-Wallet Embodiment, which does *not* reveal a customer's personal information to the merchant, would be motivated to combine—or have a reasonable expectation of success in combining—it with the PTA Embodiment, which *sends* (*i.e.*, *does* reveal) the customer's personal information (including credit card information) directly to the merchant. *See* Pet., 21-26; EX1004, [0027]-[0029].

Nor does Petitioner even explain why a POSITA would have looked to the PTA Embodiment at limitation 19(e) when earlier, Petitioner relies solely on features of the E-Wallet Embodiment (*e.g.*, for limitations 19(a) and 19(d)), which features do not appear in the PTA embodiment. Indeed, this combination would undo the security benefits of the E-Wallet Embodiment as disclosed by *Kalgi* (which, again, does not send any personal information) by directly transmitting a customer's credit card information to a merchant, thus making it vulnerable to interception—the very problem that Petitioner and its expert purport to solve with its *Kalgi-Varadarajan* combination. *See also* Pet. 24-26 (“A POSITA would have understood that *Kalgi*'s device could be vulnerable to attacks where the issuer provided account information

(e.g., PAN) is intercepted by an attacker and used for fraudulent transactions.”) (citing EX1003 ¶136 (repeating assertions in Petition verbatim)). Petitioner and its expert also do not explain how a POSITA would modify the system of Figure 1 to implement the system of Figure 9A-10B. *See* Pet., 21-26; EX1003 ¶¶130-137.

Petitioner does not cite its expert declaration in support of its assertions regarding *Kalgi*’s disclosures for this limitation 19(e), but just to *Kalgi*. *See* Pet., 21-23. Nevertheless, for completeness, Patent Owner notes that Petitioner’s expert declaration repeats verbatim Petitioner’s assertions. *Compare* Pet. 21-23 with EX1003 ¶¶130-131. Such unsupported, conclusory testimony—if even considered⁴—should be afforded little, if any, weight. *See Precision Cancer Techs. Inc. v. Oncoustics Inc.*, IPR2025-00242, Paper 7, 15-16 (PTAB June 3, 2025) (“[W]e give [the expert’s] *ipse dixit* testimony little weight” because “[the expert’s] testimony lacks both technical reasoning and evidentiary support; it simply mirrors the statement in Petition.”); *AT&T Servs. Inc. v. Innovative Sonic Ltd.*, IPR2024-01143, Paper 15, 27 & 38 (PTAB Feb. 11, 2025); *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15-17 (PTAB Aug. 24, 2022) (precedential); *see also*

⁴ Patent Owner respectfully submits it should not be, because paragraphs 130 and 131 of Petitioner’s expert declaration are cited nowhere in the Petition (let alone for limitation 19(e)).

Upjohn Co. v. Mova Pharm. Corp., 225 F.3d 1306, 1311 (Fed. Cir. 2000) (“Lack of factual support for expert opinion going to factual determinations, however, may render the testimony of little probative value in a validity determination.”) (quoting *Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 281, 294 (Fed. Cir. 1985)); see also *ActiveVideo Networks, Inc. v. Verizon Commc’ns, Inc.*, 694 F.3d 1321, 1327-28 (Fed. Cir. 2012) (rejecting expert’s conclusory and generic testimony that “bears no relation to any specific combination of prior art elements” and “also fails to explain why a person of ordinary skill in the art would have combined elements from specific references *in the way the claimed invention does.*”) (emphasis in original).

2. Petitioner and Its Expert Fail to Show a Motivation to Combine *Kalgi* and *Varadarajan*

Petitioner argues that it would have been obvious to combine *Kalgi* and *Varadarajan*. Pet., 24-26. Not so. As discussed below, it would not have been obvious for a POSITA to add the teachings of *Varadarajan* to *Kalgi*. First, Petitioner fails to address why a POSITA would combine *Varadarajan* with the combination of both *Kalgi*’s E-Wallet Embodiment and PTA Embodiment, which, as discussed above, are two separate and incompatible embodiments. See *supra* Section VI.A.1. Second, Petitioner’s assertions about alleged motivation to combine and reasonable expectation of success in combining *Kalgi* with *Varadarajan* are often conclusory and rely only on its expert’s unsupported and conclusory testimony.

Patent Owner addresses each of these, in turn, below.

First, just as Petitioner fails to address the incompatibility of *Kalgi*'s E-Wallet Embodiment and the PTA Embodiment, *see supra* Section VI.A.1, Petitioner also fails to explain how, or why, a POSITA would combine *Varadarajan* with these two incompatible embodiments.

Petitioner asserts that “[i]t would have been obvious and a POSITA would have been motivated to configure *Kalgi*'s device processor to dynamically generate a DCV or PAN to be used in place of at least a portion of the selected issuer payment account information responsive to receiving a valid user transaction payment approval” and that “[a] POSITA would have understood that *Kalgi*'s device could be vulnerable to attacks where the issuer provided account information (e.g., PAN) is intercepted by an attacker and used for fraudulent transactions.” Pet., 24-26. This entirely ignores the E-Wallet Embodiment of Figure 1, which, as explained above, does not transmit a customer's payment information at all—even though Petitioner relies on the E-Wallet Embodiment for the element of limitation 19(a), “receiving an... input signal corresponding to a request for payment of an online payment transaction by said electronic device” that begins a transaction, and for the whole of limitation 19(d), “receiving, from a valid device user, a payment selection and authorization approval input on the electronic device.” *See supra* Sections III.A, VI.A.1.

Petitioner also asserts that “[a] POSITA would have had a reasonable expectation of success in modifying Kalgi in this way because Kalgi already uses dynamic CVVs in a transaction.” Pet., 25-26 (citing EX1003 ¶137); EX1003 ¶137 (citing EX1004, [0069]-[0070]). This also entirely ignores the E-Wallet Embodiment of Figure 1, which, as explained above, does not transmit a customer’s payment information at all. *See supra* Sections III.A, VI.A.1. Petitioner and its expert do not explain why a POSITA would choose to implement the less secure PTA Embodiment of Figures 9A through 10B—and *then* modify it to incorporate the DCV of *Varadarajan*—over the E-Wallet Embodiment of Figure 1 which does not transmit any personal information (including credit card information) to a merchant to make a payment transaction. *See* Pet., 24-26; EX1003 ¶¶136-137. Nor do Petitioner and its expert explain how a POSITA would combine the E-Wallet Embodiment with the PTA Embodiment.

Also as discussed above, Petitioner’s proposed combination would undo the security benefits of the E-Wallet Embodiment by directly transmitting a customer’s credit card information to a merchant, thus making it vulnerable to interception—the very problem that Petitioner and its expert purport to solve with the *Kalgi-Varadarajan* combination. *See* Pet., 21-26; EX1003 ¶¶130-137. Petitioner and its expert do not explain how a POSITA would add *Varadarajan*’s DCV to the combination of *Kalgi* Figure 1 and Figures 9A-10B. *See* Pet., 21-26; EX1003 ¶¶130-

137. Petitioner and its expert also do not explain what information used in *Kalgi*'s E-Wallet Embodiment, if anything, a POSITA would substitute with *Varadarajan*'s DCV, let alone any reason why a POSITA would do so. *See* Pet., 21-26; EX1003 ¶¶130-137.

Second, Petitioner makes several conclusory assertions about alleged motivation to combine and reasonable expectation of success in combining the references identified in this Ground. Its expert repeats, often verbatim without any additional analysis or support, the Petition's conclusory assertions.

Patent Owner provides a few examples below, which are likewise dispositive of Petitioner's Grounds.

For its *Kalgi-Varadarajan* combination, Petitioner conclusorily asserts that (1) a POSITA would have been motivated to "configure *Kalgi*'s device processor to dynamically generate a DCV or PAN to be used in place of at least a portion of the selected issuer payment account information responsive to receiving a valid user transaction payment approval"; (2) that "a POSITA would have been motivated to configure *Kalgi* to implement *Varadarajan*'s method of dynamically generating a DCV to be used in place of a PAN or CVV to improve similar mobile payment

systems in the same way for online transactions”;⁵ and (3) that the “[s]ubstitution of Kalgi’s CVV or PAN with Varadarajan’s DCV is utilizing known techniques to improve similar devices that would have predictably increased the security of Kalgi’s payment system and further protected the user’s account information.” Pet., 24-25. Petitioner relies solely on its expert declaration to support these assertions, which repeats the Petition verbatim, down to the same citation to *Varadarajan*. Compare Pet., 24-25 with EX1003 ¶136. Such unsupported, conclusory testimony should be afforded little, if any, weight. See *Precision Cancer*, IPR2025-00242, Paper 7, 15-16; *AT&T Servs.*, IPR2024-01143, Paper 15, 27 & 38; *Xerox*, IPR2022-00624, Paper 9, 15-17; see also *Upjohn*, 225 F.3d at 1311; *ActiveVideo Networks*, 694 F.3d at 1327-28.

Petitioner also asserts that “[t]he concept of dynamic CVVs and PANs was well-known and a POSITA would have been familiar with using such numbers in connection with payment transactions,” and its expert largely repeats these assertions. Pet., 25; EX1003 ¶136. Petitioner’s expert, purportedly in support of

⁵ Petitioner’s expert’s declaration also, at times, discusses an entirely different combination. See EX1003 ¶136 (“[A] POSITA would have been motivated to configure Lin’s mobile device to generate a dynamic card value, such as a DCV, as a replacement for the issuer provided CVV.”).

these statements, describes references disclosing “us[e of] dynamic verification values that were unique to each transaction in place of static CVVs” in payment transactions. *See* EX1003 ¶136 (citing “Section V.C.2”,⁶ EX1043, EX1033, EX1007). Beyond being an improper incorporation by reference—Petitioner never cites or discusses the underlying references in the Petition⁷—each of the cited references disclose a *complete* solution in which dynamic CVVs are used as a security measure when transmitting actual, issued credit card numbers when making a payment transaction. *See* EX1029, FIG. 27, [0163], [0225] (noting that inputs from a point-of-sale for verifying a cryptogram received for a transaction “may comprise

⁶ Section V.C.2 does not exist. *See* EX1003. Patent Owner will assume, for purposes of this Preliminary Response, that Petitioner’s expert intended to cite to Section VI.B.2 of his report, which relies on U.S. Patent App. Pub. Nos. 2008/00110983 (“Ashfield”), 2011/0140841 (“Bona”), and 2013/0054474 (“Yeager”). *See* EX1003 ¶¶78-82 (citing EX1033, EX1043, EX1029).

⁷ *See NearMap US, Inc. v. Pictometry Int’l Corp.*, IPR2024-00729, Paper 9, 21-22 (PTAB Oct. 10, 2024) (“We also agree that, to the extent Petitioner is relying on [the expert] to supply arguments and explanations missing from the Petition, such reliance is improper.... Our rules expressly prohibit such incorporation by reference.”) (citing 37 C.F.R. §42.6(a)(3)).

a cryptogram, a PAN, a UN, a transaction data”); EX1033, FIG. 5, [0032], [0034] (“‘[C]redit card data’ ... refers to the standard package of information that describes a payment card for use in a transaction, *such as, card number, expiration date, card holder name*, etc. [I]f the dynamic CVV card to be authorized ... is a credit card and processing branches to block 522 [of Figure 5], where the dynamic CVV is again separated from the credit card data” (emphasis added)); EX1043, FIG. 2B, [0053] (“The card controller 216 controls the magnetic stripe emulator 214 for transmitting secure transaction data during a transaction, e.g., a credit card swipe transaction. Importantly, this data includes not only standard secured data, such as the static transaction data called for by governing specifications (e.g., account holder name, account number, etc.) but also dynamic information.”); EX1007, 6:49-54 (“FIG. 4 depicts an exemplary record format for transmitting payment data, with the dCVV embedded therein [It] is created by concatenating a primary account number 401 for the payment service, with a time of day 402, and a service code 403.”).

Accordingly, Petitioner has failed to meet its burden to show a motivation to combine the two embodiments of *Kalgi* to disclose “generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information[]” which is dispositive of Ground 1, as well as Grounds 2, 3, and 5 (as it pertains to claim 23), which challenge claims 20-24 that depend from claim 19. That is, this should be

dispositive given that this limitation is in every Challenged Claim that depends from claim 19. However, for completeness, Patent Owner further notes that Petitioner does not rely on *Khan* to disclose a “generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information[.]” *See* Pet., 21-26.

B. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combinations for Grounds 3 and 7 Have A “Static Device Account Number [] of a Limited Scope of Valid Use to a Specific Device” of Claim 21 or a “Static Device-Specific Account Number . . . Limited in Use To the Device” of Limitation 27(b)

Grounds 3 and 7 of the Petition also fail for a dispositive reason. Petitioner fails to show that its proposed obviousness combination for Ground 3 includes a “static device account number [] of a limited scope of valid use to a specific device” as required by the following limitations:

1. 21(a), requiring “wherein at least a portion of said limited-use number *comprises a static device account number*, and wherein the *static device account number is of a limited scope of valid use to a specific device*,
2. 21(b), requiring “wherein further a payment processing authority provides *said device account number unique for the specific electronic device*, in place of payment issuer information, in performing payment transactions by the electronic device, and further comprising:”

3. 21(d), requiring “combining the dynamically-generated number and *the static device account number* within a *device-generated complete payment information*; and”
4. 21(e), requiring “conveying said *device-generated complete payment information*, in place of a selected payment issuer information, when the device is performing payment transactions; and”
5. 21(f), requiring “wherein a using of *said static device account number* without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage.”

EX1001, 23:51-24:8 (emphases added).

Petitioner similarly fails to show that its proposed obviousness combination for Ground 7 includes a “static device-specific account number ... limited in use to the device” as required by limitation 27(b), which recites, “a *static device-specific account number* known to a payment processing authority and *limited in use to the device* use [*sic*: used] in place of an issuer payment method[.]” EX1001, 25:41-26:5 (emphases added).

1. Petitioner Fails to Show That *Smith*’s PPAN is “For a Specific Device” or “Limited in Use To [A] Device”

Petitioner relies solely on *Smith* as allegedly disclosing the claimed “static device account number [] of a limited scope of valid use to a specific device” of claim 21 and “static device account number ... limited in use to the device” of

limitation 27(b). Pet., 36-44, 72. In particular, Petitioner asserts, in reference to Ground 3 regarding limitation 21(a), that the PPAN of *Smith* is the “static device account number [] of a limited scope of valid use to a specific device” and does not rely on any other reference for this element when discussing this element in limitations 21(b) through 21(f). See Pet., 36-44 (“Therefore, a POSITA would understand because the PPAN is associated with a specific account and mobile device, it is a static device account number for a specific device.” (emphasis in original)); EX1003 ¶¶153-159, 165-169 (same). Petitioner does not make any substantive arguments for the element “static device account number ... limited in use to the device” of limitation 27(b) in Ground 7, stating only, “See Claims 19(f), 21(a)-(e), 29(a).”⁸ See Pet., 72; see also EX1003 ¶236 (same).

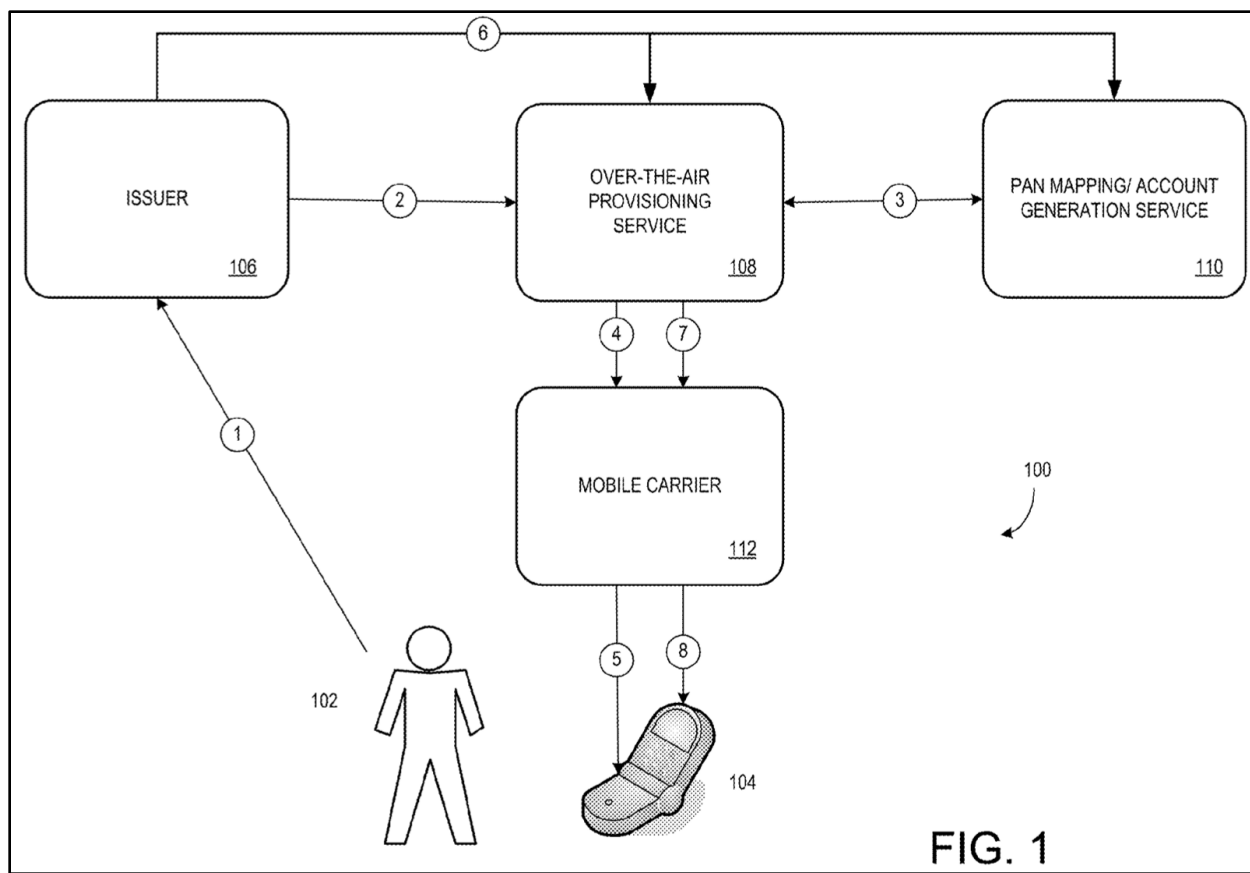
Petitioner’s assertion is incorrect. *Smith* never once says that the PPAN is a “static device account number [] of a limited scope of valid use to a specific device,” or is a “static device account number ... limited in use to the device,” or is limited to (or even based on) a particular device in any way. Rather, the PPAN is account-

⁸ Claim limitations 19(f), 21(c), and 29(a) do not require a “static device account number [] of a limited scope of valid use to a specific device” of claim 21 or a “static device-specific account number ... limited in use to the device” of limitation 27(b). See EX1001, 23:16-18, 23:54-55, 23:62-64, 25:47-50, 26:35-53.

based and, per *Smith*'s explicit language, can be mapped to multiple devices and used independently of whether a device is enabled or disabled for payment transactions. EX1008, [0029], [0041]. In sum, as explained further below, there is no indication anywhere in *Smith* that the PPAN is tied to a device identifier, or is limited in use to a particular device.

* * * *

As explained in Section III.D, above, *Smith* is directed to a temporary account number (temporary "PAN") that a customer can use during the delay between "a request from a consumer to activate a payment account in connection with a mobile device and the time at which an issuer can establish an actual account in response to that request." EX1008, [0002]. The *Smith* invention allows an account holder to "access the account during a time period in which the issuer systems are updated to include the actual payment account number (or 'actual PAN')." EX1008, [0012]. Once the issuer systems have updated, the actual PAN is used instead of the temporary one. EX1008, [0012].



EX1008, FIG. 1.

Figure 1 (above) outlines a PAN and temporary PAN provisioning system. The process starts (transaction “1”) when a customer contacts an issuer 106 “via one or more web sites or by contacting a customer service representative.” EX1008, [0014]. The customer is then taken through a registration process in which the customer selects a verification code that will be used in a mobile device 104 personalization process. EX1008, [0014]. Importantly, there is no disclosure that the user ever provides a device ID during this registration process. *See* EX1008, [0014]. Indeed, the user does not even need to register the device they are using to carry out the registration; the user can simply visit a website or call a customer representative

(presumably from any device). *See* EX1008, [0014], [0028]. The user gets a verification code that allows for personalization on the device, but the disclosure suggests this is device-agnostic—it could be any device, or multiple devices. *See* EX1008, [0014], [0028]. But either way, the issuer is blind to the device information during this registration step.

In the next step (transaction “2”), the issuer transmits data elements to an OTA provisioning service. These can include a request to “provision a new account with the temporary PAN” and “risk data elements,” such as a spending limit. EX1008, [0015]. *Smith* does not indicate that any “device” based information is transmitted; it is all account-based. Petitioner focuses on transaction “3,” where the OTA provisioning service forwards a message “to a PAN mapping/account generation service 110 so that a PayPass PAN (or ‘PPAN’) may be assigned to the mobile device 104. EX1008, [0016]; Pet., 37. “The PAN mapping/account generation service 110 assigns a PPAN to the device 104, and also maps the newly-assigned PPAN to the temporary PAN provided by the issuer 106.” EX1008, [0016]. These two sentences in *Smith* effectively form the basis for the entirety of Petitioner’s argument that the PPAN is a “static device account number [] of a limited scope of valid use to a specific device” of claim 21 and is a “static device-specific account number ... limited in use to the device” of limitation 27(a). *See* Pet., 37 (citing EX1008, [0016]), 72. Petitioner misinterprets *Smith*’s disclosure and, notably, omits

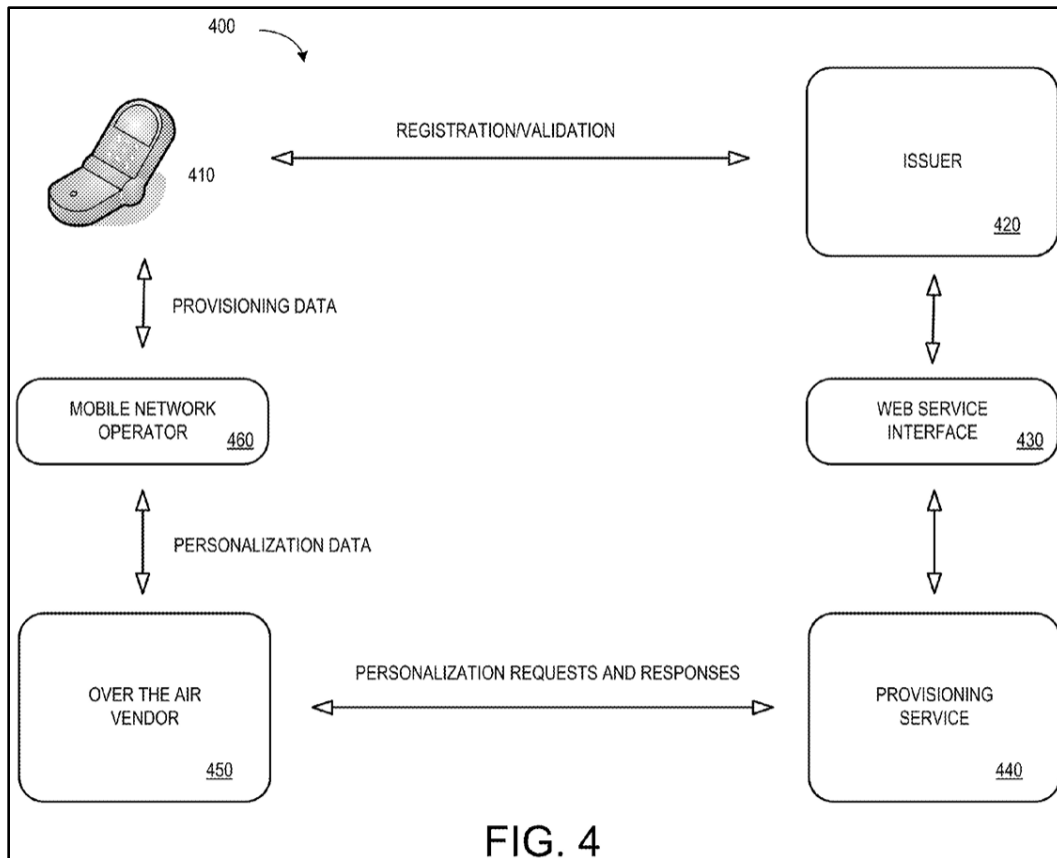
any contextual explanation of this paragraph or *Smith*'s actual invention in its discussion of these device-specific static limited-use payment information limitations. *See* Pet., 36-44, 72.

Smith explains that upon receipt of the request (transaction "2") to provision (or install) the payment application and account information in the customer's mobile device, "the OTA provisioning service 108 begins creating a software package or applet for delivery to the customer's mobile device. [sic] 104." EX1008, [0016]. Once the mapping has been established (*i.e.*, the PPAN to temporary PAN), the "newly assigned PPAN is returned to the OTA provisioning service 108 for inclusion in the software package to be installed on the mobile device 104." EX1008, [0016]. *Smith* explains that the "software package may contain the software code required to install the PPAN, the risk parameters (if any), and other application information in the mobile device 104[.]" EX1008, [0017]. In other words, the provisioning of the PPAN to a mobile device is based upon the need to include that PPAN in the software package instance that is going to be provisioned; it is tied to the software and account, and not any device-identifying information.

In connection with transactions "4" and "5," the customer enters a verification code "to confirm the customer's identity and to authorize the installation of the software." EX1008, [0018]. Again, the verification code may be entered in a device,

but it is used to confirm the “customer’s identity,” and not a device identity. *Smith*’s approach is device-agnostic.

Once the identity of the customer is established, the personalization process is initiated. EX1008, [0018]. This is described in further detail with respect to Figure 4 of *Smith* (below) and related disclosure. EX1008, FIG. 4, [0028]-[0029]. In order to initiate that process, the consumer can access a website or contact a customer service representative and input personal information, a “model number” of the mobile telephone, or a phone number. EX1008, [0028]. Notably, there is no discussion of inputting a Device ID. As part of the personalization process, the provisioning service may “obtain or create a PPAN and add it to a PAN mapping database.” EX1008, [0029]. Importantly, *Smith* indicates that “multiple NFC-enabled handsets may be managed for a single account.” EX1008, [0029]. In other words, *Smith* indicates that none of the PPAN, the temporary PAN or the actual PAN is device specific. They are each available for use on multiple devices.



EX1008, FIG. 4.

After personalization and after the issuer has updated their systems, the issuer provides a message to the mapping/account generation service 110 to update the database with the actual PAN, replacing the temporary PAN. EX1008, [0019]. This is transaction “6.” In all of *Smith’s* examples, this actual PAN, as well as the temporary PAN and the PPAN, are mapped to the customer account (and the actual PAN is mapped to the PPAN). They are not mapped to a device identifier or a specific device. Figure 6 (below), illustrates this. It is an example of a “database 600 that may be used in connection with the payment account apparatus 500.” EX1008, [0038].

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

EX1008, FIG. 6. As can be seen from Figure 6, there is no “Device ID” or any specific device identified. Rather, a “Consumer ID” is mapped to various account numbers, including a temporary PAN, a Mobile PAN, and an Actual PAN. *See also* EX1008, [0039]. The PPAN is a type of Mobile PAN. EX1008, [0026]. *Smith* explains that “[t]he consumer identifier 602 might be [a] code that uniquely identifies a consumer who has requested that his or her mobile device be enabled to complete purchase transactions.” EX1008, [0040]. Again, this is a mapping to a “Consumer ID,” irrespective of which device(s) that consumer wants to enable.

The other disclosures in *Smith* all indicate that the PPAN is linked to an actual PAN or a temporary PAN at any given time, and that these PANs are account numbers, not device numbers. EX1008, [0013] (“a primary *account* number (or

‘PAN’)), [0023] (“the payment network 218 *identifies the PPAN and requests a look up of the related PAN;*” and “where the issuer 206 has not yet issued an actual PAN, the look up will return the *temporary PAN associated with the PPAN.*”) (emphases added).

Smith further describes that a “PayPass *account*” is a type of “payment *account*”; indeed, “PPAN” literally stands for PayPass Primary *Account* Number. EX1008, [0012] (“In some embodiments, features of the present invention allow a payment account issuing financial institution (an ‘issuer’) to effect instant issuance of a payment *account* (such as a *PayPass account*) over a mobile network to a mobile device without the need to set up the payment account within the issuer systems at the time of issuance.”) (emphases added); *see also, e.g.*, EX1008, [0016] (“a PayPass PAN (or ‘PPAN’)”). Logically, a PPAN—*i.e.*, a PayPass payment *account* number—is simply a PAN for a PayPass account generally (and not device-based). *Smith* effectively states as much, indicating that a PPAN is mapped to a “funding account,” and not to a particular device. EX1008, [0041] (“[A] provisioning service might arrange for a mobile phone to be associated with a funding account (e.g., by creating a PPAN and *mapping the PPAN to a provided funding account* in an account management system”) (emphasis added). *Smith* states that the mobile device may also be associated with that funding account, but that does not mean that the mobile device and the PPAN are associated with each other. Rather, each of the

PPAN or the mobile device may be independently disassociated from that funding account. *See* EX1008, [0041] (disclosing that the provisioning service may “disable the payment application on the mobile phone (without [*sic*: with] or without removing the personalization details)”); EX1008, [0028]-[0029], FIG. 4 (disclosing that personalization details include the PPAN). A PPAN could be re-assigned to a new device, or the same device could be provisioned with a new PPAN. *See* EX1008, [0041]. *Smith* is consistent with each of these possibilities.

* * * *

In sum, Petitioner latches on to two sentences in Paragraph 16 of *Smith* to argue that the PPAN is a “static device account number [] of a limited scope of valid use to a specific device” of claim 21 or a “static device account number ... limited in use to the device” of limitation 27(b). Pet., 36-44, 72. But, when read in context, it is clear that the PPAN is linked to an account—initially a temporary PAN, and then later, an actual PAN—and not a particular device. *Smith*’s statement that a PPAN is “assigned to the mobile device,” is nothing more than shorthand to explain that a PPAN is provisioned to a mobile device (or “multiple NFC-enabled handsets,” EX1008, [0029]) as part of a personalized software package, which itself is tied to a Consumer ID and customer account. Figure 6 is strong evidence of this—it maps all of the different account numbers to a Customer ID without any mention of a device identifier. EX1008, [0039]-[0040], FIG. 6. And, even during the registration process,

the user only provides a phone number (device-agnostic, and device-changeable), personal information, and a model number (which could apply to countless actual devices). EX1008, [0028]. There is no indication anywhere in *Smith* that there is any mapping of a PPAN to a particular device, or even that the provisioning service is aware of the identity of the device to which it is provisioning the software. It appears to just be using the “phone number.” *See* EX1008, [0028].

Accordingly, Petitioner has failed to meet its burden to show that *Smith* discloses a “static device account number [] of a limited scope of valid use to a specific device” of claim 21 or a “static device account number ... limited in use to the device” of limitation 27(b). This is dispositive of Petitioner’s Grounds 3 and 7 and demonstrates that Petitioner has not shown a reasonable likelihood of success as to challenged claims 21 and 27. However, for completeness, Patent Owner notes that *Kalgi*, *Khan*, and *Varadarajan* also fail to disclose a “static device account number [] of a limited scope of valid use to a specific device” of claim 21 or a “static device account number ... limited in use to the device” of limitation 27(b)—nor does Petitioner so argue. *See* Pet., 36-44, 72. Although each of *Kalgi*, *Khan*, and *Varadarajan* disclose using substitute payment information, none of them disclose that such information is “for a specific device” or “limited in use to the device.” *See supra* Sections III.A-C.

2. Petitioner and Its Expert Fail to Show a Motivation to Combine *Kalgi* with *Smith* and with *Varadarajan*

Petitioner argues that it would have been obvious to combine *Kalgi* and *Smith*. Pet., 39-41. Not so. As discussed below, it would not have been obvious for a POSITA to add the teachings of *Varadarajan* to *Kalgi*. First, Petitioner fails to address why a POSITA would combine *Smith* with the combination of both *Kalgi*'s E-Wallet Embodiment and PTA Embodiment and with *Varadarajan*, which, as discussed above, are two separate and incompatible embodiments. *See supra* Section VI.A.1. Second, Petitioner's assertions about alleged motivation to combine and reasonable expectation of success in combining *Kalgi* with *Smith* are often conclusory and rely only on its expert's unsupported and conclusory testimony.

Patent Owner addresses each of these, in turn, below.

First, similar to its proffered motivation to combine for limitation 19(e), Petitioner's proffered motivations to combine for limitations 21(a) and 27(b)—Petitioner does not proffer any separate motivation to combine for limitations 21(b) and 21(d)-(f)—also entirely ignore the E-Wallet Embodiment of Figure 1 of *Kalgi*, which does not transmit a customer's payment information in a transaction at all. *See supra* Sections III.A, VI.A.1-2; Pet., 36-44, 72. Petitioner and its expert do not explain why a POSITA would choose to implement the less secure PTA Embodiment—and *then* modify it to replace the transmitted payment information with *Smith*'s PPAN and *then further* modify *Smith*'s PPAN with *Varadarajan*'s

DCV—over the E-Wallet Embodiment which does not transmit *any* personal information (including credit card information) to a merchant to make a payment transaction *See supra* Sections III.A, VI.A.1-2; Pet., 24-26, 36-41, 72; EX1003 ¶¶136-137, 160-164.

Second, for its *Kalgi-Smith* combination, Petitioner asserts that a POSITA would have “appreciated that storing a PPAN would be safer than storing the actual account number on Kalgi’s device,” that “[a] POSITA would have been motivated to use Smith’s PPAN in place of Kalgi’s account number so that Kalgi’s mobile device would not be required to store the account number, which is a sensitive financial number” and that “[i]t was well known in the art that a mobile device could be vulnerable to malicious attacks and therefore storing Smith’s PPAN instead of the account number on Kalgi’s mobile device would have increased security for the user’s account,” Pet., 39-40, but Petitioner relies *solely* on its expert declaration to support these assertions, which largely repeats the same language as the corresponding passages of the Petition without *any* evidence or analysis. *Compare* Pet., 39-40 *with* EX1003 ¶¶160-161. Such unsupported, conclusory testimony should be afforded little, if any, weight *See Precision Cancer*, IPR2025-00242, Paper 7, 15-16; *AT&T Servs.*, IPR2024-01143, Paper 15, 27 & 38; *Xerox*, IPR2022-00624, Paper 9, 15-17; *Upjohn*, 225 F.3d at 1311; *ActiveVideo Networks*, 694 F.3d at 1327-28.

The sole analysis that Peititoner’s expert provides in support of this motivation to combine is that a POSITA “would have understood that it is valuable to remove account numbers from a user device so that if the device were stolen, the thief would have access only to PPAN(s),” and “would have recognized that this is beneficial because if a user’s device is lost or stolen, only the PPAN(s) would have to be cancelled.” See EX1003 ¶161 (citing EX1043, [0007], [0014], [0074], FIG. 6). Neither *Kalgi* nor *Smith* describe cancelling a PPAN. See generally EX1004, EX1008. And Petitioner’s citation to its expert’s discussion of *Bona* does not support these assertions.⁹ *Bona* at [0074] describes storing a fingerprint template on a smart chip of a smart card as part of the “biometric enrollment process” of Figure 6 “for initializing the smart card 200 with a user’s fingerprint template for later use in authenticating the user during transactions.” See EX1043, [0068], [0074], FIG. 6. *Bona* at [0007] describes preventing fraud using smart cards by “includ[ing] some dynamic data in the transaction authorization process” and chip and PIN systems where customers enter a PIN to authorize their smart card transactions—*i.e.*, using additional numbers to verify static issued payment information. See EX1043, [0007].

⁹ To the extent Petitioner relies on citations to its expert’s declaration to supply arguments missing from the Petition (about references missing from the petition), such reliance is also improper. See *NearMap*, IPR2024-00729, Paper 9, 21-22.

Finally, *Bona* at [0014] states: “FIG. 1 is a block diagram of a smart card application management system.” *See* EX1043, [0014]. Petitioner’s expert does not explain how any of these paragraphs from *Bona* relate to PPAN(s), “remov[ing] account numbers from a user device,” or cancelling a device’s PPANs in the event it is compromised, let alone the “static device account number [] of a limited scope of valid use to a specific device” of limitation 21(a) or the “static device account number ... limited in use to the device” of limitation 27(b). *See* EX1003 ¶161. For the same reasons above, such unsupported, conclusory testimony should be afforded little, if any, weight.

Petitioner also asserts that “[a] POSITA would have further found it obvious and been motivated to use the PPAN to generate a dynamic partial PPAN, as taught by Varadarajan,” and that “in combination, Kalgi-Khan-Varadarajan-Smith would generate a dynamic CVV and dynamic partial PPAN (DCV + portion of the PPAN, which is of limited scope of valid use to the user’s specific device.” *Pet.*, 41 (citing EX1003 ¶164 (same) and “Claim 19(e)”). Such unsupported, conclusory testimony should, again, be afforded little, if any, weight. *See Upjohn*, 225 F.3d at 1311; *ActiveVideo Networks*, 694 F.3d at 1327-28.

The Petition and paragraph 164 of Petitioner’s expert report reference back to “Claim 19(e).” *See Pet.*, 41. Even if searched and considered,¹⁰ Petitioner and its

¹⁰ *NearMap*, IPR2024-00729, Paper 9, 21-22.

expert's discussion of that limitation do not support the particular limitation or combination Petitioner relies on here. *See supra* Section VI.A. For limitation 19(e), Petitioner and its expert assert that it would have been obvious to modify the *Kalgi* to dynamically generate *Varadarajan*'s DCV. *See* Pet., 21-26 (citing EX1003 ¶¶134, 136-137); *see supra* Section VI.A. It says nothing, for example, about a PPAN (an element disclosed by *Smith*, not *Kalgi* or *Varadarajan*, *see supra* Section III), let alone “us[ing] the PPAN to generate a dynamic partial account number,” or “dynamic partial PPAN.” *Compare* Pet., 21-26 (citing EX1003 ¶¶134, 136-137) *with* Pet., 41 (citing EX1003 ¶164); *see supra* Section VI.A. And regardless, as discussed above, Petitioner fails to show a motivation to combine *Kalgi* and *Varadarajan* in the manner asserted and its assertions are likewise conclusory. *See supra* Section VI.A.2.

Accordingly, Petitioner has failed to meet its burden to show a motivation to combine *Kalgi*, *Smith*, and *Varadarajan* to disclose the “static device account number [] of a limited scope of valid use to a specific device” of limitation 21(a) and the “static device-specific account number ... limited in use to the device” of limitation 27(b), which is dispositive of Grounds 3 and 7. That is, this should be sufficient to deny institution as to these Grounds. However, for completeness, Patent Owner further notes that, in Ground 3, Petitioner does not rely on *Khan* to disclose the “static device account number for a specific device” of limitation 21(a). *See* Pet.,

36-41. Petitioner also does not rely on *Kranzley* or *Hammad* in Ground 7 to disclose the “static device-specific account number ... limited in use to the device” of limitation 27(b). *See* Pet., 72.

C. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combinations for Ground 4 Includes “Generat[ing] A Device-Specific Limited-Use Payment Information” of Limitations 25(f), 25(g), and 25(h).

Ground 4 of the Petition fails because Petitioner fails to show that its proposed obviousness combination includes “generat[ing] a device-specific limited-use payment information” as required by the following limitations:

1. 25(f), requiring “responsive to receiving a valid user transaction payment approval, *generate a device-specific limited-use payment information* for use in place of at least a portion of said selected issuer payment account information on the device,”
2. 25(g), requiring “form a *complete combined device payment information* from a *dynamically generated portion* and a statically generated portions stored in a memory of the device,”
3. 25(h), requiring “wherein the communication interface is operable to transmit said *complete device payment information* from said electronic device to the recipient of the online purchase transaction[.]”

EX1001, 24:66-25:10 (emphasis added).

1. Petitioner Fails to Explain Why Its “Dynamic Partial PPAN” Is “Device-Specific.”

Petitioner and its expert assert, “[a]s discussed in Claim 21(a), a DCV can be generated and used as part of a PPAN Because the PPAN is device-specific, a POSITA would understand a dynamic partial PPAN is device-specific limited-use payment information that is used in place of the PPAN.” Pet., 50 (citing “See Claim 21(a), *see also* Claim 19(e);¹¹ Dec. [EX1003], ¶180.”) (alternation and emphasis in original); EX1003 ¶180 (same). As discussed above, *Smith* does not teach that its PPAN is device-specific—to the contrary, *Smith* teaches that the PPAN can be shared on multiple mobile devices. *See supra*, Section VI.B; EX1008, [0018], [0029], [0041]-[0042]. Accordingly, Petitioner’s reliance on *Smith*’s PPAN is insufficient for Petitioner to carry its burden to show this claim limitation is disclosed in *Smith*.

2. Petitioner Fails to Explain Why *Varadarajan*’s DCV is “Device-Specific”

Petitioner also asserts that “Varadarajan’s DCV, e.g., dynamic PAN and/or CVV, is device-specific limited-use payment information that is dynamically generated for use in place of at least a portion of said selected issuer payment

¹¹ Claim 19(e) does not recite “device-specific.” *See* EX1001, 23:11-14. Petitioner’s assertions regarding claim 19(e) do not argue otherwise. Pet., 21-24.

account information (e.g., the PAN, CVV, etc.) on the device.” Pet. 51, (alteration and emphasis in original). Petitioner’s sole basis for asserting that the DCV is device specific consists of a single conclusory sentence: “Additionally, or alternatively, Varadarajan’s DCV is also device-specific because the DCV generator uses ‘a device derived identification parameter ... which is unique to the user device or machine used to host the DCV generating application.’” Pet., 50-51 (alterations and emphases in original and citing EX1006, [0029], [0053]). Its expert includes the same conclusory sentence—verbatim with the *same* emphasis and alterations and *without* any additional explanation or analysis. EX1003 ¶181. However, such conclusory assertion—simply quoting (and as explained below, mischaracterizing and oversimplifying) *Varadarajan*—is insufficient for Petitioner to carry its burden to show this claim limitation is disclosed in *Varadarajan*. See *Precision Cancer*, IPR2025-00242, Paper 7, 15-16; see also *Xerox*, IPR2022-00624, Paper 9, 15-17.

Indeed, not only does Petitioner’s (and its expert’s) conclusory assertion fail to show that the DCV is device-specific, but it is also an oversimplification and mischaracterization of *Varadarajan*’s actual disclosure. In context, when the teachings of *Varadarajan* are considered—including the full statements that Petitioner misleadingly and partially quotes—*Varadarajan* makes plain that the “device-derived identification parameter” is *not* used to generate, and itself is *not* a

part of, the DCV. Instead, it is used in various steps to ensure the security of the DCV application which hosts the DCV generator that actually generates the DCV.

To begin, Petitioner combines and selectively quotes portions of sentences from separate disclosures in *Varadarajan* (at paragraphs [0029] and [0053]). Pet., 50-51. The full quotes that Petitioner combines and ellipses overstate the following (underline to show material omitted by Petitioner; bolding and italics added for emphasis):

Additional advantages can be realized with the ability to securely host the software client (DCV generating application) on a variety of mobile phones and user handheld devices (iPhone™, Blackberry™, etc.), including increased user convenience, for example, by not requiring a user to contact the bank to obtain a replacement credit or debit card when the user believes his PAN and/or CVV may have been compromised. The ability to generate a DCV (PAN or CVV), without a PIN input to the user device may provide an additional user convenience. Another layer of security can be provided where the DCV generator is further protected using a device derived identification parameter or device generated PIN which is unique to the user device or machine used to host the DCV generating application. As would be understood, the system and method described herein could also be provided and securely hosted, for example, in

JavaScript™ within a browser used by a desktop computer, laptop, netbook, or other Internet accessible computing device, to generate DCVs for online transactions.

EX1006, [0029].

It would be understood that the DCV application can be downloaded and activated on multiple user devices for the same credit/debit account. As an example, for a joint account, the DCV application could be activated on both of the joint cardholder's user devices, which also could be of different types, for example, an iPhone™ and a Blackberry™, with transparency to each user. Each user can be provided a DCV generator corresponding to the joint account, or specifically to the card issued to each of the joint cardholders, where each card may have the same or different static DCV (PAN and/or CVV). By including a device identifier in the DCV generator, where the included device identifier is unique to each user device accessing a joint account, each transaction and DCV is further identifiable to the user device conducting a transaction or requesting a DCV. In the event of multiple incorrect DCV inputs during a DCV request sequence, resetting the DCV generator can be expedited through a support telephone call and reset of the DCV application on the user device, which can, if necessary, include providing a new DCV key and providing a new DCV generator.

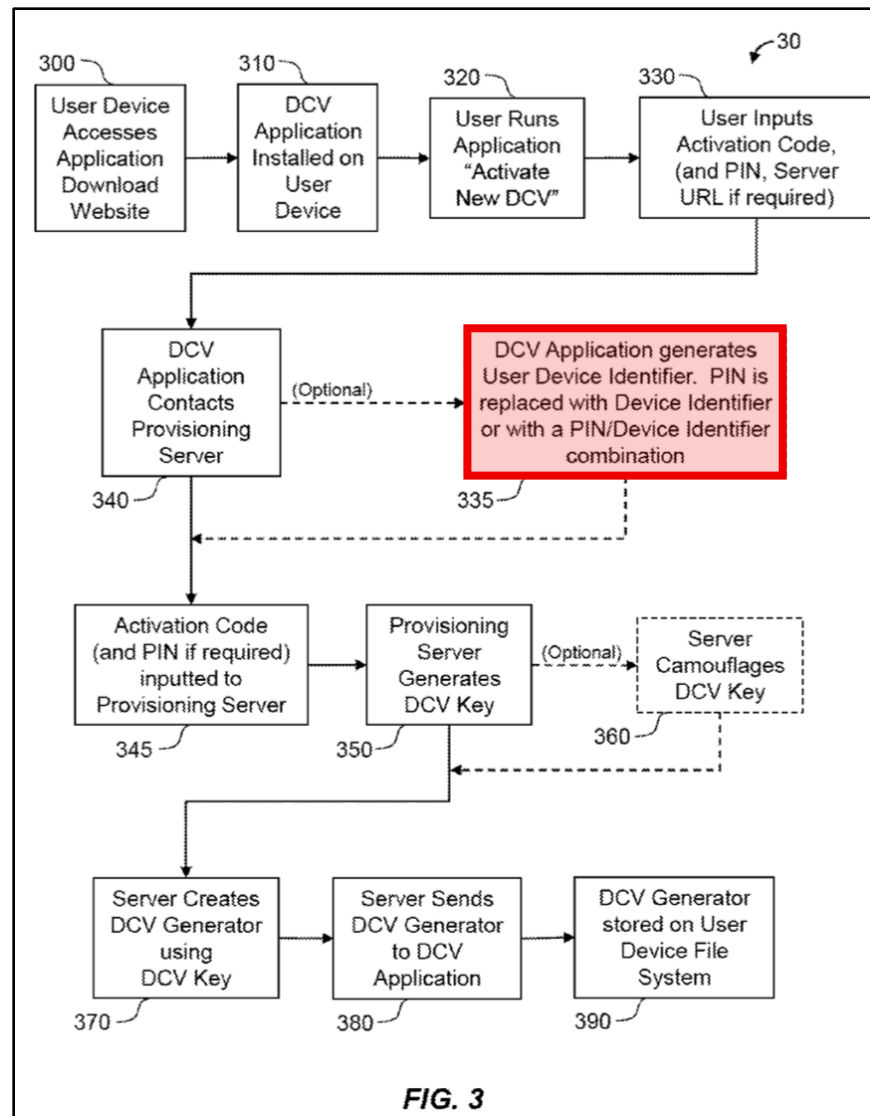
EX1006, [0053].

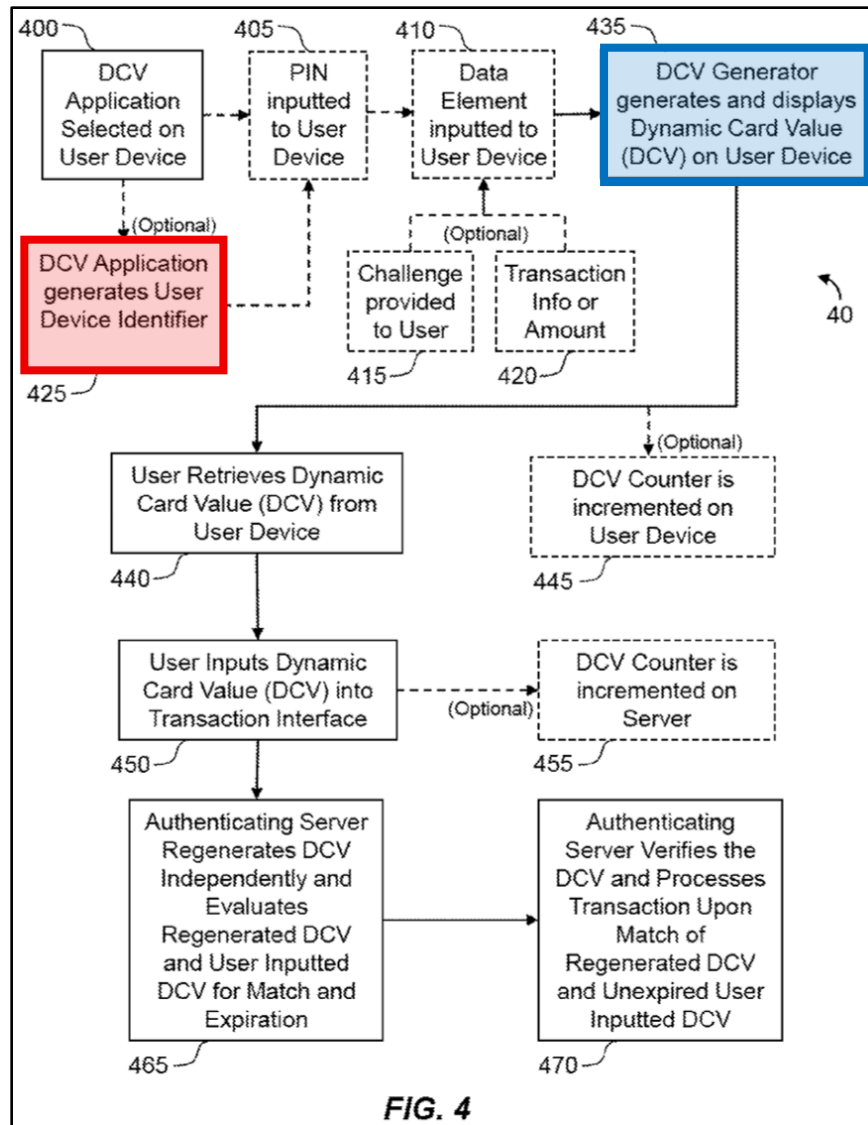
Nowhere, however, do these paragraphs show that the DCV—which Petitioner asserts is the claimed “dynamically generat[ed] ... device-specific limited-use payment information”—is itself *device-specific*. As reflected above, including in the omitted portions of the paragraphs, the “device derived identification parameter”—which Petitioner asserts makes the DCV “device-specific”—is “[a]nother layer of security [that] can be provided where the DCV generator is further protected.” EX1006, [0029] (“Another layer of security can be provided where the DCV generator is further protected using a device derived identification parameter or device generated PIN which is unique to the user device or machine used to host the DCV generating application.”). But providing “[a]nother layer of security” to the generator does *not* make the separately generated DCV itself “device-specific.”

Varadarajan further confirms Petitioner has failed to meet its burden to show that the DCV is device-specific. For example, *Varadarajan* discloses that the device identifier may be used to “cryptographically camouflage[]” the DCV generation key. *See* EX1006, [0035] (“For example, the DCV generation key may be cryptographically camouflaged using a PIN, which may be the user’s fixed or static account CVV, a device identification parameter generated from the user’s device, or some other data element. A combination of two or more of a PIN, a DCV, a device

identifier and another data element may also be used in the camouflaging process.”).

And, as shown below in Figures 3 and 4—and the corresponding explanation from *Varadarajan* excerpted below—it is used with or instead of a PIN as an extra security step (**red**), *prior to* activating the DCV application for requesting provisioning of a DCV generator or requesting generation of a DCV—generation of the DCV by the DCV generator is *a completely separate step* (shown in **blue**). See EX1006, [0049], [0054].





EX1006, FIGs. 3, 4 (annotated).

Varadarajan also explains that use of the device identifier helps detect “porting” of the DCV application. EX1006, [0049], [0054]. That is, if the DCV application is “ported to another (unauthorized) device by an attacker,” then the ported DCV application on the unauthorized device “will generate an invalid device identifier which may prompt the DCV generator to *display* a DCV which would be

recognizable as an alert code by the authenticating server.” *See* EX1006, [0054] (emphasis added). The authenticating server may decline a transaction from an unauthorized device that used the “alert code” DCV and may store the “alert code” DCV to detect further transaction requests by the same unauthorized device, making this “alert code” DCV “further identifiable to the user device conducting a transaction or requesting a DCV.” *See* EX1006, [0053]-[0054]. Accordingly, and as noted above from the excerpts that Petitioner omits in its quotations, the device identifier is “[a]nother layer of security” that protects access to the DCV generator by associating the DCV application with a particular user device—but it is *not* used to generate, nor is it part of, a DCV. *See* EX1006, [0029], [0049]; *see also* EX1006, [0049] (“Optionally, a user device identification parameter, or device identifier, may be generated at step 335 of FIG. 3, to enable an additional level of security”).

Accordingly, Petitioner has failed to meet its burden to show that *Varadarajan* discloses a “*device-specific* limited-use payment information” as required by limitations 25(f), 25(g), and 25(h), which is dispositive of Ground 4 and demonstrates that Petitioner has not shown a reasonable likelihood of success as to challenged claim 25. However, for completeness, Patent Owner notes that *Kalgi* and *Smith* also fail to disclose a “*device-specific* limited-use payment information”—nor does Petitioner so argue. *See* Pet., 50-52. *Kalgi* uses substitute and actual issued payment information in transactions which is not “dynamically generated” or

“device-specific.” *See supra* Section III.A. *Smith* uses provisioned static payment information which is not “dynamically generated” or “device-specific.” *See supra* Section III.D, VI.B.

3. Petitioner and Its Expert Fail to Show A Motivation to Combine *Kalgi*, *Varadarajan*, and *Smith*

Petitioner and its expert do not provide any motivation to combine *Kalgi*, *Smith*, and *Varadarajan* in support of its combination for Ground 4, let alone for limitation 25(f). *See* Pet., 44-54; EX1003 ¶¶170-189. Petitioner and its expert cite their discussion of limitations 19(e) and 21(a), but even if Petitioner intended by such citation to rely on the motivation to combine it asserted as to those limitations, it cannot meet its burden. *See* Pet., 44-54; EX1003 ¶¶170-189.

As explained above in reference to limitations 19(e) and 21(a), Petitioner’s proffered motivations to combine *Kalgi*, *Varadarajan*, and *Smith* are conclusory and do not explain how or why a POSITA would combine *Kalgi*’s E-Wallet Embodiment, which does not transmit payment information in making a payment transaction with *Kalgi*’s less-secure PTA Embodiment (which transmits actual issued payment information to a merchant), or why a POSITA would choose the PTA Embodiment over the E-Wallet Embodiment, and *then* combine it with *Varadarajan*’s DCV. *See supra* Sections VI.A.2 & VI.B.3. For the same reasons, Petitioner cannot meet its burden to provide a motivation to combine here.

Accordingly, Petitioner has failed to meet its burden to show a motivation to combine *Kalgi*, *Smith*'s PPAN, and *Varadarajan*'s DCV to disclose "generat[ing] a device-specific limited-use payment information for use in place of at least a portion of said selected issuer payment account information on the device" of claim 25, which is dispositive of Ground 4, as well as Grounds 5 (as it pertains to claims 28-30), 6, and 7, which challenge claims 26-30 that depend from claim 25. That is, this should be dispositive given that this limitation is in every Challenged Claim that depends from claim 25. However, for completeness, Patent Owner further notes that Petitioner does not rely on any other references in Ground 4 to challenge claim 25. *See Pet.*, 44-54.

D. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combinations for Ground 4 Includes "A Statically Generated Portions Stored In A Memory of the Device" of Limitation 25(g) and 25(h).

Ground 4 of the Petition also fails because Petitioner fails to show that its proposed obviousness combination includes "a statically generated portions stored in a memory of the device" as required by the following limitations:

1. 25(g), requiring "form a *complete combined device payment information* from a dynamically generated portion and a *statically generated portions stored in a memory of the device*,"

2. 25(h), requiring “wherein the communication interface is operable to transmit said *complete device payment information* from said electronic device to the recipient of the online purchase transaction[.]”

EX1001, 25:4-10 (emphases added).

Petitioner and its expert point to “(mobile wallet) account number, account name, billing address, etc. (a statically generated portions stored in a memory of the device).” Pet., 51-52 (citing EX1003 ¶184; “see Claims 19(e), 21(a)”). Petitioner and its expert, repeats the Petition verbatim including emphases, do not explain (1) why any of the identified pieces of information are “statically generated portions,” or (2) which reference in its proposed combination discloses these pieces of information and where these pieces of information are stored. *See* Pet., 51; EX1003 ¶184. Petitioner and its expert both cite back to their respective discussions regarding limitations 19(e) and 21(a), but do not explain why these limitations are relevant when neither limitation requires “a statically generated portions stored in a memory of the device.” *See* Pet., 21, 36, 51; EX1003 ¶184.

Accordingly, Petitioner has failed to meet its burden to show that its *Kalgi-Varadarajan-Smith* combination discloses a “a statically generated portions stored in a memory of the device” of claim 25, which is also dispositive of Ground 4, as well as Grounds 5 (as it pertains to claims 28-30), 6, and 7 which challenge claims

26-30 that depend from claim 25. That is, this should be dispositive given that this limitation is also in every Challenged Claim that depends from claim 25.

E. Additional Reasons that Petitioner has Failed to Meet Its Burden

Patent Owner has focused on three glaring issues with the Petition that pertain to all Challenged Claims. But there are many more that would need to be addressed should the Board decide to institute (and further show the lack of a reasonable likelihood of success that any challenged claim is unpatentable), including the following:

- *Smith* is incompatible with a multi-network and multi-issuer payment system. It provides that a “system” that provisions a payment application including a PPAN to customers of a single payment network, but does not explain how it could provide payment applications including a PPAN for a single customer’s multiple payment accounts spanning different networks (*e.g.*, Visa vs. MasterCard) and different issuing banks. Petitioner does not explain why a POSITA would look to *Smith* as a cross-network and cross-issuer solution. *See supra* Section III.D. In contrast, *Kalgi*’s Figure 2 shows that its payment application can accommodate multiple payment networks and banks. *See supra* Section III.A.

VII. CONCLUSION

For the reasons stated above, Petitioner's proposed combinations fail to disclose key limitations of the Challenged Claims of the '538 Patent. Petitioner has also failed to show a motivation to combine or reasonable expectation of success in combining the references in its Grounds. Therefore, Petitioner has failed to show a reasonable likelihood of success that any challenged claim is unpatentable for any Ground. Patent Owner respectfully submits that institution should be denied.

Dated: October 15, 2025

Respectfully submitted,

/Matt Berkowitz/

Matthew G. Berkowitz (Reg. No. 57,215)

mberkowitz@reichmanjorgensen.com

REICHMAN JORGENSEN

LEHMAN & FELDBERG LLP

100 Marine Parkway, Suite 300

Redwood Shores, CA 94065

Telephone: (650) 623-1401

Facsimile: (650) 560-3501

Lead Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE

I hereby certify that this paper complies with the type-volume limitation of 37C.F.R. §42.24 (as determined by the Microsoft Word word-processing system used to prepare this paper) because it contains 13,628 words, excluding the parts of the paper exempted by 37 C.F.R. §42.24(a).

Dated: October 15, 2025

/Matt Berkowitz/

Matthew G. Berkowitz (Reg. No. 57,215)

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6, the undersigned certifies that on October 15, 2025 a copy of the foregoing document, along with any exhibits not previously served, were served by email to counsel for Petitioner:

Adam P. Seitz (Reg. No. 52,206)

adam.seitz@eriseip.com

Mark Lang (Reg. No. 55,356)

Mark.Lang@eriseip.com

Lydia Raw (Reg. No. 76,436)

Lydia.raw@eriseip.com

PTAB@eriseip.com

ERISE IP, P.A.

7015 College Boulevard, Suite 700

Overland Park, Kansas 66211

Telephone: (913) 777-5600

Facsimile: (913) 777-5601

By: /Matt Berkowitz/

Matthew G. Berkowitz (Reg. No. 57,215)