

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CARDWARE INC.,
Patent Owner.

IPR2025-01145
Patent 10,339,520

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION.....	1
II. THE '520 PATENT CLAIMS	5
III. PETITIONER’S ALLEGED PRIOR ART	7
A. Toomer.....	7
B. Grigg.....	11
C. Hammad.....	18
D. Petitioner’s Proposed Combination.....	20
IV. CLAIM CONSTRUCTION	21
A. Static Device Account Number	21
B. Petitioner Omits its Contradictory District-Court Indefiniteness Arguments that the Claim-Scope Allegedly Cannot be Ascertained	22
V. LEVEL OF ORDINARY SKILL IN THE ART	24
VI. ARGUMENT	24
A. Petitioner Fails to Meet its Burden of Showing that its Proposed Combination has a “Static Device Account Number” as Required by Limitations 10(d) and 10(g).....	24
1. Petitioner Fails to Explain Why the Mobile Wallet Account Number of Grigg is a “Device” Number	24
2. None of the Mobile Wallet Account Number Permutations in Grigg is “Device” Number.....	25
3. Petitioner Does Not Explain Why a POSITA Would Have Selected the One Particular Permutation of Mobile Wallet Account Number from Grigg (out of a Dozen) that it Relies Upon in its Obviousness Combination.....	31

B.	Petitioner Fails to Demonstrate that a Person of Ordinary Skill in the Art Would Use the dCVV of Hammad with the Mobile Wallet Account Number of Grigg (in connection with limitation 10(g)).....	34
C.	Petitioner’s Grounds Regarding Claim 1 and its Dependent Claims Fail for the Same Reasons as Claim 10.....	42
D.	Additional Reasons that Petitioner Has Failed to Meet Its Burden	43
VII.	CONCLUSION	44

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>AT&T Servs., et al. v. Innovative Sonic Limited</i> , IPR2024-01143, Paper 15 (PTAB Feb. 11, 2025).....	38
<i>CardWare Inc. v. Samsung Elecs. Co. Ltd.</i> , Case No. 2:22-CV-141-JRG-RSP, 2023 WL 5434763 (E.D. Tex. Aug 22, 2023)	4, 23
<i>Ecolochem, Inc. v. S. Cal. Edison Co.</i> , 227 F.3d 1361 (Fed. Cir. 2000)	41
<i>InTouch Techs., Inc. v. VGo Commc'ns, Inc.</i> , 751 F.3d 1327 (Fed. Cir. 2014)	40
<i>KSR Int'l Co. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007).....	41
<i>Microchip Tech. Inc. v. Aptiv Techs. AG</i> , IPR2024-00558, Paper 12 (PTAB Oct. 7, 2024).....	23
<i>Novo Nordisk v. Caraco Pharm. Lab'ys, Ltd.</i> , 719 F.3d 1346 (Fed. Cir. 2013)	34
<i>Precision Cancer Techs. Inc. v. Oncoustics Inc.</i> , IPR2025-00242, Paper 7 (PTAB June 3, 2025)	38
<i>Samsung Elecs. Co., Ltd. v. CardWare, Inc.</i> , IPR2023-00210, Paper 3 (PTAB Nov. 15, 2022).....	1
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	41
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022).....	38
Regulations	
37 C.F.R. § 11.18	23

37 C.F.R. § 42.11	23
37 C.F.R. § 42.12(b)	23

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	Email Correspondence between counsel for Patent Owner and Petitioner, dated May 19, 2025

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)
2025	DocketNavigator Time to Trial Statistics for Patent Cases in the Western District of Texas
[New] 2026	DECISION Denying Institution of <i>Inter Partes</i> Review in <i>Samsung Elecs. Co., Ltd. v. CardWare, Inc.</i> , IPR2023-00210, Paper 13 (PTAB June 13, 2023)

I. INTRODUCTION

On June 24, 2025, Apple Inc. (“Apple” or “Petitioner”) filed a Petition requesting *inter partes* review (“IPR”) of claims 1-17 (“Challenged Claims”) of U.S. Patent No. 10,339,520 (“the ’520 Patent”) (EX1001), entirely on 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. There are two main reasons that concern each Challenged Claim and all of Petitioner’s proposed Grounds.

First, none of Petitioner’s cited prior art references teach a “static device account number,” as required by limitations 10(d) and 10(g) in independent claim 10 (and similar limitations in claim 1—the other independent challenged claim).

This is not the first IPR on the ’520 Patent. Samsung filed a petition on November 15, 2022 asserting that a combination of references (not dissimilar from those presented here) rendered obvious claims 1 and 4-17. *See Samsung Elecs. Co., Ltd. v. CardWare, Inc.*, IPR2023-00210, Paper 3 (Petition) (PTAB Nov. 15, 2022); *see also* EX2026 (IPR2023-00210, Paper 13), 1, 4-5. The Board denied institution

on the merits because Samsung’s references failed to disclose this same “static device account number” limitation. *See, e.g.*, EX2026, 13.

Petitioner’s references fail for similar reasons. Petitioner relies upon a “mobile wallet account number” allegedly disclosed by reference to Grigg. Pet., 16. But this is not a “device” number; it is just what the phrase suggests—a number that is tied to a mobile wallet (software) and can be used across multiple devices. Indeed, Grigg never even discloses that the system provisioning mobile wallet account numbers has any idea what device is involved; the system only knows the mobile wallet (software) information, regardless of the device on which the software resides. Moreover, Grigg discloses a dozen different permutations of mobile wallet account numbers, including “one time use” numbers. These “one time use” numbers would not be “static” (as per the Board’s ruling in denying institution in IPR2023-00210, Paper 13 (EX2026)), and Petitioner never explains why a POSITA would be motivated to use the one particular permutation (of a dozen) it relies upon in combining the teachings with Toomer and Hammad (even putting aside that the mobile wallet account number is not a “device” number). Indeed, elsewhere, Petitioner argues that a POSITA would be motivated to use an additional dynamic (one time use) number, without ever explaining why a POSITA wouldn’t simply select the non-static one time mobile wallet number disclosed by Grigg.

Second, Petitioner fails to address a significant flaw in its obviousness combination based on Hammad. Hammad is a reference that is exclusively directed to “skimming,” which it defines as the “electronic copying of a card’s magnetic stripe data to create counterfeit cards.” EX1006, 1:21-23, 1:35-45 (noting that skimming is also applicable in a wireless environment). To address this, Hammad uses a dynamic CVV number based on multiple data elements, which gets “embedded into the payment data transmitted from the portable consumer device to the point of sale terminal.” EX1006, 6:40-42. Together, this data gets used to verify the transaction; without it, the account information cannot be used in connection with the Hammad system to make a payment.

Petitioner argues that a POSITA would have used the dynamic CVV of Hammad with the “mobile wallet account number” of Grigg for some (unspecified) “security” reason. Pet., 32. But, the whole idea of Grigg is to use the mobile wallet account number *instead* of real account information; that real account information is removed from, and is not stored on, the electronic device. In other words, with Grigg, there is no account information to “skim” and therefore no reason to look to Hammad’s solution to the “skimming” problem. Petitioner does not even address this. Rather, Petitioner and its expert simply regurgitate boilerplate obviousness positions about “reasonable expectation of success,” and application of “straight-forward and known methods” without ever considering the actual teachings of the

references and the particular payment problems they are trying to solve. Pet., 32; EX1003 ¶¶160-61. On its face, Petitioner’s obviousness position is little more than a grab-bag approach—picking disclosures from three disparate and incompatible references just because they independently disclose various limitations (even then Petitioner could not find a “static device account number”).

Lastly, Petitioner fails to tell the Board that in a parallel district court proceeding, it argued that all of the claims that are the subject of this Petition are indefinite because the claim scope allegedly cannot be determined. It used one expert in district court to support this indefiniteness point but picked a different one in this proceeding to apply what Petitioner says is the “ordinary and customary meaning,” excepting two terms for which Petitioner purports to “adopt[]” (without analysis) “[f]or purposes of this proceeding only” the constructions “proposed by Patent Owner.” Pet., 6. Petitioner also omits that Challenged Claims 1-9 of the ’520 Patent were found indefinite in a prior case based on “the payment information” limitation in independent claim 1. *See CardWare Inc. v. Samsung Elecs. Co. Ltd.*, Case No. 2:22-CV-141-JRG-RSP, 2023 WL 5434763, at *11 (E.D. Tex. Aug 22, 2023). And while Petitioner lost its indefiniteness argument in district court as to claims 10-17 (*see* EX2024, 1), it has not waived its appellate rights on this issue. This is yet another reason the Board should deny institution, as Petitioner’s failure to even inform the Board about its district court position is an undisclosed material fact,

violates the duty of candor, and further demonstrates that Petitioner has failed to show a reasonable likelihood of success that any challenged claim is unpatentable.

For these reasons and those explained below, the Board should deny institution. Petitioner has not demonstrated a reasonable likelihood of success on any claim.

II. THE '520 PATENT CLAIMS

When David Wyatt conceived of the invention claimed in the '520 Patent over a decade ago, there were “several different types of credit cards available in the marketplace.” EX1001, 1:32-33. As the '520 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 '520 Patent generally relate to systems and methods for reducing fraud during payment transactions. Independent claim 1 is illustrative and is directed to an electronic device wherein a user can input issued payments

information (such as a traditional credit card number). EX1001, 15:64-16:33 (claim 1). The device has memory with both device-specific and user-specific information and wirelessly receives a “static device account number.” EX1001, 16:18-20. Wirelessly receiving this static device account number permits the security risk to be separated from the actual device maker. In other words, by wirelessly receiving the static device account number, it can come from a third party that is not the device maker itself and is not also in possession of other secure information, such as the algorithm for generating other cryptographic information. If the static device account number came pre-loaded onto the electronic device, then a single hack of a device maker may expose all of the secure payment information necessary to complete a payment transaction. Claim 1 also requires “dynamically generating a one-time limited-use number[]” and “using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information.” EX1001, 16:24-33. In other words, the device dynamically generates a one-time limited use number and combines it with the static device account number. It uses these numbers together in place of issuer provided payment information (*e.g.*, a traditional credit card number) for making a payment transaction. EX1001, 16:30-33.

III. PETITIONER’S ALLEGED PRIOR ART

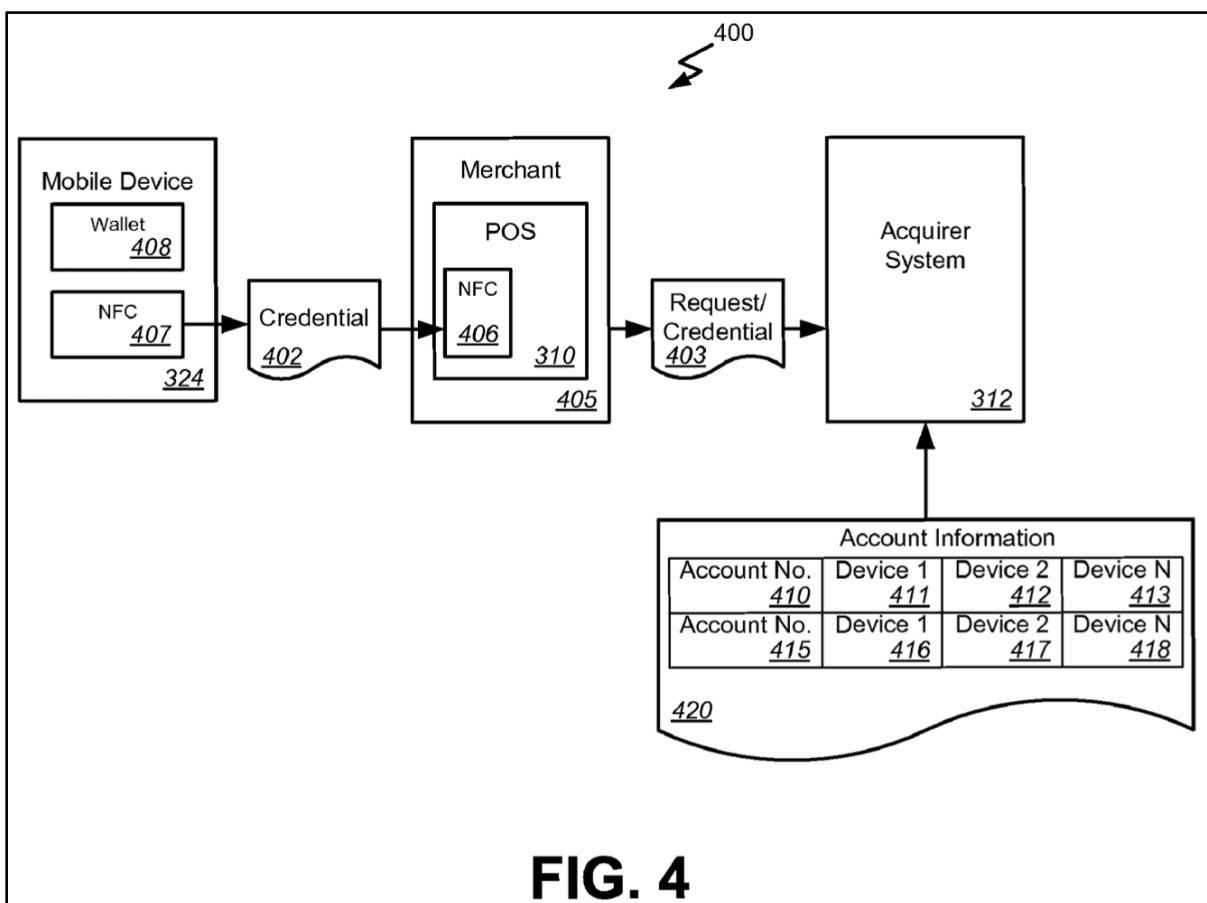
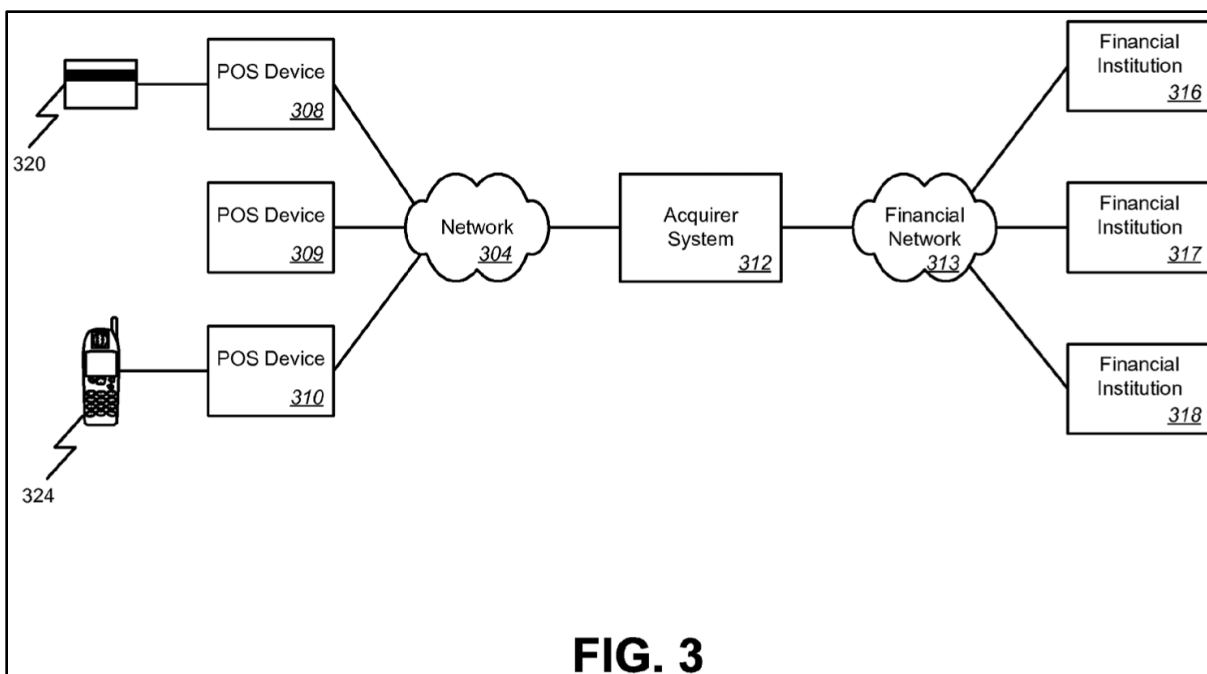
At its core, Petitioner’s proposed obviousness combination is based on a combination of Toomer, Griggs, and Hammad. Pet., 12-33. As best that Patent Owner can discern, Petitioner proposes that Toomer is the base reference, including its mobile device and associated mobile wallet, in which a user can store multiple payment vehicles. Pet., 12-33. Petitioner then proposes that it would have been obvious to “wirelessly receive and store Grigg’s mobile wallet account number in place of Toomer’s account number, akin to Toomer’s ‘unique identifier for use by other systems in identifying’ an account.” Pet., 23. From there, Petitioner proposes that a POSITA would build in the dCVV disclosure of Hammad. Pet., 28. Per Petitioner, “[a] POSITA would have found it obvious to include this information [multiple data elements] in addition to Grigg’s mobile wallet account number (*account information*) in generating a dCVV to be used with the payment credentials of Toomer-Grigg when conducting a payment transaction.” Pet., 31 (emphasis in original). These three references describe completely different and incompatible payment systems, as described below.

A. Toomer

U.S. Patent App. Pub. No. 2009/0210308 (“Toomer”) discloses use of a “device identifier,” in combination with actual issued payment information, in order to make a payment. EX1004, [0005].

As per the Background of the Invention section, Toomer explains that, “[c]onveniently, accounts represented by information stored in [] electronic devices, i.e., an electronic payment credential, can be programmed or provisioned to the electronic device in many different ways.” EX1004, [0003]. But Toomer identifies potential drawbacks with using an electronic device, noting, “it is important to assure that the account information is not provisioned to or used by electronic devices which are not authorized to utilize that account information.” EX1004, [0003]. “For example, a particular electronic credential may be authorized for use on one or a small group of electronic devices.” EX1004, [0003].

Accordingly, Toomer describes systems and methods to include a device identifier (either static or dynamic), together with real (issued) account information, in connection with a payment transaction. Figure 3 of Toomer, shown below, represents a system for utilizing a mobile electronic device to process a transaction. EX1004, FIG. 3. Figure 4, also shown below, provides “additional details” of the system of Figure 3. EX1004, [0012], FIG. 4.



EX1004, FIGs. 3-4.

Toomer explains that the mobile device 324 (e.g., in Figure 3 above) “can store and/or execute a mobile wallet application adapted to maintain account numbers and/or other information, i.e., electronic payment credentials, related to one or more financial accounts such as credit accounts, debit accounts [etc.]” EX1004, [0052]. Importantly, when a transaction is processed, Toomer contemplates sending the *actual issued payment information (the credential)*: “Upon selection of an account for use in the transaction, the user of the mobile device can scan or swipe the device 324 in front of or near the POS device 310 causing the credential of other information related to the selected account to be read from the mobile device 324 via the NFC connection.” EX1004, [0052]. That credential “can identify the account to be used in supporting transactions, for example, including an indication of the financial institution 316 where the account is maintained, an account number, etc.” EX1004, [0053]. While authorization is based on the “validity of the account number” and other account-related information, “authorization can also be based at least in part on determining whether the mobile device is authorized to use the account for which the information or credential has been provided.” EX1004, [0054].

As described with reference to Figure 4 (also above), an acquirer system (which is a “system operated by an acquirer [such as First Data Corp.] that processes and authorizes credit card and/or other transactions” (EX1004, [0021])) can

“maintain information 420 identifying one or more accounts 410 and 415” as well as “one or more devices 411-413 and 416-418 which are authorized to use the account.” EX1004, [0057], FIG. 4.

Toomer explains that the information identifying the electronic device presenting the payment credential can be a “unique static identifier” such as a “device serial number.” EX1004, [0059]. Or, “[i]n other cases, the information identifying the electronic device presenting the payment credential can comprise a unique dynamic identifier.” EX1004, [0059]. Either of these identifiers can be provisioned to the device. EX1004, [0059].

In sum, Toomer describes a traditional payment method using a mobile wallet, with the addition of some device identifier, either static or dynamic. But there are two important takeaways from Toomer: (1) it uses *actual* issued payment information (*e.g.*, account numbers 410 and 415); and (2) it uses a device identifier that is *either* static or dynamic. EX1004, [0057], [0059], FIG. 4. Toomer does not contemplate using *both* a static and dynamic number. Nor does it explain any reason why a POSITA would want to do that.

B. Grigg

U.S. Patent App. Pub. No. 2014/0006276 (“Grigg”) is directed to payments using a mobile wallet. In particular, Grigg explains that a “need exists for a way to provide security to the financial accounts associated with a mobile wallet such that

if an individual's mobile phone is lost or stolen, the individual's financial information is secure." EX1005, [0004].

Grigg contemplates use of a "mobile wallet account number for the user's mobile wallet and/or each of the payment devices associated therewith." EX1005, [0011].¹ With this, "if a mobile wallet is misplaced, the user may cancel the mobile wallet account number without affecting any payment device account itself." EX1005, [0006].

Grigg describes various permutations of this mobile wallet account number. It could be "permanently associated with the mobile wallet," "temporarily associated with the mobile wallet," or "a one-time use account number for the mobile wallet." EX1005, [0011], [0037]. Moreover, the mobile wallet account number could be unique to an underlying payment device (*i.e.*, payment account), or "there may be one mobile wallet account number for all of the payment devices associated with the mobile wallet" such that it is not tied to any payment device (*i.e.*, payment account) and is instead payment account agnostic. EX1005, [0011], [0091] ("The mobile wallet account number may not be directly associated with any payment device.").

¹ Grigg explains that "[a] 'payment device' as used herein may refer to any *means* of payment for a product of a transaction. As such a payment device may include, but is not limited to a credit card, debit card [etc.]." EX1005, [0029].

Grigg further discloses that in some instances of completing a payment transaction, “the system may provide the merchant with the appropriate payment device and account number associated therewith in replace [sic] of the mobile wallet account number the merchant received.” EX1005, [0013]. In other words, in this iteration, the merchant still receives the actual issued payment information; it differs from a traditional transaction in the sense that the issued payment information is provided by a remote system and need not be stored on the phone (such that “if the mobile wallet is misplaced, lost, or the like the financial accounts associated with the payment devices on the mobile wallet are not also misplaced.”). EX1005, [0014]. Alternatively, Grigg discloses that a financial institution application may determine the payment devices that the user has added, stores the payment numbers, and associate them with a mobile wallet account number. EX1005, [0049]-[0051]. Grigg does not explain how this would work universally across payment devices issued by different networks (Visa vs. Mastercard) and issuers (different banks). Nor does Petitioner.

Figure 2, reproduced below, “provides a mobile wallet account number differentiation system environment” and includes a “financial institution server 208 [that] can send information to and receive information from the user device 204” and other components in the system. EX1005, [0040], FIG. 2.

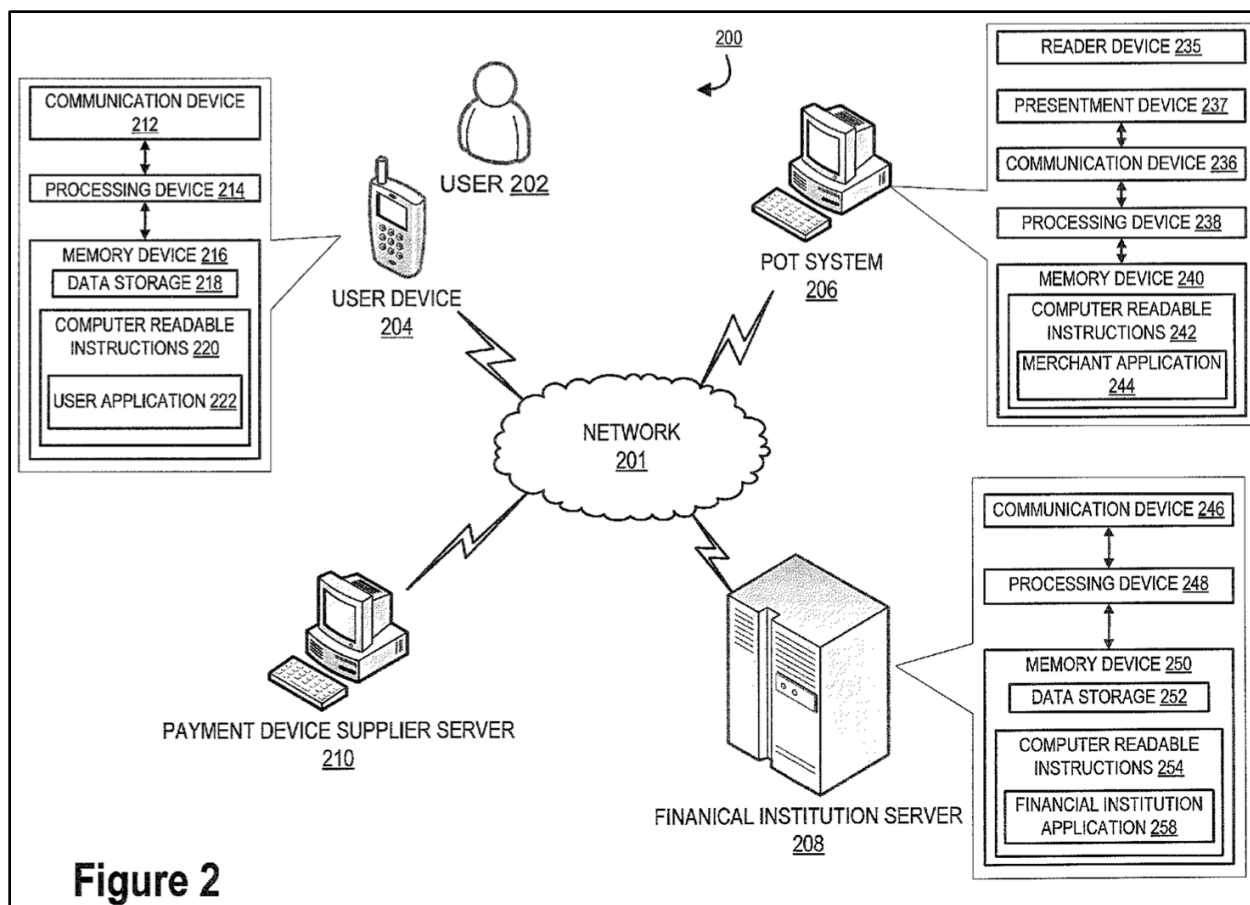


Figure 2

EX1005, FIG. 2.

The financial institution server 208 includes a “financial institution application 258 [that] allows for the replacement of payment device account numbers with mobile wallet account numbers in a mobile wallet.” EX1005, [0047]. The application 258 may “store the payment device account numbers associated with the payment devices a user 202 has on his/her mobile wallet” such that when “a mobile wallet transaction is processed by a merchant” the “application 258 may subsequently provide the merchant with the payment device account number to apply the transaction to.” However, in other embodiments, “the financial institution

application 258 may subsequently apply the transaction directly to the payment device account number without merchant involvement.” EX1005, [0050]. In other words, Grigg discloses two use cases for each transaction—one in which the actual issued payment information is used (by providing it to a merchant) and one in which it is not (where it applied “without merchant involvement”). EX1005, [0047]-[0050]. In the latter case, Grigg discloses various permutations of how the transaction can be applied to particular payment accounts. EX1005, [0054]-[0057].

There are several important takeaways from Grigg that are relevant to Petitioner’s Petition and that are set out below.

- 1) At no point does Grigg indicate that the mobile wallet is associated with any particular device, or include any indication of the device from which it comes. To the contrary, Grigg explains that the mobile wallet is accessed by a user application 222, which is software. EX1005, [0070]. Grigg also explains that the system environment 200 of Figure 2 “may contain numerous user devices 204” without indicating that there might be different mobile wallet account numbers for each. EX1005, [0070], FIG. 2. In other words, a user could own multiple devices (*e.g.*, a phone, a tablet, or other) that are each linked to the same mobile wallet. Or, the user could get a replacement device (*e.g.*, a new phone) and keep the same mobile wallet account number. Grigg says

nothing about what happens when a user gets a new phone in the ordinary course (such that, for example, the mobile wallet is installed on the new phone). Grigg also does not say anything about informing the financial institution about the particular user device (*e.g.*, a device serial number) on which the mobile wallet is being used. In sum, at no point does Grigg ever indicate that the mobile wallet account number is tied to the particular user device; it is instead tied to the mobile wallet software and the user's accounts. *See e.g.*, EX1005, [0071] (“[T]he user application 222 may ... receive the mobile wallet account number ***assigned to the mobile wallet***, and allow the user 202 to utilize the user device 204 as a mobile wallet for transactions[.]”), [0081] (“[I]f the user's user device 204 gets misplaced, the user 202 may not have to cancel and/or re-open each account associated with the mobile wallet. The user 202 may simply cancel the mobile wallet account number ***associated with the mobile wallet*** and be re-issued a new mobile wallet account number. The system may then tie the new mobile wallet account number ***to the user's payment device accounts*** stored.”).

- 2) Grigg discloses a dozen permutations of possible mobile wallet payment account numbers and use of issued payment information. Specifically, Grigg discloses that the mobile wallet account number can

be permanent, temporary, or one-time use. EX1005, [0011]. And for each such type, the number can be unique to a payment account, or account agnostic and simply tied to the mobile wallet software. EX1005, [0011]. Further, Grigg indicates that actual issued payment information can be transmitted to the merchant for use in the transaction, or it can be reconciled later (without being transmitted to the merchant). EX1005, [0047], [0056]. It appears that Petitioner is relying on only one of these dozen permutations in connection with its obviousness position—the permutation where the number is permanent, account specific, and where the issued payment information is not used. As set out below, Petitioner never says why a POSITA would implement this particular permutation when creating the obviousness combination with Toomer and Hammad. Nor does Grigg explain any advantage of using this particular iteration.

- 3) Grigg contemplates a single “financial institution server 208” that can handle “each payment device account that the user 202 may have on his/her mobile wallet” regardless of which bank issued the payment device, and/or which network (*e.g.*, Visa or Mastercard) would clear the transaction. EX1005, [0073]. Grigg does not explain who would control or operate such a financial institution server or what it might look like.

Such a financial institution server (that handles *each* payment device account) would have to be able to handle traffic across every bank and network. Petitioner does not say how this would work, or why a POSITA would implement Grigg's new system in combination with other references

- 4) Grigg is directed to a system that allows removal of the underlying payment information from the mobile wallet after receiving the mobile wallet account number. EX1005, [0081]. It is specifically directed to the convenience factor of not having to cancel all underlying payment accounts in the event of a lost device. EX1005, [0071]. But Grigg does not address what happens when a particular POT does not accept mobile wallet account numbers. Nor does Petitioner explain why a POSITA would adopt this approach in view of such a limitation.

C. Hammad

U.S. Patent No. 7,740,168 ("Hammad") is concerned with "skimming", which refers to "electronic copying of a card's magnetic stripe data to create counterfeit cards." EX1006, 1:21-23.

Hammad explains that:

Skimming is predominantly a phenomenon affecting magnetic stripe based transactions. This is because the magnetic stripe, which is placed on the back of a

transaction card and stores a variety of data on three separate tracks, is a passive medium. In other words, the digital content of the magnetic stripe can be perfectly copied, without any difference between the copy and the original.

EX1006, 1:24-30.

Hammad notes that this problem is even more acute in a wireless environment:

In fact, in a wireless environment the opportunity to skim magnetic stripe data is more prevalent. In a wireless environment, a potential skimmer need not physically possess the card to be skimmed nor have access to any of the physical equipment (e.g., POS terminal, communication lines, etc.) which is required for skimming in a wired based environment.

EX1006, 1:36-42.

Hammad explains, “To address the above problems [i.e., skimming from a physical card], a dCVV or a dynamic card verification value can be used.” EX1006, 1:46-47. Hammad explains that the dCVV value can be generated by either a portable consumer device or a POS terminal. EX1006, 1:51-52. Per Hammad, the prior art typically only includes one dynamic data element to generate the dCVV, which could result in compromised security. EX1006, 1:66-2:4. Accordingly, the entirety of Hammad’s disclosure is about the use of a dCVV based on multiple data

elements, such that it can be “embedded into the payment data transmitted” to the point of sale terminal. EX1006, 6:40-42. The point, as Hammad articulates, is to disguise the real account number by inserting the dCVV such that “the point of sale terminal may not be able to determine if a dCVV is embedded and where such dCVV may be located. There is no indication to the point of sale terminal that a dCVV is embedded into the data received from the portable consumer device.” EX1006, 6:44-48.

The key takeaway about Hammad, discussed below, is that it addresses the skimming problem, specifically. This problem is rooted in the storage and use of actual account information that a fraudster might try to steal with skimming devices. To address this, Hammad discloses a particular dCVV configuration with particular placements within standard mag stripe data. Hammad does not disclose any use case of this dCVV invention in a situation where actual payment data is not used (and therefore not at risk of being skimmed).

D. Petitioner’s Proposed Combination

At its core, Petitioner’s proposed obviousness combination is based on a combination of Toomer, Griggs, and Hammad. As best that Patent Owner can discern, Petitioner proposes that Toomer is the base 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 “wirelessly

receive and store Grigg’s mobile wallet account number in place of Toomer’s account number, akin to Toomer’s ‘unique identifier for use by other systems in identifying’ an account.” Pet., 23. From there, Petitioner proposes that a POSITA would build in the dCVV disclosure of Hammad. Pet., 30. “A POSITA would have found it obvious to include this information [multiple data elements] in addition to Grigg’s mobile wallet account number (account information) in generating a dCVV to be used with the payment credentials of Toomer-Grigg when conducting a payment transaction.” Pet., 31 (emphasis in original).

IV. CLAIM CONSTRUCTION

A. Static Device Account Number

All Challenged Claims require a “static device account number.” This number is each of a “static number,” a “device number,” and an “account number”; the applicant simply put all three of those descriptors together in one and referred to it as a “static device account number.”

The Board has already effectively determined as much in connection with IPR2023-00210, which also involved independent claims 1 and 10 (and others) as here. In that proceeding, the Board denied institution on the merits because it determined that Petitioner (Samsung) failed to demonstrate that any of its references disclosed a “static device account number.” EX2026 (IPR2023-00210, Paper 13), 9. The Board held that “the ’520 Patent does not support construing ‘a static device

account number’ as encompassing a number that is dynamically generated and valid for only a finite number of transactions or a specified period of time, such as two minutes, ten minutes, or three hours.” EX2026, 14.

The Board did not specifically address the words “device” or “account,” but it did determine that “static” modifies “number” and that Petitioner needed to show that the prior art disclosed such a “static” number. EX2026, 8. The same logic should apply to the words “device” and “account.” Just like a “static device account number” must be a “static number,” it also must be a “device” number and an “account” number.

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

In its IPR petition, Petitioner purports to “adopt[]” Patent Owner’s constructions for two terms “[f]or purposes of this proceeding *only*,” and “Petitioner applies the ordinary and customary meaning of the claim terms as understood by a POSITA” for everything else. Pet., 6 (emphasis added). Its expert also purports to apply the plain and ordinary meaning. EX1003 ¶25.

Importantly, however, Petitioner omits that—in district court using a different expert—Petitioner asserts that, for Challenged Claims 10-17, the term “the payment information” in independent claim 10 renders claim 10 (and by dependency, claims 11-17) indefinite. EX2016 at 5-9; EX2018 at 1-4; EX2020 at 2. The district court has now rejected Petitioner’s arguments (*see* EX2024), but regardless, Petitioner’s

positions are completely inconsistent and it will surely insist on preserving those indefiniteness positions for appeal (and it has not waived its right to do so).

Petitioner also omits that it asserted that claims 1-9 were indefinite for a similar reason, EX2010 at 34-36; EX2016 at 5 n.1, and that in a prior claim construction order, Judge Gilstrap found “that ‘the payment information’ in Claim 1 of the ’520 Patent is indefinite.” *See CardWare Inc. v. Samsung Elecs. Co. Ltd.*, Case No. 2:22-CV-141-JRG-RSP, 2023 WL 5434763, at *11 (E.D. Tex. Aug 22, 2023).

Patent Owner respectfully submits that Petitioner should not be able to assert, on the one hand, that the claimed scope cannot be ascertained and the claims are indefinite in district court, and on the other hand, tell the Board that they are amenable to an obviousness challenge, in Petitioner’s words, “[f]or purposes of this proceeding only.” Worse, Petitioner does not even inform the Board about its inconsistent positions.

Petitioner’s failure to inform the Board about these material facts should be reason to deny the Petition as it believes that the Challenged Claims cannot actually be construed. Indeed, Petitioner is taking different positions concerning the claims as the need suits and seeking to adopt (without analysis or support) a construction it believes to be incorrect. *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 has a “Static Device Account Number” as Required by Limitations 10(d) and 10(g)

1. Petitioner Fails to Explain Why the Mobile Wallet Account Number of Grigg is a “Device” Number

Just like Samsung in connection with IPR2023-00210, Petitioner fails to show that its proposed obviousness combination includes a “static device account number” as required by limitations:

- 10(d), requiring “receiving wirelessly a static device account number payment information for storage on the electronic device;”² EX1001, 17:18-19, and

² In IPR2023-00210, the parties and the Board treated this same limitation as element 10(e). EX2026 (IPR2023-00210, Paper 13), 8.

- 10(g), requiring “using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.” EX1001, 17:30-33.

Petitioner asserts that the “mobile wallet account number” of Grigg constitutes the “static device account number.” *See, e.g.,* Pet., 22 (“Grigg’s mobile wallet number is a device account number.”) (emphasis in original), 23 (“A POSITA would have found it obvious and been motivated to wirelessly receive and store Grigg’s mobile wallet account number in place of Toomer’s account number.”). But Grigg never says that the “mobile wallet account number” is a “*device*” number. And, in many of the dozen permutations of the “mobile wallet account number” outlined in Grigg, it is also *not* a “static” number or an “account” number. The reasons are set out below.

2. None of the Mobile Wallet Account Number Permutations in Grigg is “Device” Number

Grigg repeatedly explains that the mobile wallet is embodied as software. EX1005, [0008] (“A mobile wallet may be any type of digital wallet...”), [0011] (“The system may then assign a mobile wallet account number for the user’s mobile wallet and/or each of the payment devices [*i.e.*, the user’s payment accounts] associated therewith.”), [0029]. Grigg explains that the system “create[s] a mobile wallet account number for the user’s mobile wallet,” which, again, is embodied as

software. EX1005, [0037]. In particular, Grigg explains, with reference to Figure 2: “[t]he user device 204 comprises computer-readable instructions 220 stored in the memory device 216, which in one embodiment includes the computer-readable instructions 220 of a user application 222. In this way, the user application 222 allows a user 202 to have and/or support a mobile wallet.” EX1005, [0070], FIG. 2.

Grigg never once indicates that the “mobile wallet account number” is a “device” number. To the contrary, Grigg states, again with reference to Figure 2, that “[a]lthough only a single user device 204 is depicted in FIG. 2, the system environment 200 may contain numerous user devices 204.” EX1005, [0070]. Grigg further indicates that the mobile wallet account number is not associated with a particular user device. EX1005, [0071], [0081]. This suggests that the same mobile wallet account number may be used across devices, for example, if a user has multiple mobile phones, or a mobile phone and a tablet.

This interpretation would also be consistent with the problem that Grigg is trying to address. Specifically, Grigg explains that:

[A] mobile wallet is typically associated with the individual’s mobile device, such as his/her mobile phone. Mobile phones are misplaced, lost, stolen, and the like. As such, the financial data associated with the individual’s mobile wallet may also be lost and/or stolen. Since the mobile wallet may store most of the individual’s payment devices [e.g., the underlying credit card accounts], a lost

or stolen mobile phone may require an individual to call each payment device supplier and cancel those accounts.

Therefore, a need exists for a way to provide security to the financial accounts associated with a mobile wallet such that if an individual's mobile phone is lost or stolen, the individual's financial information is secure.

EX1005, [0003]-[0004].

The Grigg invention simplifies this problem because “if a mobile wallet is misplaced, the user may cancel the mobile wallet account number without affecting any payment device account itself.” EX1005, [0006]. In other words, Grigg is concerned with the situation where a mobile wallet falls into the wrong hands such that it compromises the underlying accounts. Grigg does not explain *any* reason to have different mobile wallet account numbers across “numerous user devices 204,” in the situation where these various devices all remain secure and in the user's possession. EX1005, [0070]. If anything, multiple mobile wallet account numbers for the same user would likely create confusion and complexity. Nor does Grigg address the situation where a user upgrades their mobile device in the normal course, and installs all their software including the mobile wallet itself. In those instances, the mobile wallet is not “lost,” “stolen,” or otherwise compromised. There is no reason, given the Grigg teachings, to have different a different mobile wallet account numbers across devices.

Petitioner and its expert offer almost nothing to the contrary. Petitioner states:

Grigg’s mobile wallet number is a device account number.

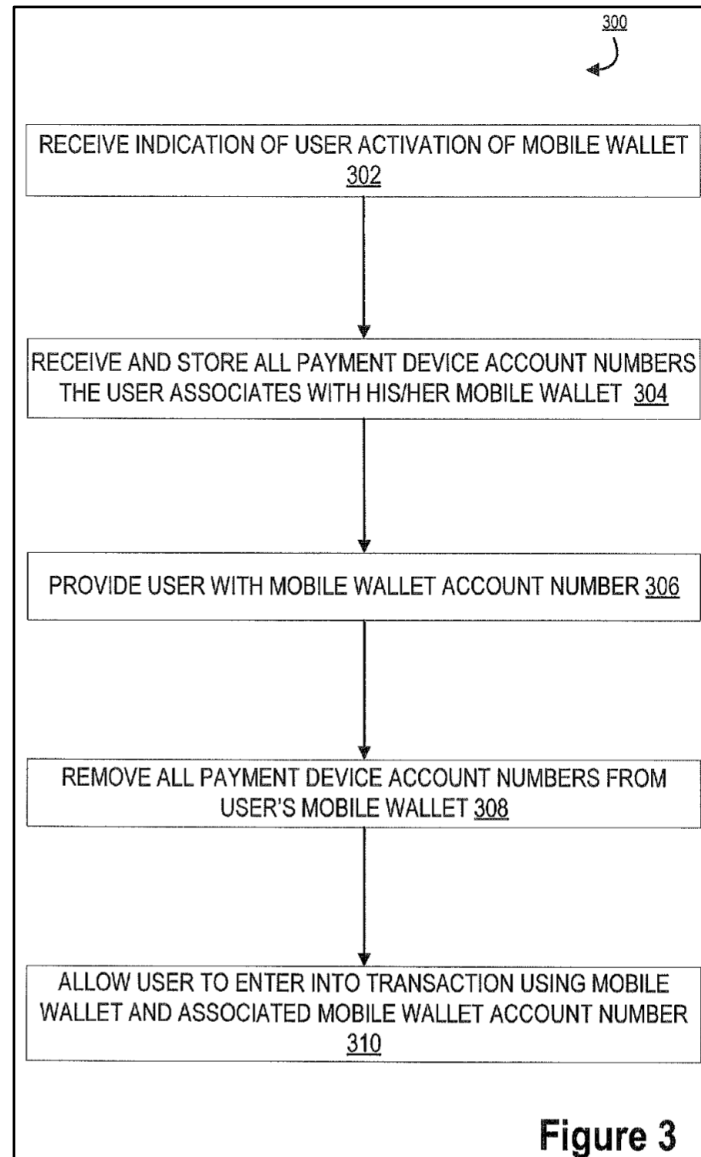
Grigg teaches that “the user 202 may use his/her user device 204 as a mobile wallet” (Grigg, [0043]) and that the “mobile wallet account number” is created “for the user’s mobile wallet” and “permanently associated with the mobile wallet.” *Grigg*, [0037], [0051], [0081]; Dec. ¶136.

Pet., 22; EX1003 ¶136 (mirroring the petition, including emphasis).

Petitioner is correct, of course, that a user may use his/her device as a wallet, but this does not say anything about whether it is a “device” number. In other words, it is of no moment that a mobile wallet is used in connection with a device (just the same as any software would be). The point is that the mobile wallet account number is tied to the mobile wallet and *not* any particular device. Petitioner and its expert fail to address Grigg’s explanation that the system environment may contain “numerous user devices 204” without any mention of separate mobile wallet account numbers for each device. Nor does Petitioner address the situation where a user simply upgrades their mobile device in the normal course, porting over all software from the prior device.

Indeed, there is no indication in Grigg that the financial institution that provisions the mobile wallet account number even knows the identity of the user’s

device. Figure 3 is representative of the provisioning process and does not mention anything about a device identifier:



EX1005, FIG. 3.

Grigg explains the above process as follows:

- “As illustrated in block 302, the system may first receive an indication that a user 202 has activated his/her mobile wallet.” EX1005, [0078].

- “Next, as illustrated in block 304, once the system has determined that the user 202 uses a mobile wallet, the system may receive and store all payment device account numbers that are associated with the user’s mobile wallet.” EX1005, [0079].
- “As illustrated in block 306, once the system has received and stored all the payment device account numbers that are associated with the user’s mobile wallet, the system may provide the user 202 with a mobile wallet account number.” EX1005, [0080].

Again, all of these steps for provisioning a mobile wallet account number have to do with identification of a mobile wallet, and not any particular device. It is software that happens to operate on one or more devices, but nothing more.

Accordingly, Petitioner has failed to meet its burden that Grigg discloses a “static device account number.” This should be sufficient to deny institution of the Petition given that this limitation is in every challenged claim and Petitioner relies on Grigg to meet it for every claim and every ground. However, for completeness, it is worth noting that Toomer also fails to disclose a static device account number (and Petitioner clearly only relies on Hammad for the dCVV). Toomer discloses, in one embodiment, a static device number, but does not ever indicate that this is a static device account number. EX1004, [0059]. Moreover, Toomer uses actual issued payment information, and, to the extent Petitioner relies on Toomer’s static device

number plus issued payment information approach, this would fail to meet at least limitation 10(g) requiring use of certain information “in the place of issuer provided payment information for making a payment transaction.”

3. Petitioner Does Not Explain Why a POSITA Would Have Selected the One Particular Permutation of Mobile Wallet Account Number from Grigg (out of a Dozen) that it Relies Upon in its Obviousness Combination

Grigg discloses various permutations of mobile wallet account numbers. They can be permanent, temporary, or one-time use. EX1005, [0011], [0037]. Moreover, the mobile wallet account number could be unique to an underlying payment device (*i.e.*, payment account), or “there may be one mobile wallet account number for all of the payment devices associated with the mobile wallet” such that it is not tied to any particular payment device (*i.e.*, payment account) and is account agnostic. EX1005, [0011], [0091] (“The mobile wallet account number may not be directly associated with any payment device.”). Grigg further discloses that in some instances of completing a payment transaction, “the system may provide the merchant with the appropriate payment device and account number associated therewith in replace [sic] of the mobile wallet account number the merchant received.” EX1005, [0013].

Accordingly, Grigg discloses the below combinations of mobile wallet account numbers. It appears that Petitioner is only relying on permutation number 2, where the mobile wallet account number is permanent and specific to each payment

device (and where the issued payment information is not used in the transaction). Accordingly, while Petitioner is correct that this is a disclosure of a static mobile wallet account number (albeit not a “device” number), this is just one of twelve permutations and Petitioner does not ever explain why a POSITA would pick *this* permutation when combining the Grigg, Toomer and Hammad teachings. Pet., 21-23. Petitioner and its expert simply assume that this would have been the case. Pet., 21-23; EX1003 ¶¶132-140.

Permutation #	Permanent/ Temporary/ Rotating Number?	Tied to Account or Account Agnostic?	Use Issued Payment Information in Transaction?
1	Permanent	Account specific	Yes
2	<i>Permanent</i>	<i>Account specific</i>	<i>No</i>
3	Permanent	Account agnostic	Yes
4	Permanent	Account agnostic	No
5	Temporary	Account specific	Yes
6	Temporary	Account specific	No
7	Temporary	Account agnostic	Yes
8	Temporary	Account agnostic	No
9	One Time Use	Account specific	Yes
10	One Time Use	Account specific	No

Permutation #	Permanent/ Temporary/ Rotating Number?	Tied to Account or Account Agnostic?	Use Issued Payment Information in Transaction?
11	One Time Use	Account agnostic	Yes
12	One Time Use	Account agnostic	No

Petitioner’s position is particularly problematic when considered in connection with its position on Hammad, discussed further below. Petitioner argues, in connection with limitation 10(f) that “[b]ased on the teachings of Hammad, it would have been obvious, and a POSITA would have been motivated to generate a dCVV including dynamic and static data elements, as taught by Hammad, in Toomer-Grigg.” Pet., 30.

This makes no sense when considering the various permutations of “mobile wallet account numbers” disclosed by Toomer. Specifically, Toomer already discloses a “One Time Use” mobile wallet account number; why would a POSITA pass on that option, and instead choose the “permanent” mobile wallet account number, only to then add in Hammad’s dynamic CVV? Why wouldn’t a POSITA simply use the one-time use mobile wallet account number permutation of Toomer, and, if anything, build in Hammad’s teachings about basing that on multiple data elements? Petitioner never even addresses these questions. Rather, Petitioner simply assumes that because Toomer discloses a permanent mobile wallet account number that a POSITA would pick *that* option and then build in a separate dynamic number

that is, at best, superfluous of what could have been achieved with Toomer alone (when selecting a different mobile wallet account number). Pet., 30-33. This is yet another reason why Petitioner fails to meet its burden as it concerns limitation 10(d). *See also, e.g., Novo Nordisk v. Caraco Pharm. Lab'ys, Ltd.*, 719 F.3d 1346, 1365 (Fed. Cir. 2013) (“In the search for scientific truth one cannot pick and choose among isolated disclosures in the prior art to deprecate the claimed invention; it is necessary to consider prior art that supports unobviousness of the claimed invention, as well as that which weighs against it.”) (cleaned up).

B. Petitioner Fails to Demonstrate that a Person of Ordinary Skill in the Art Would Use the dCVV of Hammad with the Mobile Wallet Account Number of Grigg (in connection with limitation 10(g))

There are multiple reasons why Petitioner’s obvious combination does not make sense. As it concerns limitations 10(f) and 10(g), Petitioner ignores all of the reasons why Hammad’s dCVV would not fit with the Toomer-Grigg combination it proposes.

Limitation 10(f) requires “dynamically generating a one-time limited-use number...” and limitation 10(g) requires “using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.” EX1001, 17:24-33. With respect to these limitations, Petitioner argues that:

- (i) It would have been obvious to a POSITA to include the “dCVV including dynamic and static data elements, as taught by Hammad, in Toomer-Grigg.” Pet., 30.
- (ii) A POSITA would have added a dCVV because “it would require straight-forward and known methods of generating a dynamic CVV and providing the same with other account information . . .” Pet., 32.
- (iii) A POSITA “would have had a reasonable expectation of success” (Pet., 32), that it would have “required only basic software modifications and routine skill” (Pet., 33) and that it “would beneficially provide an additional layer of security.” Pet., 34.

Petitioner’s expert parrots Petitioner’s petition (or vice versa—they are effectively the same) and adds the non-specific conclusion that “a POSITA would have been motivated to increase security of a transaction and a user’s account information by implementing these [dCVV] functionalities.” EX1003 ¶¶159-166.

All of these obviousness arguments, from both Petitioner and its expert, ignore (1) the purpose of Hammad, which has no applicability to the proposed Toomer-Grigg combination; and (2) the teachings of Toomer, which already describe a one-time use number (without having to resort to Hammad).

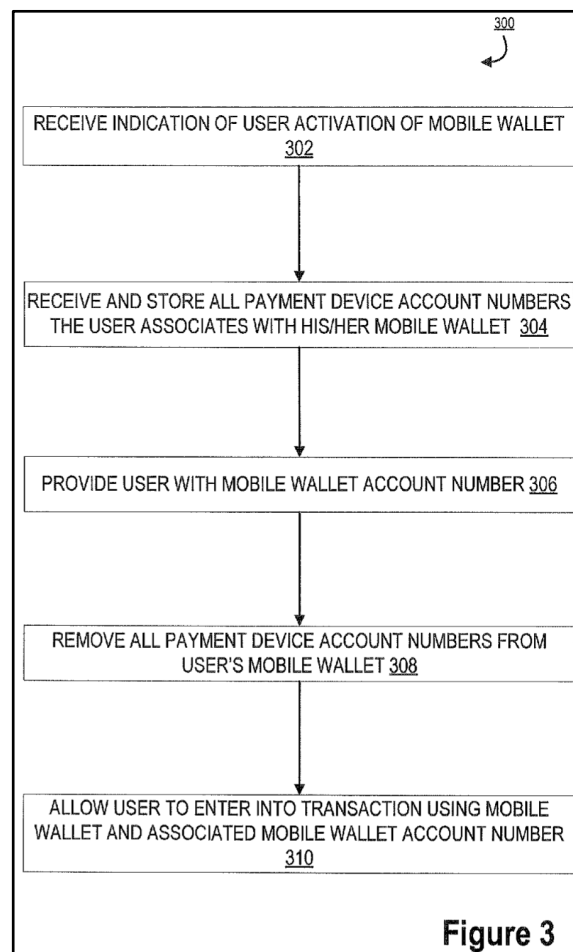
First, Hammad is directed *exclusively* to skimming, which is a problem concerning misuse and theft of the *actual* payment information. EX1006, 1:21-23

(skimming refers to “electronic copying of a card’s magnetic stripe data to create counterfeit cards”). Petitioner’s expert acknowledges this when discussing the background of Hammad, but never considers it in connection with the proposed combination. *Compare* EX1003 ¶¶98 with ¶¶159-166.

The reason this is important is that there is no skimming risk associated with the Toomer-Grigg combination that Petitioner proposes. Specifically, the Toomer-Grigg combination (as Petitioner proposes it) does not use the actual payment information (and if it did, it would not meet limitation 10(g) requiring use of “in the place of issuer provided payment information”).³ Not only does the Toomer-Grigg combination not use actual payment information, it doesn’t even store issued payment information on the device. Grigg specifically explains that “a mobile wallet utilizing the mobile wallet account number differentiation system may not have stored and/or have access to the actual financial accounts associated with payment devices on the mobile wallet.” EX1005, [0014]. As shown, for example, in Figure 3 of Grigg, after the user receives the mobile wallet account number, the system

³ See, e.g., Pet., 34 (“It would have been obvious to use the mobile wallet account number and dCVV in place of Toomer’s account number and other information (issuer provided payment information) in conducting a transaction.”) (emphasis in original).

removes all payment device account numbers from the user's mobile wallet. EX1005, FIG. 3, [0081] ("Once all of the payment device account numbers associated with the user's mobile wallet are stored and the user 202 has received the mobile wallet account number, the system may allow for the removal of all payment device account numbers from the user's mobile wallet, as illustrated in block 308."), *see also*, EX1005, [0074].



EX1005, FIG. 3.

Grigg is therefore an *alternative* solution to the problem of compromised actual payment information on a device (whether through skimming or other theft

or loss). Grigg contemplates removing the issued payment information from the device as a solution to this problem, in favor of a mobile wallet number. There is therefore no need for Hammad, which is solving for the exact same thing, albeit in a different way (using a dCVV). Petitioner and its expert never consider the purpose of each disclosure or the problem that each reference is solving for. Instead, they just regurgitate boilerplate obviousness positions about expectations of success, minimal work, and basic software modifications, etc. that have zero connection to the references and disclosures themselves. Pet. 31-32, EX1003 ¶¶160-161; *see also 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.”); *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15-17 (PTAB Aug. 24, 2022) (precedential) (finding that conclusory testimony that “does not cite to any additional supporting evidence or provide any technical reasoning to support [that testimony] ... is entitled to little weight”); *AT&T Servs., et al. v. Innovative Sonic Limited*, IPR2024-01143, Paper 15, 28, 38 (PTAB Feb. 11, 2025).

Petitioner and its expert briefly mention increased security (generally) with use of a dCVV, but never explain what security issue the dCVV would address when the payment information has already been removed from the device. Pet. 31-32,

EX1003 ¶¶160-161. In this situation, the dCVV of Hammad would do nothing more than increase complexity of the overall system, and use processing (and battery) power, without any specifically articulated security benefit.

Second, even if a POSITA would want to use a dynamic number (for some unspecified security reason), there is no reason they would look to the dCVV of Hammad given that Grigg already discloses a one-time use number. Specifically, Grigg already discloses that “the mobile wallet account number may be a one-time use account number for the mobile wallet.” EX1005, [0011], [0080]. To the extent a POSITA would have wanted a different number for each transaction, they could have used the one-time use mobile wallet account number of Grigg without having to resort to another combination or the additional cost and complexity of generating a dCVV on the device itself. Moreover, there is no reason that a POSITA would need to use the multiple “data elements” of Hammad. The point of using multiple data elements is because this makes it “highly unlikely that a skimmer can determine the dCVV.” EX1006, 4:48-49. In other words, the point of multiple data elements is to avoid reverse-engineering of the dCVV, which is “generated on the portable consumer device” (EX1006, 4:62) and which is vulnerable when simply based on a transaction “counter.” EX1006, 1:66-2:4. In Toomer, the mobile wallet account number comes from a remote system, and appears to be random. There is therefore no reason that a POSITA would need to base anything (coming from a remote

system) on multiple data elements, even assuming they would want to use a dCVV in Toomer-Grigg (for some redundant and unexplained security reason).

Third, it is worth noting that Petitioner’s obviousness combination picks and chooses from different references for fundamental parts of claim 10. In other words, this is not a situation where Petitioner has one reference that is close and is simply relying on a secondary references for trivial, routine concepts. Not one of Petitioner’s references discloses using multiple different pieces of replacement information. Two of them—Toomer and Hammad—envision using actual issued payment information in connection with the transaction (which is antithetical to the ’520 Patent claims). And Petitioner pulls a dynamic CVV from a reference (Hammad) that never envisions using a static device account number (or anything close to it), and suggests putting that Hammad disclosure together with a reference (Toomer) that never envisions any type of dynamic CVV (and doesn’t even mention a CVV at all). This is not how obviousness law works; it is not an exercise in pulling random disclosures from disparate references and asserting that because it could have been combined without much effort and would have improved “security” that a POSITA would have put them together. *See, e.g., InTouch Techs., Inc. v. VGo Commc’ns, Inc.*, 751 F.3d 1327, 1351 (Fed. Cir. 2014) (“A reason for combining disparate prior art references is a critical component of an obviousness analysis; ‘this

analysis should be made explicit.’’)) (quoting *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007)).

If anything, this approach illustrates improperly using the ’520 Patent as a blueprint in Petitioner’s obviousness challenge. *See, e.g., Ecolochem, Inc. v. S. Cal. Edison Co.*, 227 F.3d 1361, 1372 (Fed. Cir. 2000) (“In this case, the district court used the [] patent as a blueprint, with the Houghton process as the main structural diagram, and looked to other prior art for the elements present in the patent but missing from the Houghton process. The district court opinion does not discuss any specific evidence of motivation to combine, but only makes conclusory statements. Broad conclusory statements regarding the teaching of multiple references, standing alone, are not evidence.”) (cleaned up); *see also 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.”).

Petitioner simply fails to explain anything about the references or payment systems that would suggest this was a logical and obvious combination.

C. Petitioner’s Grounds Regarding Claim 1 and its Dependent Claims Fail for the Same Reasons as Claim 10

Petitioner’s Grounds that concern independent claim 1 and its dependents rely on the same Toomer-Grigg-Hammad combination and fail for the same reasons as explained above for Grounds 1 and 2.

Specifically, claim 1 of the ’520 Patent requires computer readable medium having instructions that cause an electronic device to perform operations comprising: “wirelessly receiving a static device account number” (limitation 1(k)) and “using said static device account number and said dynamically generating one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.” EX1001, 16:18-20, 16:30-33.

For these limitations, Petitioner simply incorporates by reference its discussion of elements 10(d) and 10(g). Pet., 52, 61.⁴ For all the same reasons as Patent Owner set forth above, Petitioner has likewise failed to meet its burden to show a reasonable likelihood of success for any claim with respect to Grounds 3-6.

⁴ Petitioner’s Petition does not even identify what it is deeming to be limitations 1(h)-1(n). Petitioner simply states that for limitations “1(h)-(n)” the Board should “See Ground 1, Claims 10(a)-(g).” Pet., 52. Patent Owner therefore presumes that, as Petitioner has defined it, Petitioner is taking the same position with limitation 1(h) as it does with limitation 10(a), and so on down the list.

D. Additional Reasons that Petitioner Has Failed to Meet Its Burden

Patent Owner has focused on a handful of glaring issues with Petitioner's 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 demonstrate the lack of a reasonable likelihood of success), including the following:

- Grigg is incompatible with a multi-network and multi-issuer payment system. It provides that a "system" provides a mobile wallet account number, but does not explain how it could issue separate mobile wallet account numbers for each payment device in a mobile wallet, when those payment devices span different networks (*e.g.*, Visa vs. Mastercard) and different issuing banks. Petitioner does not explain why a POSITA would look to this reference as a cross-network and cross-issuer solution (which Toomer is, as evidenced by Figure 3 showing multiple financial institutions in the financial network).
- Limitations 10(g) and 1(n) require using two separate pieces of replacement information—a static device account number and a dynamically generated one-time limited-use number. This is different than *each* of Toomer, Grigg, and Hammad. Every one of those references uses just a single piece of replacement information. Petitioner never addresses a reason why a POSITA would use two

pieces of replacement information, or the complexities associated with doing so.

- Grigg involves removing issued payment information (such as account information) from the electronic device. While this may be effective in solving Grigg's particular problem (concerning lost devices), it creates an additional problem, which is that sometimes a user needs to have their account information available in their device (such as when a merchant does not accept a mobile wallet account number). Petitioner never addresses this consideration or explain why a POSITA would use Grigg's teachings to create a system does not allow a user to access their actual payment information.

VII. CONCLUSION

For the reasons stated above, Petitioner's proposed combinations fail to disclose key limitations of the Challenged Claims of the '520 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 9,003 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)