

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. IPR2025-01149
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	3
III. Petitioner's Alleged Prior Art	5
A. <i>Lin</i>	6
B. <i>Smith</i>	7
C. <i>Varadarajan</i>	10
D. Petitioner's Proposed Combinations	14
IV. Level of Ordinary Skill in the Art	15
V. Argument: The Petition Fails to Show a Reasonable Likelihood of Success..	15
A. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination Has A "Device-Specific Static Limited-Use Payment Information" of Limitations 1(e) and 1(h).	15
B. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination Includes a "Dynamically Generat[ed] ... Device-Specific Limited-Use Payment Information" of Limitations 1(f) and 1(h).	26
1. Petitioner Fails to Explain Why <i>Varadarajan</i> 's DCV is "Device-Specific."	26
2. Petitioner and its Expert Fail to Show a Motivation to Combine or Explain Why A POSITA Would Have Selected Only One Particular Type of DCV From The Many Types Disclosed In <i>Varadarajan</i> for its <i>Lin-Smith-Varadarajan</i> Combination.	35
C. Petitioner Fails to Demonstrate that Any of the References in Ground 1 Disclose Limitations 1(g).	46
D. Petitioner Fails to Demonstrate That A POSITA Would Have Been Motivated to Combine The References In Ground 1 To Disclose Limitation 1(h).	48
E. Additional Reasons that Petitioner has Failed to Meet Its Burden.	51
VI. Conclusion	52

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.</i> , 776 F.2d 281 (Fed. Cir. 1985)	38
<i>AT&T Servs., et al. v. Innovative Sonic Limited</i> , IPR2024-01143, Paper 15 (PTAB February 11, 2025)	38, 40, 43, 51
<i>NearMap US, Inc. v. Pictometry Int’l Corp.</i> , IPR2024-00729, Paper 9 (PTAB Oct. 10, 2024)	39, 41
<i>Precision Cancer Techs. Inc. v. Oncoustics Inc.</i> , IPR2025-00242, Paper 7 (PTAB June 3, 2025)	<i>passim</i>
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	46
<i>Upjohn Co. v. Mova Pharm. Corp.</i> , 225 F.3d 1306 (Fed Cir. 2000)	38, 40, 44, 51
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022)	<i>passim</i>

Regulations

37 C.F.R. § 42.6(a)(3)	39
------------------------------	----

PATENT OWNER’S UPDATED 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	DocketNavigator 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	DocketNavigator 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)
[New] 2025	May 10, 2022 Certificate of Correction for U.S. Patent No. 11,176,538

I. INTRODUCTION

On June 24, 2025, Apple Inc. (“Apple” or “Petitioner”) filed a Petition requesting *inter partes review* of claims 1-18 (“Challenged Claims”) of U.S. Patent No. 11,176,538 (“the ’538 Patent”) (EX1001), entirely on multi-reference combination obviousness grounds. Paper 1 (“Petition” or “Pet.”). On July 10, 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 4.

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 for reducing the risk of fraud in connection with completing payment transactions. Petitioner’s arguments regarding **Ground 1**, which challenges independent claim 1 and dependent claims 2-5 and 7-18 of the ’538 Patent, are representative of the Petition’s four main flaws—each of which is dispositive.

First, Petitioner fails to show that its proposed obviousness combination includes a “device-specific static limited-use payment information.” 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.” EX1005, [0029]. Petitioner makes no further obviousness argument based on *Smith* and this limitation. *See* Pet., 19-25.

Second, Petitioner fails to show that its proposed obviousness combination includes a “dynamically generat[ed] device-specific limited-use payment information.” 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., 27 (alteration in original). But *Varadarajan* does not teach that the “device derived identification parameter” is used to generate the DCV, instead, it is separately used as a layer of security to limit access to the DCV generating application (like an authenticator app) that hosts the DCV generator.

Third, because of these first two failures, Petitioner cannot show that its proposed obviousness combination includes “using said limited-use payment information[s] in place of at least a portion of said selected original issuer-supplied payment information for the transaction” or “combining [] said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information,” which refer back to these elements that are missing from its proposed obviousness combination.

Lastly, Petitioner's (and its expert's) obviousness positions, including its alleged motivation to combine and reasonable expectation of success in combining, lack evidentiary support and are belied by the teachings of the prior art themselves.

These same problems exist with the remaining **Ground 2** (challenging dependent claim 6), at least because Petitioner relies on the same combination of references and disclosure as Ground 1 (as relevant to independent claim 1), plus one additional reference, *Kranzley* (addressing only the additional limitations in claim 6). *See* Pet., 64-69.

For these reasons, as those are further explained below, because Petitioner has failed to show a reasonable likelihood of success that any Challenged Claim is unpatentable, Patent Owner respectfully submits that the Board should 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 '538 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 1—the sole challenged independent claim—is illustrative and is directed to a method of performing a payment transaction via a near-field communication (NFC) interface of an electronic device. EX1001, 19:35-20:29 (claim 1). The method involves receiving a request for a transaction payment at an electronic device via an NFC interface. EX1001, 19:46-48. The electronic device then displays the payment request as well as at least a portion of an original account number (such as a traditional credit card number) “for a user selection.” EX1001, 19:49-53. The method then “retriev[es] from a memory [of the electronic device] a device-specific static limited-use payment information, associated with said selected payment method.” EX1001, 19:54-57. In other words, the user makes a “selection” from one of multiple payment methods, and then the claimed method retrieves a device-specific static limited-use number associated with that particular selected payment method. *See* EX1001, 19:54-57.

The method further “dynamically generat[es] ... device-specific limited-use payment information, for said selected method” and combines it with the “static limited-use payment information, to generate a complete device payment information” that is used to complete a payment transaction. EX1001, 19:58-20:29.

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

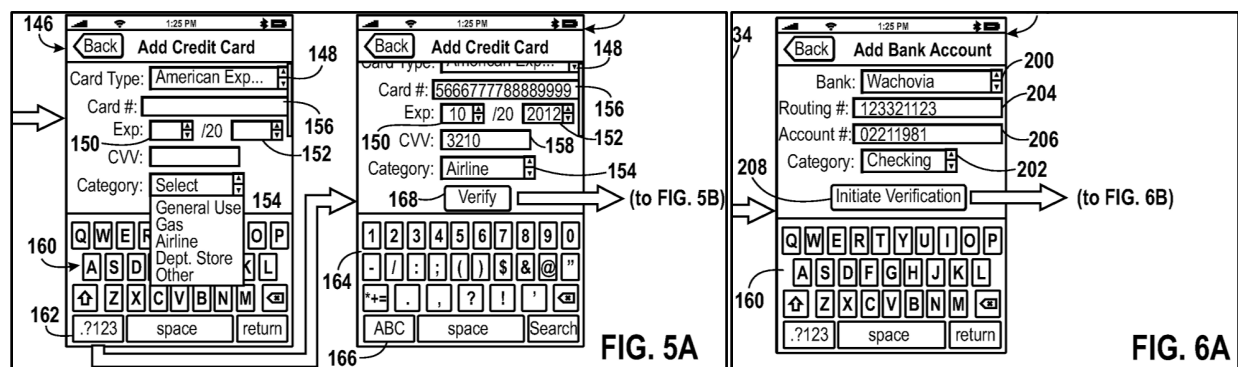
Petitioner relies upon five references in its Grounds (*Lin, Smith, Varadarajan, Hammad, and Kranzley*). In Ground 1, Petitioner presents the combination of *Lin, Smith, Varadarajan, and Hammad* to challenge independent claim 1 and dependent claims 2-5 and 7-18. In Ground 2, Petitioner adds a fifth reference to the combination (*Kranzley*) to challenge dependent claim 6.

Patent Owner provides in this Section III an overview of the select references relevant to demonstrating in this Preliminary Response that Petitioner has failed to show a reasonable likelihood of success that any Challenged Claim is unpatentable. Patent Owner then explains in the following sections how Petitioner’s Grounds using such references fail to demonstrate such a reasonable likelihood of success.

A. *Lin*

International Publication No. WO 2010/039337 (“*Lin*”) is directed to techniques for carrying out peer-to-peer financial transactions (*i.e.*, between consumers) using portable electronic devices. EX1004, Abstract, 1:27-2:20, 3:1-15. *Lin* explains that it is “not uncommon for consumers to hold multiple non-currency accounts concurrently (e.g., multiple credit cards or debit cards corresponding to a respective banking provider)” and for different types of financial exchanges. EX1004, 1:27-2:10. “As the number of payment accounts held by the consumer increases, however, it may become increasingly inconvenient to carry such a large number of credit/debit cards. Further, while payments made using the above-discussed accounts may be readily compatible with retailer and vendor businesses, including those established online on the Internet, payments made from these accounts may not always be readily accepted by other consumers or ‘peers.’” EX1004, 2:14-20. *Lin* explains in reference to Figure 5A and 6A (excerpted below) that a user may manually enter payment information—*e.g.*, credit card or account numbers, expiration date, and CVV—into their mobile device, where it is stored for transmission in transactions. *See* EX1004, FIGs. 5A, 6A, 37:17-20, 38:17-42:2, 43:23-44:23. The credit card provider or bank, as the case may be, verifies the payment information and sends a verification code to the user to confirm the user’s identity. EX1004, FIGs. 5B, 6B, 42:3-43:9, 44:24-45:24. When making a

transaction, the user's device transmits this payment information to the payee's device via an NFC connection. *See* EX1004, FIG. 12A, 59:16-25.



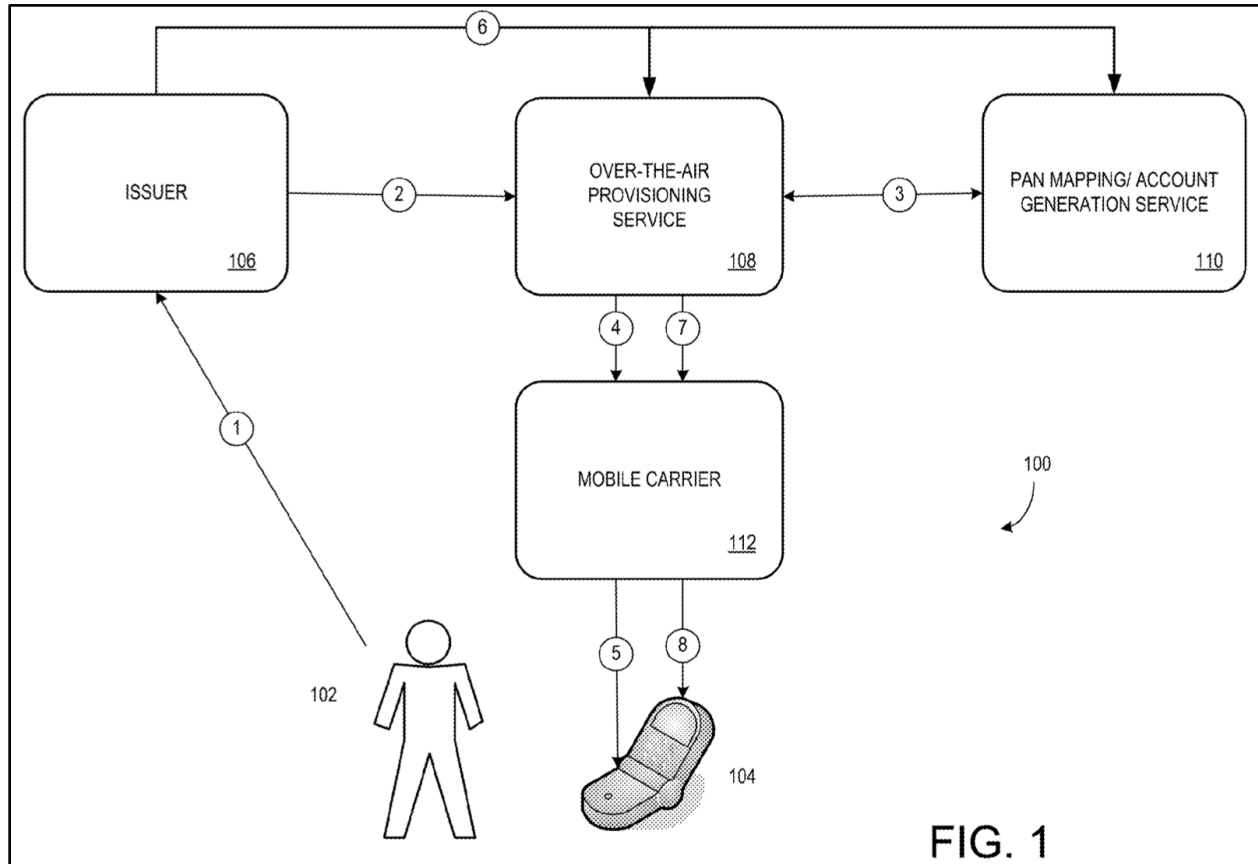
EX1004, FIGs. 5A, 6A (excerpted).

B. *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')." EX1005, [0012]; EX1005, 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." EX1005, [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.” EX1005, [0003].



EX1004, 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:

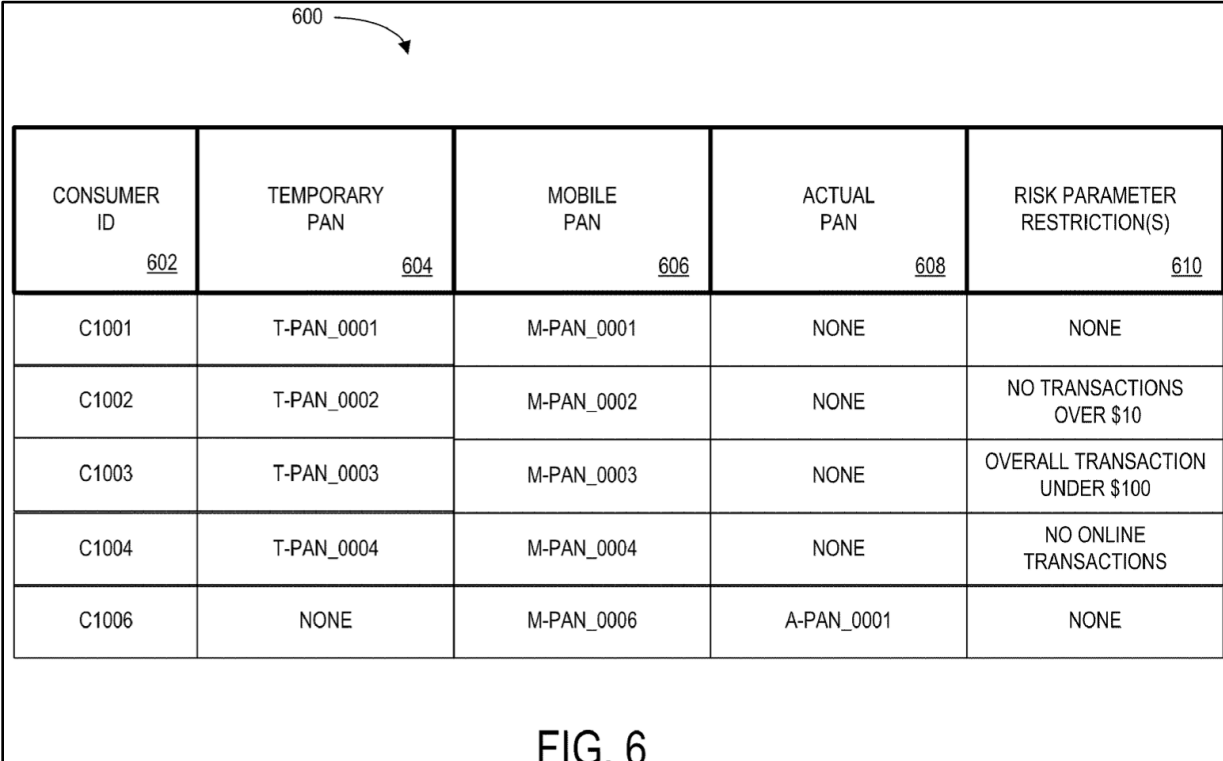
1. Transaction 1: A customer 102 enters account registration data and requests an issuer 106 issue a payment account using their mobile device 104.
2. Transaction 2: The issuer 106 assigns a temporary PAN to the customer's account registration data and transmits the temporary PAN

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 to 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.

EX1005, [0013]-[0019]; *see also* EX1005, 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.” EX1005, [0039].



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

EX1005, FIG. 6.

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; EX1006, [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 “card based transactions,” such as: (1) “skimming” 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; and (4) viruses or screen wipers on a user’s device that record static payment information as it is entered. *See* EX1006, [0003]-[0010].

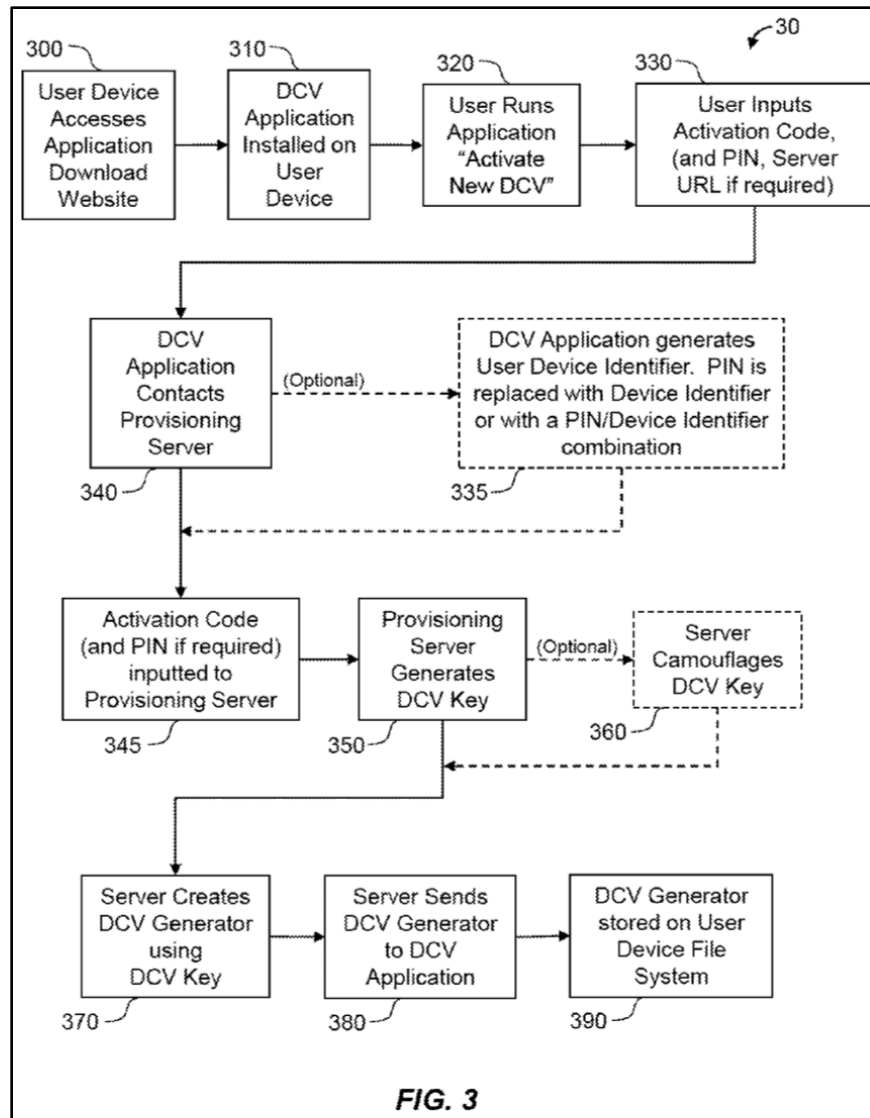
Varadarajan explains, in reference to Figure 3 below, the process of preparing a user’s mobile device to generate a DCV as follows.

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 for storage.

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 is “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. Petitioner’s Proposed Combinations

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

Relevant to this Preliminary Response, and as further discussed below, as best that Patent Owner can discern, Petitioner proposes that *Lin* is the primary reference, including its mobile device and associated mobile wallet, to which a user can store multiple payment vehicles. Petitioner then proposes that it would have been obvious to “store Smith’s PPAN in place of Lin’s payment account number,” Pet., 23-25. From there, Petitioner further proposes that a POSITA would add to the *Lin-Smith* combination the DCV of *Varadarajan*: “[I]t would have been obvious to configure the processor of the Lin-Smith electronic device to dynamically generate a DCV to be used in place of a CVV.” Pet., 27-29.

IV. 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.

V. ARGUMENT: THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD OF SUCCESS

A. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination Has A “Device-Specific Static Limited-Use Payment Information” of Limitations 1(e) and 1(h).

Both Grounds in the Petition fail because Petitioner fails to show that its proposed obviousness combination includes a “device-specific static limited-use payment information” as required by the following limitations in independent claim 1 of the ’538 Patent:

1. 1(e), requiring “retrieving from a memory attached to a processor of the device, *a device-specific static limited-use payment information*, associated with said selected payment method; and,”
2. 1(h), requiring “combining of said dynamically-generated limited-use payment information with *said static limited-use payment information*, to generate a complete device payment information[.]”

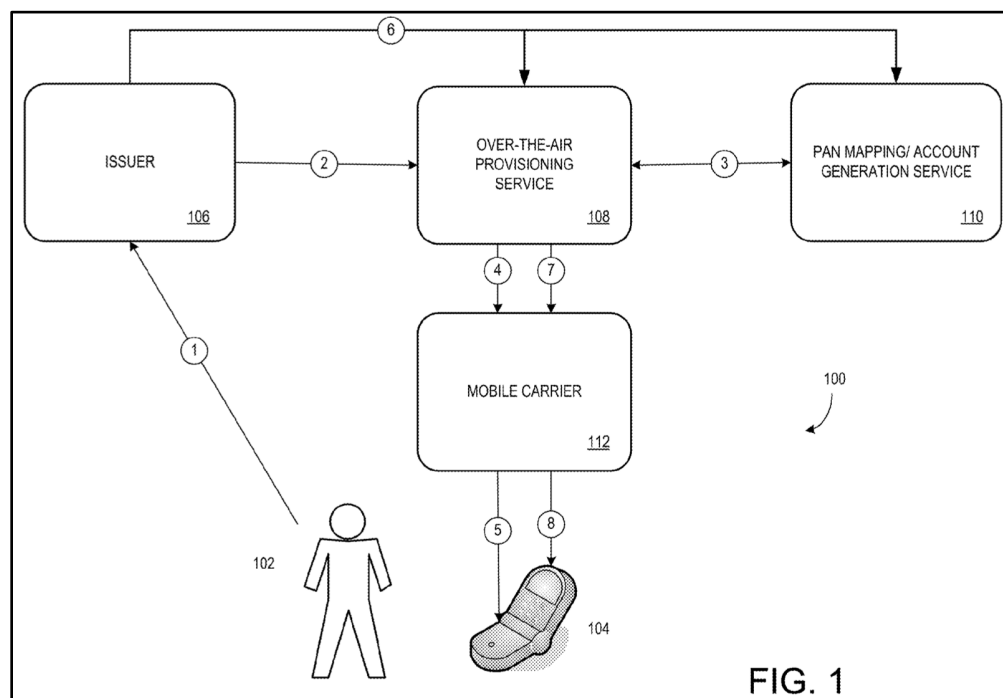
EX1001, 19:54-57, 19:64-67 (emphases added).

Petitioner relies solely on *Smith* as allegedly disclosing the claimed “device-specific static limited-use payment information.” Pet., 19-23, 30. In particular, Petitioner asserts that the “PPAN” of *Smith* is the “device-specific static limited-use payment information.” See Pet., 21, 30 (“The PPAN is, therefore, a *device-specific payment information*.” (emphasis in original)); EX1003 ¶125 (same); see also Pet., 23 (“A POSITA would have found it obvious and been motivated to store Smith’s PPAN in place of Lin’s payment account number.”); EX1003 ¶130 (same). Petitioner’s assertion is incorrect. *Smith* never once says that the PPAN is a “device-specific static limited-use payment information” or is limited to (or even based on) a particular device in any way. Rather, the PPAN is account-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. EX1005, [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.B, 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.” EX1005, [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’).” EX1005, [0012]. Once the issuer systems have updated, the actual PAN is used instead of the temporary one. EX1005, [0012].



EX1005, 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.” EX1005, [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. EX1005, [0014]. Importantly, there is no disclosure that the user ever provides a device ID during this registration process. *See* EX1005, [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* EX1005, [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* EX1005, [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. EX1005, [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

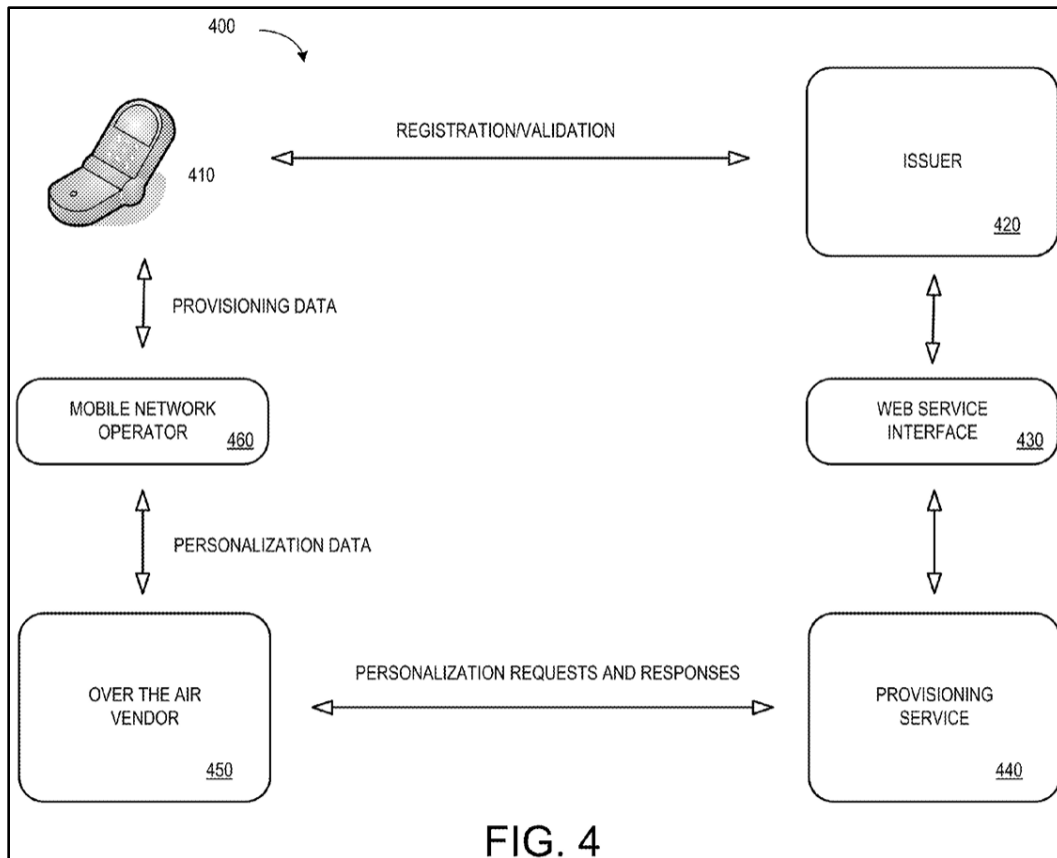
service 110 so that a PayPass PAN (or ‘PPAN’) may be assigned to the mobile device 104. EX1010, [0016]; Pet., 21. The PAN mapping/account generation service 110 assigns a PPAN to the device 104, and also maps the newly-assigned PPAN to the temporary PAN provided by the issuer 106.” EX1005, [0016]. These two sentences in *Smith* effectively form the basis for the entirety of Petitioner’s argument that the PPAN is a “device-specific static limited-use payment information.” See Pet., 21 (citing EX1005, [0016]). 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., 6-7, 19-25.

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 104.” EX1005, [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.” EX1005, [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.” EX1005, [0016]. 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.” EX1005, [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. EX1005, [0018]. This is described in further detail with respect to Figure 4 of *Smith* (below) and related disclosure. EX1005, 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. EX1005, [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.” EX1005, [0029]. Importantly, *Smith* indicates that “multiple NFC-enabled handsets may be managed for a single account.” EX1005, [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.



EX1005, 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. EX1005, [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.” EX1005, [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				

EX1005, 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* EX1005, [0039]. The PPAN is a type of Mobile PAN. EX1005, [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.” EX1005, [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. EX1005, [0013] (“a primary *account* number (or ‘PAN’)”), [0023] (“the payment network 218 *identifies the PPAN and requests a*

lookup 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. EX1006, [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 with the issuer systems at the time of issuance.”) (emphasis added); *see also, e.g.*, EX1005, [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. EX1005, [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* EX1005, [0041] (disclosing that the provisioning service may “disable the payment application on the mobile phone (without [*sic*: with] or without removing the personalization details)”); EX1005, [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* EX1005, [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 device-specific static limited-use payment information. Pet., 19-23. 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,” EX1005, [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. EX1005, 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). EX1005, [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 EX1005, [0028].

Accordingly, Petitioner has failed to meet its burden to show that *Smith* discloses a “*device-specific* static limited-use payment information” as required by limitation 1(e) and 1(h). This is dispositive of both of Petitioner’s Grounds and demonstrates that Petitioner has not shown a reasonable likelihood of success that any Challenged Claim is unpatentable. However, for completeness, Patent Owner notes that *Lin* also fails to disclose a “*device-specific* static limited-use payment information”—nor does Petitioner so argue. See Pet., 19-20. *Lin* uses actual issued payment information in transactions, which is not “device-specific,” and which further would fail to meet at least limitation 1(g) requiring use of limited-use payment information, “in place of at least a portion of said selected original issuer-supplied payment information for the transaction.” See *supra* Section III.A.

For at least the foregoing reasons, Petitioner fails to meet its burden of showing that its proposed combination has “*device-specific* static limited-use payment information” as required in limitations 1(e) and 1(h).

B. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination Includes a “Dynamically Generat[ed] ... Device-Specific Limited-Use Payment Information” of Limitations 1(f) and 1(h).

Both Grounds of the Petition fail for an additional dispositive reason because Petitioner fails to show that its proposed obviousness combinations disclose a “dynamically generate[d] ... device-specific limited-use payment information” as required by the following limitations:

1. 1(f), requiring “*dynamically generating*, by a processor of the device, *device-specific limited-use payment information*, for said selected payment method; and,”
2. 1(h), requiring “combining of *said dynamically-generated limited-use payment information* with said static limited-use payment information, to generate a complete device payment information[.]”

EX1001, 19:58-60, 19:64-67 (emphases added).

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

Petitioner asserts that “[i]t would have been obvious to modify Lin-Smiths [sic] to *dynamically generat[e]*, by a processor of the device, *device-specific limited-use payment information*, for said selected payment method in view of *Varadarajan*.” Pet., 25 (alteration and emphasis in original). More particularly, and relevant here, Petitioner asserts that the “DCV” of *Varadarajan* is the claimed “dynamically-

generat[ed] ... device-specific limited-use payment information.” *See* Pet., 27; EX1003 ¶139 (same). Petitioner’s sole basis for asserting that the DCV is device specific consists of a single conclusory sentence: “Varadarajan teaches, and a POSITA would understand, the DCV is also device-specific because the DCV generator uses ‘a device derived identification parameter ... which is unique to the user device or machine used to host the DCV generating application’ such that ‘the included device identifier is unique to each user device ... [and] each transaction and DCV is further identifiable to the user device conducting a transaction or requesting a DCV.’” Pet., 27 (alterations and emphasis in original and citing EX1006, [0029], [0053], [0043], [0049], [0054]). Its expert includes the same conclusory sentence—verbatim with the *same* emphasis and alterations and *without* any additional explanation or analysis. EX1003 ¶139. 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 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.”); *see also Xerox*, IPR2022-00624, Paper 9, 15-17.

Indeed, not only does Petitioner's (and its expert's) assertion fail to show that the DCV is device-specific, but it is also an oversimplification and mischaracterization of *Varadarajan*'s actual disclosure. The "device derived identification parameter" in *Varadarajan* 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, in turn, generates the DCV.

To begin, Petitioner cherry-picks portions of sentences from separate disclosures in *Varadarajan* (at paragraphs [0029] and [0053]). Pet., 27. When read in full, they do not support the conclusion that Petitioner proffers. The below shows material omitted by Petitioner (with underline), and includes bolding and italics 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 (iPhoneTM, BlackberryTM, 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

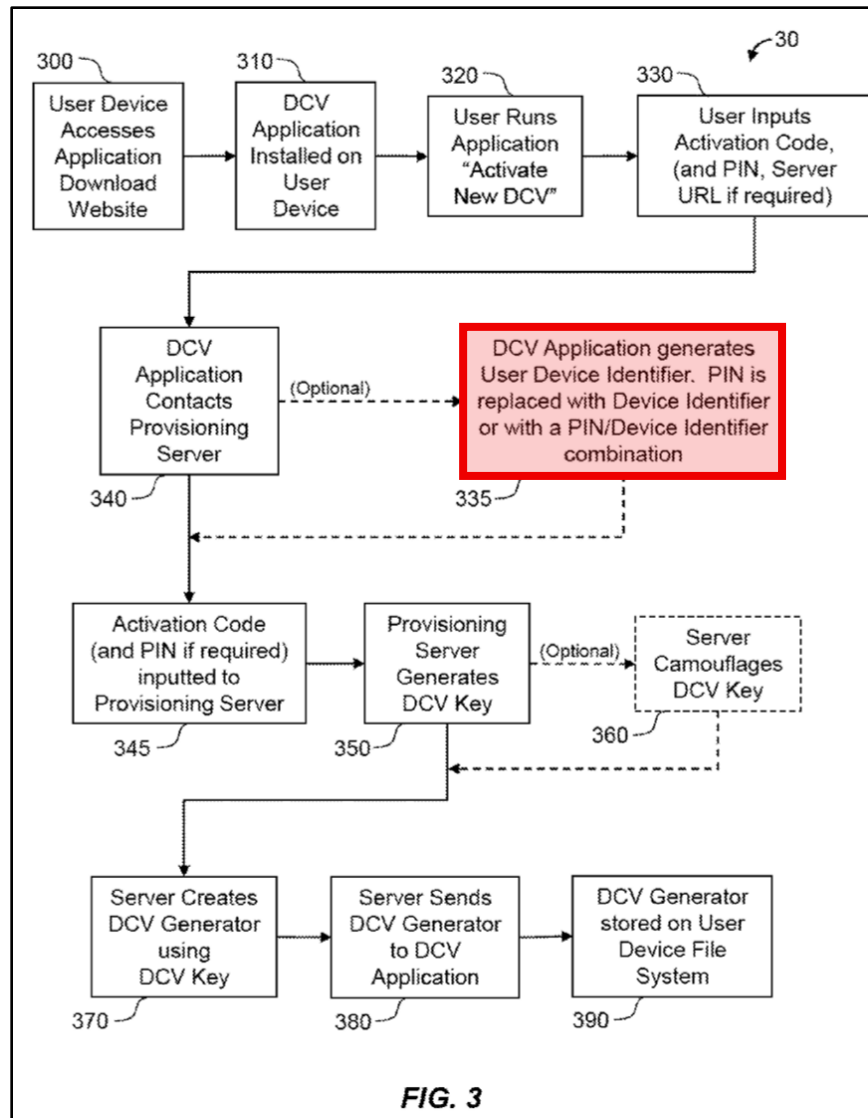
incorrect DCV inputs during a DCV request sequence, resetting the DCV generator can be expedited through a support telephone call and reset of the DCV application on the user device, which can, if necessary, include providing a new DCV key and providing a new DCV generator.

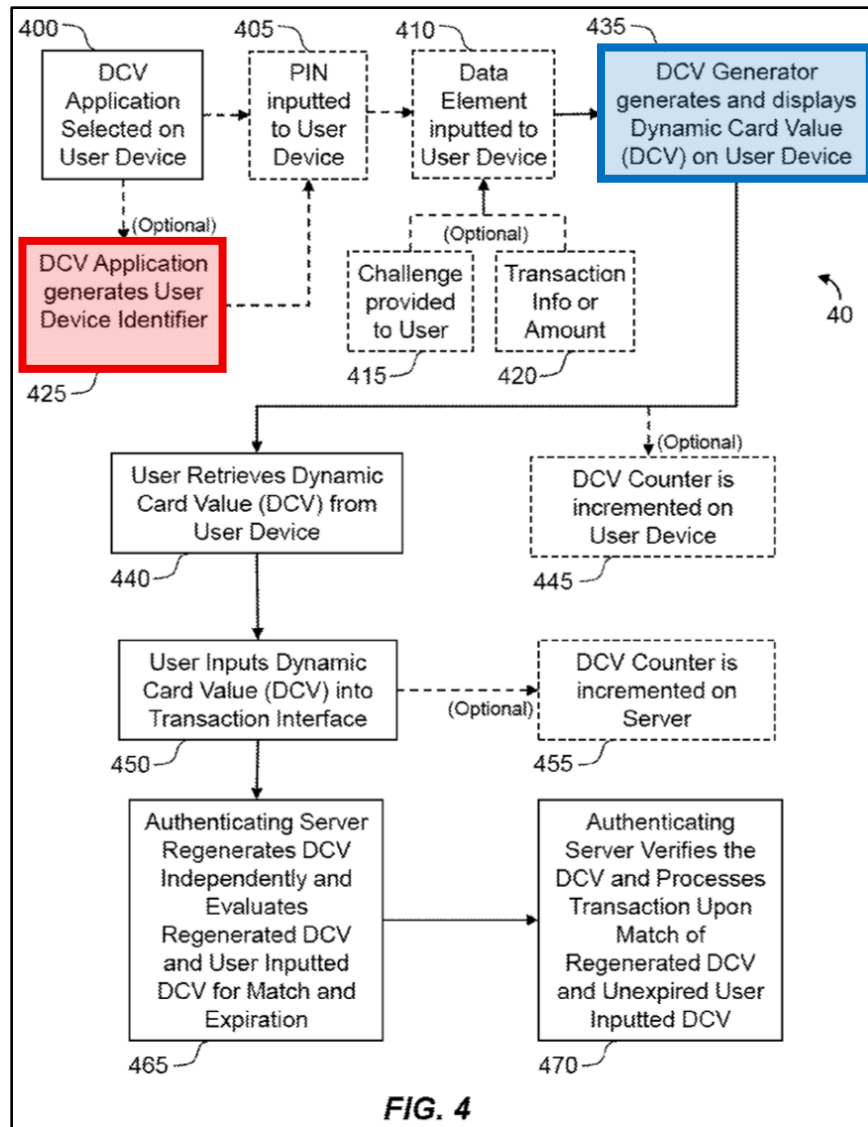
EX1006, [0053].

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, 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.” The device derived identification parameter is not disclosed as an input to the DCV; it is entirely separate.

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, [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]; *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 “dynamically generat[ed] ... *device-specific* limited-use payment information” as required by limitations 1(f) and 1(h), which is likewise dispositive of both Grounds. However, for completeness, Patent Owner notes that *Lin* and *Smith* also fail to disclose a “dynamically generat[ed] ... *device-specific* limited-use payment information”—nor does Petitioner so argue. *See* Pet., 25-27. *Lin* uses actual issued payment information in transactions which is not “dynamically generated” or “device-specific,” and which further would fail to meet at least limitation 1(g)

requiring use of limited-use payment information, “in place of at least a portion of said selected original issuer-supplied payment information for the transaction.” *See supra* Section III.A. *Smith* uses provisioned static payment information which is not “dynamically generated” or “device-specific.” *See supra* Sections III.B, V.A.

2. Petitioner and its Expert Fail to Show a Motivation to Combine or Explain Why A POSITA Would Have Selected Only One Particular Type of DCV From The Many Types Disclosed In *Varadarajan* for its *Lin-Smith-Varadarajan* Combination.

Petitioner argues that it would have been obvious to combine *Lin*, *Smith*, and *Varadarajan*. Pet., 23-25, 27-29. Not so. As discussed below, it would not have been obvious for a POSITA to add the teachings of *Smith* and *Varadarajan* to *Lin*. First, Petitioner fails to explain why a POSITA would have been motivated to combine *Lin* and *Smith*, when neither are directed to payment transaction security. Second, Petitioner’s assertions about alleged motivation to combine and reasonable expectation of success in combining *Lin* with *Smith*, and then the *Lin-Smith* combination with *Varadarajan* are often conclusory and rely only on its expert’s unsupported and conclusory testimony. Finally, Petitioner does not explain why a POSITA would choose to replace specifically the CVV of the *Lin-Smith* combination with a DCV, out of the many different types of DCV’s disclosed in *Varadarajan*.

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

First, *Lin* and *Smith* are not directed to payment transaction security at all. *See generally* EX1004; EX1005. *Lin* is directed to resolving the inconvenience to consumers of carrying a large number of credit and debit cards and to facilitating peer-to-peer transactions. *See supra* Section III.A; EX1004, 1:27-2:20. *Smith* is directed to minimizing the amount of time a consumer must wait between applying for a payment account and using such account to complete a transaction using its PPAN. *See supra* Section III.B; EX1005, [0002]-[0003]. Petitioner and its expert assert that a POSITA “would have appreciated that storing a PPAN would be safer than storing the actual number on *Lin*’s device.” Pet., 23; EX1003 ¶130. But there is no evidence of this. *Smith* does not explain what a PPAN is aside from a Mastercard-specific idea, and never explains whether it is more or less secure than anything else (e.g., whether it is just as susceptible to fraud as a PAN). Nor does Petitioner’s expert explain this—he simply assumes that it is true.

Moreover, neither Petitioner nor its expert address why a POSITA would have been motivated to include *Lin* and *Smith* in a combination when neither of these references have anything at all to do with payment security, especially when *Smith* does not disclose any relationship between the PPAN and security. *See generally* Pet. Further, *Lin* and *Smith* both describe complete systems with existing measures to prevent unauthorized access to customers’ payment information. *See, e.g.*, EX1004, 26:27-28:15 (describing security features of the disclosed system, *e.g.*,

“cryptographic protocols, such as a secure sockets layer (SSL) or a transport layer security (TLS) protocol, for establishing *secure communications* between the device 10 and an external device,” “secure access-restricted storage area,” features to “allow a user to lock or temporarily disable (*e.g.*, lock on power-up),” and “requiring that the PIN be provided prior to the sending or transmissions of payment account information to external devices” (emphasis added)); EX1005, [0015], [0029], [0032]-[0033] (disclosing use of “a secure web service or other data protocol, such as a Simple Object Access Protocol (‘SOAP’) service,” a “secure element,” and “an encryption key for security purposes”). Petitioner and its expert do not address why the combination of *Lin* and *Smith* would be necessary given the security measures already implemented in their systems. *See generally* Pet. Moreover, *Smith* is also an already-complete solution that depends upon a *Smith*-specific PPAN-mapping and account-generation service and over-the-air vendor. *See supra* Section III.B.

Second, Petitioner makes several conclusory assertions about alleged motivation to combine and reasonable expectation of success in combining the multiple references across its two Grounds. Its expert repeats, often verbatim without any additional analysis or support, the Petition’s conclusory assertions.

Patent Owner provides a few examples below (regarding the sole challenged independent claim 1), which are likewise dispositive of Petitioner’s Grounds.

For the *Lin-Smith* combination, Petitioner asserts that a POSITA “would have found it obvious and been motivated to store Smith’s PPAN in place of Lin’s payment account number” and “would have appreciated that storing a PPAN would be safer than storing the actual account number on Lin’s device,” Pet., 23, but Petitioner relies *solely* on its expert declaration to support this assertion, which largely repeats the same language as the corresponding passages of the Petition without *any* evidence or analysis. *Compare* Pet., 23 *with* EX1003 ¶130. Such unsupported, conclusory testimony should be afforded little, if any, weight. *See, e.g., Precision Cancer*, IPR2025-00242, Paper 7, 15-16; *AT&T Servs., et al. v. Innovative Sonic Limited*, IPR2024-01143, Paper 15, 27-28, 38 (PTAB Feb. 11, 2025); *Xerox*, IPR2022-00624, Paper 9, 15-17; *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)).

The sole analysis that Petitioner’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 only have access 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,” citing U.S. Patent App. Pub. No. 2011/0140841 (“*Bona*”) (EX1043). *See* EX1003 ¶130. Neither *Lin* nor *Smith* describe cancelling a PPAN. *See generally* EX1004, EX1005. And Petitioner’s citation to its expert’s discussion of *Bona* does not support these assertions.¹ *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]. Finally, *Bona* at [0014] states: “Fig. 1 is

¹ To the extent Petitioner relies on citations to its expert’s declaration to supply arguments missing from the Petition (about references also missing from the petition), such reliance is also improper. *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 block diagram of a smart card application management system.” EX1043, [0014]. Petitioner’s expert does not explain how any of these paragraphs relate to PPAN(s), “removing account numbers from a user device,” or cancelling a device’s compromised PPANs, let alone “a device-specific static limited-use payment information, associated with said selected payment method” as claimed in limitation 1(e) of claim 1 of the ’538 Patent. *See* EX1003 ¶130. For the same reasons as above, such unsupported, conclusory testimony should be afforded little, if any, weight.

Petitioner then adds *Varadarajan* to the *Lin-Smith* combination, asserting that “a POSITA would have been motivated to configure the Lin-Smith processor to implement Varadarajan’s method of dynamically generating a DCV to be used in place of the selected payment method’s CVV to improve similar mobile payment systems in the same way.” Pet., 28. But, Petitioner again relies *solely* on its expert declaration to support this assertion, which repeats the same language as the corresponding passages of the Petition without *any* evidence or analysis. *Compare* Pet., 28 *with* EX1003 ¶141. Such unsupported, conclusory testimony should be afforded little, if any, weight. *See, e.g., 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.

Petitioner next asserts that “[t]he concept of dynamic CVVs was well-known at this time and a POSITA would have been familiar with using [dynamic CVVs] in

connection with mobile payment transactions” and that “[t]he substitution of Varadarajan’s DCV with Lin-Smith’s CVV with Varadarajan’s DCV [*sic*] is a substitution of one known element for another and a POSITA would have understood that the substitution would have predictably increased the security of Lin-Smith’s payment system and further protected the user’s sensitive account information,” relying, again, on its expert declaration. Pet., 28 (citing EX1003 ¶142). Petitioner’s expert repeats these assertions *verbatim* and, purportedly in support of these statements, describes references disclosing “us[e] [of] dynamic verification values ... in place of static CVVs” in payment transactions. *See* EX1003 ¶142 (citing “Section VI.C.2”,² EX1043, EX1033, EX1007). Beyond being an improper incorporation by reference—Petitioner never cites or discusses the underlying references in the Petition³—each of the cited references discloses a *complete*

² Section VI.C.2, as cited in paragraph 142 of the expert declaration, does not exist. *See* EX1003. Patent Owner will assume, for purposes of this Preliminary Response, that Petitioner’s expert intended to cite to Section VII.B.2, which briefly discusses U.S. Patent App. Pub. No. 2008/00110983 (“*Ashfield*”), *Bona*, and U.S. Patent App. Pub. No. 2013/0054474 (“*Yeager*”). *See* EX1003 ¶¶84-88 (citing EX1033, EX1043, EX1029).

³ *See NearMap*, IPR2024-00729, Paper 9, 21-22.

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 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 FIG. 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.”).

In addition to the issues with the *Lin-Smith* combination discussed above, Petitioner’s expert also does not explain why a POSITA would have been motivated

to “substitut[e] Lin-Smith’s CVV with Varadarajan’s DCV” or provide factual support for the same, especially when the Petitioner’s *Lin-Smith* combination *already uses* a PPAN instead of actual, issued credit card numbers. *See* EX1003 ¶142. As explained above, *Smith*’s PPAN is first mapped to a temporary PAN in response to a customer’s request for a payment account to facilitate the customer’s quick use of their new account to make payments and then to the actual PAN after it is issued. *See supra* Section III.B, V.A.

Moreover, if “[t]he concept of dynamic CVVs was well known at this time” as an obvious and useful substitute for its CVV, then *Lin* would have included them. *See* Pet., 28; EX1003 ¶142. That *Lin*, itself a 164-page and 78-figure reference, does not include dynamic CVVs demonstrates that replacing the *Lin-Smith* CVV with *Varadarajan*’s DCV is not as clearly obvious as Petitioner claims.

Petitioner further asserts that the results of its *Lin-Smith-Varadarajan* combination would have been predictable and that a POSITA would have had a reasonable expectation of success in modifying the *Lin-Smith* combination with the *Varadarajan* DCV, but Petitioner relies solely on its expert declaration to support this assertion, which, again, largely repeats the same language as the corresponding passages of the Petition without any factual support. *See* Pet., 28-29; EX1003 ¶¶143-144. And again, such unsupported, conclusory testimony should be afforded little, if any, weight *See Precision Cancer*, IPR2025-00242, Paper 7, 15-16; *AT&T*,

IPR2024-01143, Paper 15, 27, 38; *Xerox*, IPR2022-00624, Paper 9, 15-17; *Upjohn*, 225 F.3d at 1311.

For example, Petitioner and its expert assert that “because the PPAN is still being used in place of the PAN, the Lin-Smith-Varadarajan device would still retain the benefits of allowing the user to easily cancel PPANs.” *See* Pet., 28-29; EX1003 ¶143. But they cite nothing to support this statement. None of *Lin*, *Smith*, or *Varadarajan* describe cancelling a PPAN. *See generally* EX1004, EX1005, EX1006. Petitioner’s expert generally references his earlier opinions, but as discussed above *Bona*—which the Petition never discusses or cites—does not support the expert’s assertions regarding PPAN cancellation. *See* EX1003 ¶130 (citing EX1043, [0007], [0014], [0074], FIG. 6); EX1043, [0068], [0074], FIG. 6 (describing 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), [0007] (describing 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), [0014] (“Fig. 1 is a block diagram of a smart card application management system.”). Petitioner’s expert does not explain how any of these paragraphs relate to PPAN(s), “removing account numbers from a user device,” or cancelling a device’s

compromised PPANs, let alone “a device-specific static limited-use payment information, associated with said selected payment method” as claimed in claim 1(e). *See* EX1003 ¶130. Again, such unsupported, conclusory testimony should be afforded little, if any, weight.

Third, Petitioner also does not explain why a POSITA would have chosen to replace **only** *Lin*’s CVV with *Varadarajan*’s DCV. *See* Pet., 27-29. Petitioner argues that “a POSITA would have understood that the Lin-Smith electronic device would still be vulnerable to attacks where the PPAN and CVV values are intercepted by an attacker and used for fraudulent transactions, as taught by Varadarajan,” and “would have been motivated to configure the Lin-Smith processor to implement Varadarajan’s method of dynamically generating a DCV to be used in place of the selected payment method’s CVV to improve similar mobile payment systems in the same way” Pet., 28. Petitioner does not explain why a POSITA would still choose to use the *Lin-Smith* combination in light of this known security vulnerability. *See* Pet., 28-29.

Indeed, *Varadarajan* discloses that its claimed system “may provide more than one type of DCV, for example, *both a dynamic PAN and a dynamic CVV may be generated for use in the same transaction.*” EX1006, [0012]-[0013], [0021]-[0022] (emphasis added). Petitioner does not explain why a POSITA, concerned about an attacker intercepting *Smith*’s PPAN and *Lin*’s CVV of the *Lin-Smith* portion

of the proposed combination, would not simply replace **both** *Lin*’s PAN and CVV with *Varadarajan*’s dynamic PAN and dynamic CVV, respectively, thus rendering *Smith*’s PPAN superfluous. This shows that the three-reference, *Lin-Smith-Varadarajan* combination is the product of impermissible hindsight and should be rejected. *See, e.g., TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1361 (Fed. Cir. 2019) (“We repeatedly expressed concerns that crediting such testimony risks allowing the challenger to use the challenged patent as a roadmap to reconstruct the claimed invention using disparate elements from the prior art—i.e., the impermissible *ex post* reasoning and hindsight bias that *KSR* warned against.”).

This is yet another reason Petitioner has not met its burden regarding limitation 1(f) (which failure is also dispositive of both of Petitioner’s Grounds).

C. Petitioner Fails to Demonstrate that Any of the References in Ground 1 Disclose Limitations 1(g).

Limitation 1(g)—as corrected by the May 10, 2022 certificate of correction—requires “using said limited-use payment information[s] in place of at least a portion of said selected original issuer-supplied payment information for the transaction.” Pet., 29-30; EX1001, 19:61-63; EX2025. “Said limited-use payment information[s]” refers back to the “device-specific static limited-use payment information” from limitation 1(e) and the “dynamically generat[ed]...device-specific limited-use payment information” from limitation 1(f). *See* Pet., 19, 25; Ex. 1001, 19:55-60.

For this limitation Petitioner identifies only the “use [of] Varadarajan’s DCV ... in place of the selected payment method’s CVV values.[.]” Pet., 30 (citing limitation 1(f); EX1003 ¶145). However, Petitioner only asserts that *Varadarajan*’s DCV is the “dynamically generat[ed] ... device-specific limited-use payment information” of limitation 1(f). Thus, Petitioner has not identified any “device-specific static limited-use payment information” that is used in place of “original issuer-supplied payment information” as required by limitation 1(g). *See* Pet., 29-30.

Even if Petitioner were to belatedly (and improperly) seek to correct its Petition to identify *Smith*’s PPAN as the “device-specific static limited-use payment information” as it did for limitation 1(e), as discussed above, *Smith*’s PPAN is not “device-specific” as required by limitation 1(e) and also cannot satisfy the same requirement of limitation 1(g). Similarly, as discussed above, *Varadarajan*’s DCV is also not “device-specific” as required by limitation 1(f) and cannot satisfy the same requirement of limitation 1(g).

Accordingly, Petitioner has failed to meet its burden to show that its cited references render obvious limitation 1(g) (which failure is also dispositive of both of Petitioner’s Grounds).

D. Petitioner Fails to Demonstrate That A POSITA Would Have Been Motivated to Combine The References In Ground 1 To Disclose Limitation 1(h).

Limitation 1(h)—as corrected by the May 10, 2022 certificate of correction⁴—requires “combining [] said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information[.]” Pet., 30; Ex. 1001, 19:64-67. “[S]aid static limited-use payment information” refers back to the “device-specific static limited-use payment information” from limitation 1(e) and “said dynamically-generated limited-use payment information” refers back to the “dynamically generat[ed]...device-specific limited-use payment information” from limitation 1(f). See Pet., 19, 25, 30; Ex. 1001, 19:54-60, 19:64-67.

Petitioner asserts that “it would have been obvious to further configure Lin’s electronic device to combine the PPAN and DCV as a substitute for the card number and CVV to form complete device payment information.” Pet., 30 (emphasis in original). As explained above in reference to limitations 1(e) and 1(f), neither *Smith*’s PPAN nor *Varadarajan*’s DCV are device-based. See *supra* Section V.A, B. Accordingly, Petitioner has also failed to meet its burden to show that its cited references render obvious limitation 1(h).

⁴ EX2025.

Petitioner also does not identify any motivation to combine specific to limitation 1(h), instead referring back to its assertions regarding limitations 1(e) and 1(f) and to its expert’s declaration. *See* Pet., 30 (citing “Claims 1(e)-(f); Dec., ¶146”). However, Petitioner’s assertions with respect to the motivation to combine to replace *Lin*’s PAN with *Smith*’s PPAN for limitation 1(e) and to replace *Lin*’s CVV with *Varadarajan*’s DCV for limitation 1(f) do not explain why a POSITA would have been motivated to combine together a static limited-use payment information (*i.e.*, *Smith*’s PPAN) and a dynamically generated limited-use payment information (*i.e.*, *Varadarajan*’s DCV) to generate a complete payment information. *See* Pet., 30; *see also supra* Section V.B.2.

Neither *Lin* nor *Smith* address payment transaction security at all—let alone the use of a combination of static and dynamic payment information. *Lin*’s disclosure is directed to addressing the inconvenience of carrying a large number of credit and debit cards and to facilitating peer-to-peer transactions, while *Smith*’s disclosure is directed to minimizing the amount of time a consumer must wait between applying for a payment account and using such account to complete a transaction. *See supra* Sections III.A-B, V.B.2; EX1004, 1:27-2:20; EX1005, [0002]-[0003].

Varadarajan only discloses addressing security vulnerabilities associated with card-based transactions by replacing issued payment information with

dynamically-generated information. *See supra* Sections III.C, V.B.2. Thus, *Varadarajan* discloses that the DCV can be configured to be “a CVC, CVV, CSC, PAN, account number, partial PAN and a portion of an account number” and that its claimed system “may provide more than one type of DCV, for example, *both a dynamic PAN and a dynamic CVV* may be generated for use in the same transaction.” *See* Pet., 26-29; EX1006, [0012]-[0013], [0021]-[0022] (emphasis added). Petitioner does not explain why a POSITA would have selected to use the DCV to replace only *Lin*’s CVV. Nor does Petitioner explain why, if a POSITA was concerned about an attacker intercepting *Lin*’s static PAN *and* CVV for later reuse, the POSITA would not choose to replace both with *Varadarajan*’s dynamic PAN and dynamic CVV, thus rendering *Smith*’s PPAN superfluous. Indeed, *Varadarajan* teaches away from, and expressly discourages, the use of static payment data. *See* EX1006, [0009] (“The static nature of the magstripe data on a credit or debit card and the use of a static PAN and CVV may aggravate the problem of fraud prevention. If an attacker obtains the static card data, including the PAN and/or CVV, the attacker can readily use the card to complete transactions without detection”).

Petitioner’s expert merely repeats Petitioner’s assertions verbatim. *Compare* Pet., 30 *with* EX1003 ¶146. And again, 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.

Accordingly, Petitioner has failed to meet its burden to show that its cited references render obvious limitation 1(h) which failure is also dispositive of both of Petitioner's Grounds).

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

Patent Owner has focused on four 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, including the following:

- *Smith* is incompatible with a multi-network and multi-issuer payment system. It provides 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.B. In contrast, *Lin* at Figures 5A and 6A shows that its payment application can accommodate multiple payment networks and banks. *See supra* Section III.A.

- Limitations 1(g) and 1(h) require using two separate pieces of replacement information—a device-specific static limited-use payment information and a dynamically generated device-specific limited-use payment information. This is different than each of *Lin*, *Smith*, and *Varadarajan*. *Lin* does not use replacement information at all, but actual issued payment information, *Smith* uses a single piece of static replacement information, and *Varadarajan* uses one or multiple pieces of dynamically generated replacement information. *See supra* Section III.A-C. Petitioner never addresses a reason why a POSITA would use specifically one piece of static replacement information with one piece of dynamically generated replacement information, or the complexities associated with doing so.

VI. 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 10, 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 10,236 words, excluding the parts of the paper exempted by 37 C.F.R. §42.24(a).

Dated: October 10, 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 10, 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)