

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. IPR2025-01146
U.S. Patent No. 10,339,520

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION.....	1
II. THE '520 PATENT.....	3
III. PETITIONER'S ALLEGED PRIOR ART.....	3
A. <i>Gill</i>	4
B. <i>Smith</i>	8
C. <i>Kay</i>	11
D. <i>Gomez</i>	11
E. Petitioner's Proposed Combinations.....	16
IV. LEVEL OF ORDINARY SKILL IN THE ART.....	17
V. ARGUMENT: THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD OF SUCCESS.....	17
A. Petitioner Fails to Show a Reasonable Likelihood of Success Regarding Ground 1.....	17
1. The <i>Gill-Smith-Kay</i> Combination Fails To Disclose A Dynamically Generated Number, As Required By Limitation 18(h).	18
2. Petitioner Fails To Show That It Would Have Been Obvious To Combine <i>Gill</i> , <i>Smith</i> , and <i>Kay</i>	24
B. Petitioner Fails to Show a Reasonable Likelihood of Success Regarding Ground 2.....	31
VI. CONCLUSION.....	35

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.</i> , 776 F.2d 281 (Fed. Cir. 1985)	21
<i>AT&T Servs. Inc. v. Innovative Sonic Ltd.</i> , IPR2024-01143, Paper 15 (PTAB Feb. 11, 2025).....	21
<i>In re Gurley</i> , 27 F.3d 551 (Fed. Cir. 1994)	28
<i>In re Kumar</i> , 418 F.3d 1361 (Fed. Cir. 2005)	20
<i>NearMap US, Inc. v. Pictometry Int’l Corp.</i> , IPR2024-00729, Paper 9 (PTAB Oct. 10, 2024).....	23
<i>Precision Cancer Techs. Inc. v. Oncoustics Inc.</i> , IPR2025-00242, Paper 7 (PTAB June 3, 2025)	20, 21
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	27
<i>Upjohn Co. v. Mova Pharm. Corp.</i> , 225 F.3d 1306 (Fed. Cir. 2000)	21
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022).....	21

Regulations

37 C.F.R. § 42.6(a)(3)	23
37 C.F.R. § 42.104(b)(4).....	23

PATENT OWNER’S EXHIBIT LIST

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

I. INTRODUCTION

On June 24, 2025, Apple Inc. (“Apple” or “Petitioner”) filed a Petition requesting *inter partes* review of claims 18-24 (“Challenged Claims”) of U.S. Patent No. 10,339,520 (“the ’520 Patent”) (EX1001), presenting two 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.

Petitioner’s Petition fails on the merits.

First, none of the references in **Ground 1**—using *Gill*, *Smith*, and *Kay*—disclose the requirement of limitation 18(h) that the identification and authorization information includes “dynamically generated limited-use number portions.”

Second, Petitioner has failed to show a motivation to combine or reasonable expectation of success for either **Ground 1 or 2** for several reasons. Initially, Petitioner’s primary reference (*Gill*) teaches that ATM transactions—to which *Gill* is directed—involve entirely different considerations than non-ATM transactions such as point-of-sale (“POS”) transactions. Indeed, that is the entire point of *Gill*: to address ATM-specific issues that were not addressed or obvious in view of other art (e.g., POS contactless payment transactions). And as explained below, *Gill* expressly teaches that ATM transactions are “vastly different” than “simple” POS transactions and further that, at the time of its disclosure, “presently known” POS contactless

payment technology was “ineffective for use with an ATM.” Despite these teachings—which neither Petitioner nor its expert address—Petitioner seeks to combine *Gill* with POS contactless payment references (such as *Smith*) that do not address any of these unique ATM-based considerations. As detailed below, Petitioner’s attempt fails.

Moreover, *Gill* already includes a security layer, as it requires a user to complete a verification step (*e.g.*, entering a PIN code). Petitioner and its expert likewise ignore this teaching, which results in a POSITA not having any reason to seek to add an additional layer of security by using *Smith*’s cryptograms that require a significantly more complicated payment network. And contrary to Petitioner’s arguments there are no gaps in *Gill* that would urge a POSITA to look to *Smith*.

Third, in **Ground 2**, Petitioner resorts to a fourth reference, *Gomez*, for what it couches as a more explicit disclosure of “dynamically generated limited-use number portion[s].” This combination makes even less sense. *Gomez* is directed to payment cards (not mobile devices with a “user interface,” as required by limitation 18(h)) and is specifically intended to solve security problems associated with in-store fraud when presenting a payment card to a merchant or at a point-of-sale terminal. None of these considerations exist with an ATM-based transaction. Petitioner never so much as addresses these considerations, which further demonstrate its Ground 2 fails to show a reasonable likelihood of success.

For these reasons, as those 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 '520 PATENT

The claims of the '520 Patent generally relate to payment systems and methods. The Challenged Claims in this Petition are directed to “facilitating and authorizing an automated teller machine (ATM) transaction.” EX1001, 18:11-12. In particular, the sole challenged independent claim (claim 18) is directed to a method of exchanging information between an electronic device and an ATM wherein a user can select functions from an electronic device, including “identification” and “authorizing information” and wirelessly exchange those operations with the ATM. The “identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions.” EX1001, 18:39-44 (limitation 18(h)).

III. PETITIONER’S ALLEGED PRIOR ART

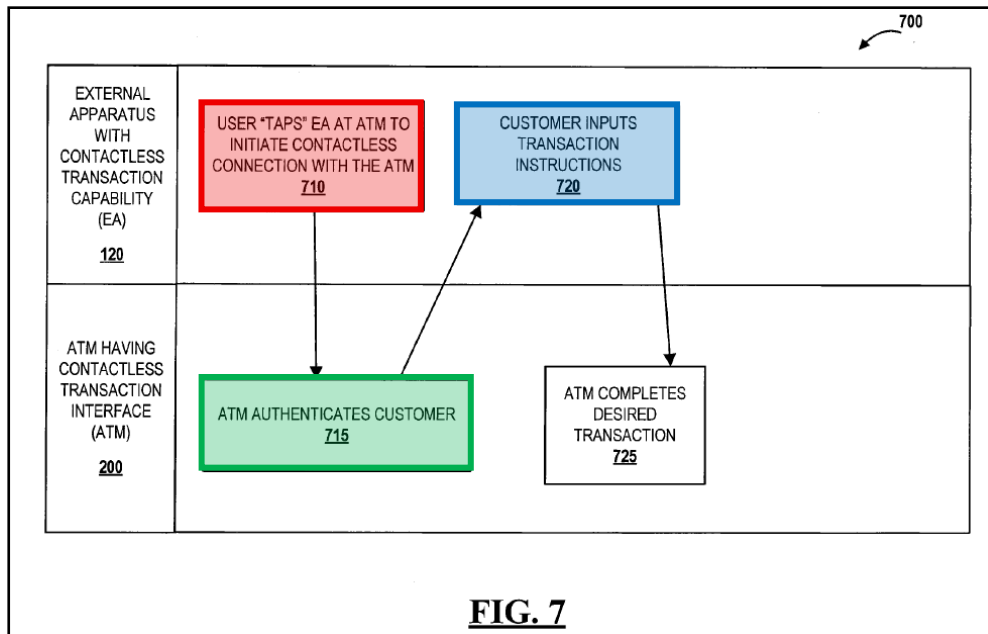
Petitioner relies upon four references in its Grounds (*Gill*, *Smith*, *Kay*, and *Gomez*). In Ground 1, Petitioner presents the combination of *Gill*, *Smith*, and *Kay* to challenge independent claim 18 and dependent claims 19-21 and 24. In Ground 2, Petitioner adds a fourth reference to the combination (*Gomez*) to challenge independent claim 18 and dependent claims 19-22 and 24.

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

A. *Gill*

U.S. Patent No. 9,098,846 ("*Gill*") describes systems and methods for performing contactless transactions at an ATM. *See* EX1004. "An ATM machine is provided that has been equipped with a contactless interface for interacting with an external apparatus such as a debit/credit card, mobile device, and/or contactless transmission equipped stickers." EX1004, Abstract.

Figure 7, reproduced below, depicts example interactions between an external apparatus 120 and an ATM in performing a contactless transaction (*e.g.*, via NFC), as taught in *Gill*:



EX1004, FIG. 7 (annotated).

As shown in Figure 7 of *Gill*, above, a user (customer) at **block 710** “taps the external apparatus 120 at the ATM 200 to initiate a contactless connection with the ATM,” *e.g.*, “by positioning the external apparatus 120 within close proximity of the contactless interface of the ATM 200.” EX1004, 14:1-8. At **block 715**, the ATM 200 “authentica[es] the customer” by requiring the user to present a valid credential such as a PIN. EX1004, 14:9-13. In some embodiments, rather than directly entering credentials at the ATM after establishing a connection, “the customer may first authenticate himself prior to the contactless connection being established” by “input[ing] authentication information ... and such transfer such data [sic] to the ATM 200 upon establishing the contactless connection.” EX1004, 14:13-20. The customer can further input instructions for the transaction at the external apparatus 120 (**block**

720), and the apparatus 120 in turn transmits the instructions to the ATM over the contactless connection (e.g., NFC). EX1004, 14:31-38, 17:56-62.

Gill also explains differences in the security associated with ATM and POS transactions resulting in the “presently known” POS contactless payment technology¹ being “ineffective for use with an ATM”:

As a general matter, automated teller machine (ATM) users have not enjoyed the benefits of contactless transactions, while numerous point-of-sale (POS) contactless payment terminals have been made available. This unavailability of contactless ATMs is largely due to security issues (actual and perceived) as well as systematic problems relating to the type of data that must be wirelessly relayed to an ATM as opposed to a simple payment terminal. *For instance, regarding security issues, in contrast to ATM transactions, POS contactless transactions do not require the entry of a personal identification number (PIN).* Indeed, generally, there is *no* personal account verification at all with the POS contactless payment terminals (e.g. no signature required). As a result (of zero verification), contactless payments are

¹ *Gill* claims priority to a non-provisional filed September 6, 2012 and provisional filed March 4, 2011. EX1004, Cover Page. That is before, for example, *Smith* (EX1005, Cover Page) and *Gomez* (EX1006, Cover Page). Moreover, as discussed below, both *Smith* and *Gomez* disclose POS contactless payment transactions.

generally limited as to the amount the transaction may be (e.g., generally \$100 or less). *As such, the POS contactless payment technology presently known is ineffective for use with an ATM.* Indeed, financial institutions (and their customers) do not wish to institute contactless ATM terminals that do not utilize any security verification prior to providing access to financial funds and personal financial records.

EX1004, 4:35-55 (emphases added). Thus, *Gill* makes clear that ATM transactions require a PIN code (a form of personal account verification), whereas POS transactions do not, and that this difference is significant.

Gill further explains the “vastly different”—which *Gill* also describes as “substantially different”—nature of ATM and POS payment transactions (the latter which are, per *Gill*, “simple”):

Furthermore, regarding the type of data transmitted (or the way the data is processed), *an ATM transaction is vastly different than a simple POS payment transaction.* With POS transactions, the transaction is processed as a “credit” transaction where the information simply must be processed in order for making a payment through a major credit provider. *Conversely, with ATM transactions, the transaction is generally a debit account transaction.* As used herein, a “debit account transaction” refers to ATM transactions directly related to a financial institution account. For instance, a debit account transaction includes

withdrawing funds, depositing funds, account balance inquiries, ordering related products such as checks, etc. Thus, *not only must an ATM be capable of receiving the account information, it must also be capable of processing the information in a manner such that the actual financial institution account is identified such that information specific to that account can be displayed and debit account transactions performed on the particular account.* Thus, the information processed and manner of processing in a debit account transaction is substantially different than a simple determination of whether the card is a valid major credit card.

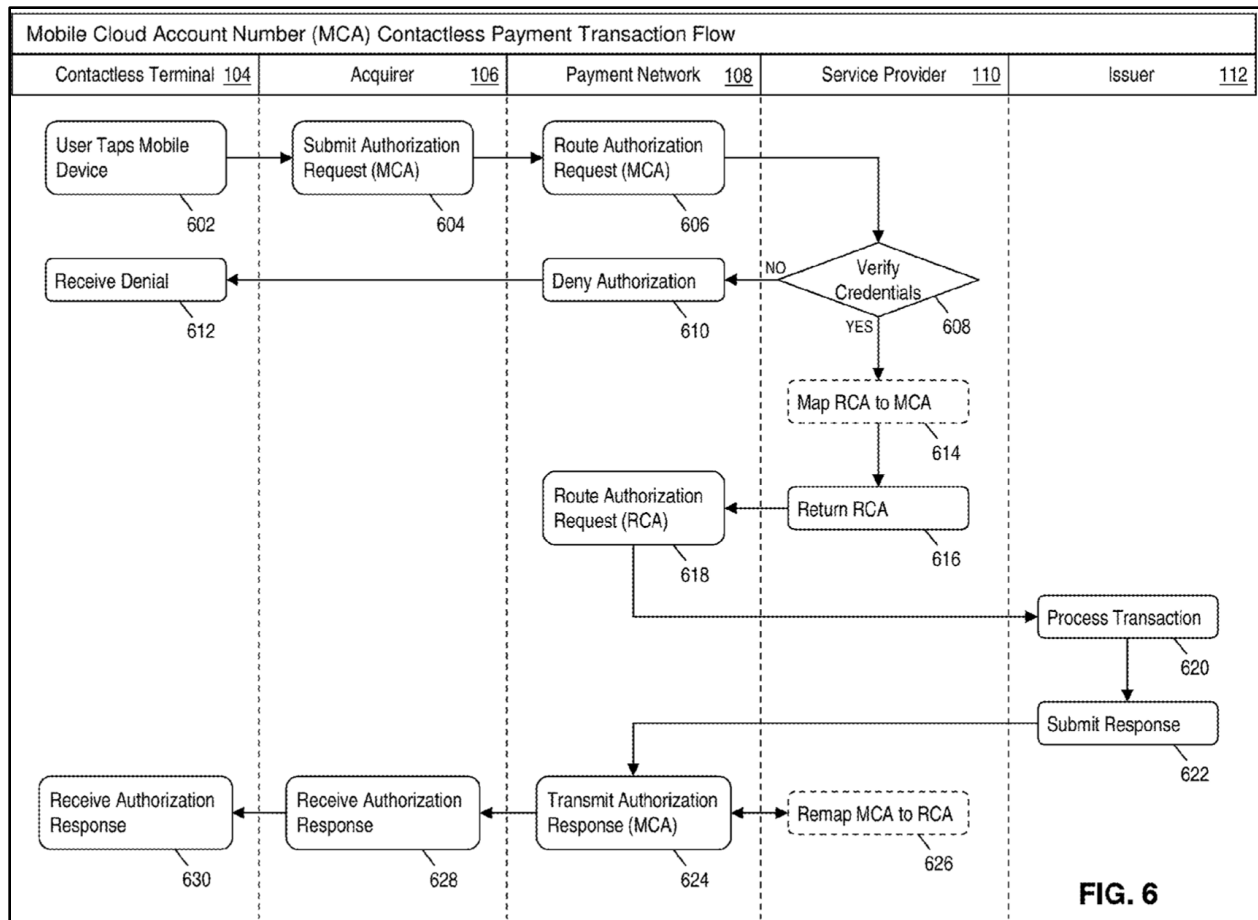
EX1004, 4:56-5:10 (emphases added).

Thus, in *Gill*, (i) at the time of *Gill*, “presently known” POS contactless payment technology was ineffective for use with an ATM; (ii) POS transactions are credit transactions, whereas ATM transactions are debit transactions; (iii) the type of data transmitted is vastly different; and (iv) ATMs must be capable of receiving and processing account information in a manner such that the actual financial institution account is identified. *Gill* again makes clear that these differences are significant.

B. *Smith*

U.S. Patent App. Pub. No. 2013/0232083 (“*Smith*”) describes techniques for conducting POS contactless payment transactions with a mobile device. EX1005, [0002], Abstract, [0035], FIG. 1. *Smith* discloses a mobile device that maintains

“mobile cloud accounts” in a virtual wallet, where any of the mobile cloud accounts can be used to conduct a POS contactless transaction. EX1005, [0032]-[0037]; *see also* EX1005, [0029] (“Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.”). “A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA).” EX1005, [0034]. “The RCA may correspond to a payment account issued to the user by an issuer 112,” and “[t]he MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.” EX1005, [0034]. “As a result, the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.” EX1005, [0034].



EX1005, FIG. 6.

As shown in Figure 6 (reproduced above), *Smith* discloses that a user initiates a POS contactless transaction by tapping his/her mobile device at a terminal. EX1005, [0066]-[0067]. The mobile device then transmits to the terminal “payment credentials” for the transaction, where the “payment credentials” include the “MCA” for the account desired for the transaction and a “payment cryptogram” such as “an authorization request cryptogram or dynamic card validation code.” EX1005, [0067]-[0068]. The payment credentials are received by an acquirer, which in turn forwards the credentials to a service provider that “verif[ies] (e.g., validate[s]) the

MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art.” EX1005, [0070]. Authorization for the transaction may be denied if the verification fails. EX1005, [0070]. However, “[i]f the credentials are successfully verified, then[] ... the service provider 110 may identify the RCA corresponding to the MCA” and returns the corresponding RCA to the payment network for further processing. EX1005, [0071]. “[T]he payment network 108 may route the authorization request with the RCA in place of the MCA to the issuer 112,” and “the issuer 112 may approve and process the financial transaction.” EX1005, [0072].

C. *Kay*

As Petitioner states in its bare-bones overview of U.S. Patent App. Pub. No. 2013/0124410 (“*Kay*”):

Kay generally describes techniques to “allow greater access to a banking platform via a mobile device.” [EX1006], Abstract. For example, “the customer can initiate a financial transaction using a mobile device,” and the mobile device provides a user interface with which the user can interact to facilitate the transaction.

Pet., 12.

D. *Gomez*

U.S. Patent No. 9,600,808 (“*Gomez*”) is specifically concerned with fraud risk associated with in-store payments at a point-of-sale (“POS”) terminal or with a

merchant present. EX1007, 4:64-5:2 (“[T]he risk is much higher regarding interactions with the merchant 406, whose employees may have access to the physical payment card ... and can either manually copy the information from the card, or discreetly use a credit card ‘skimmer’ to quickly capture all the information on the card’s magnetic stripe.”).

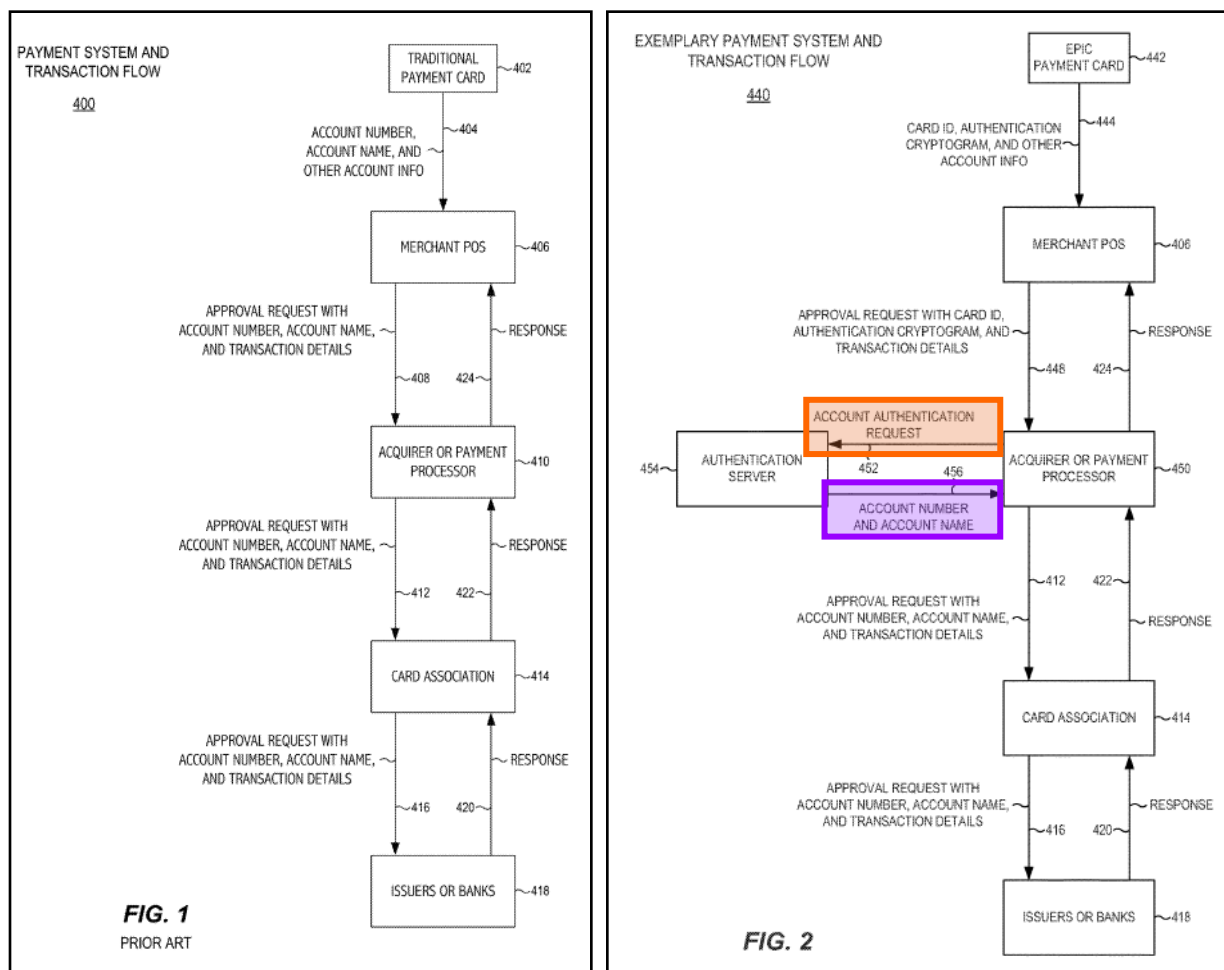
To address this in-person problem, *Gomez* discloses a proprietary payment card that incorporates an “EPIC account number” in place of a standard credit/debit card number. This substitute account number is for an EPIC user’s account and is used in payment transactions together with an “authentication cryptogram” that is generated at the time of a transaction and is designed to “greatly reduce[], if not virtually eliminate[]” theft and fraud. EX1007, 1:57-62.

More generally, *Gomez* is directed to a “payment card system” with a payment card that stores an “EPIC account number,” which *Gomez* describes as a “static payment card identifying number,” also called a “static payment card number,” that may represent either (i) a “live” credit or debit card number itself or (ii) “an identifying number for an EPIC account” that is, in turn, “linked [to] one or more live payment card accounts.” EX1007, Abstract, 2:19-39; 5:7-24, 6:7-22. *Gomez* further discloses “generat[ing] an authentication cryptogram for each attempted transaction” which is “based at least upon a seed value stored within the payment card and a temporal signal value, such as date/time of the attempted purchase.”

EX1007, 5:13-27. Unlike the EPIC account number—which is associated generally with an EPIC account, rather than a particular device—*Gomez* discloses that the “seed value is unique for each payment card.” EX1007, 7:27-31.

According to *Gomez*, when a card holder wishes to complete a transaction, the card holder “swipes the payment card through a POS terminal at the merchant just like a traditional magnetic stripe payment card,” and the information such as the public identifying number is ““left behind”” and “readily observable.” EX1007, 5:32-40; *see also* EX1007, 13:63-65 (“the payment card identifying number [is] visible to merchant employees and left behind after a transaction”).

Gomez compares a “traditional” “prior art” system (Figure 1, below left) with its disclosed system (Figure 2, below right). EX1007, 3:18-22, 3:65-67, 5:48-50.



EX1007, FIGs. 1-2 (annotated).

In effect, *Gomez*'s system adds a cryptogram into the account cardholder name field (*i.e.*, not in place of an issuer's payment information), and an associated substitute "account number" into an otherwise traditional system. The EPIC number and the cryptogram are later authenticated by an EPIC authentication server 454 (as in Figure 2 above). EX1007, 6:7-37. This can be seen by comparing the above Figures 1 and 2 from *Gomez* and the corresponding disclosure. An "account authentication request 452" (in orange) is created, which includes "the EPIC account number, the

date and time of the transaction, and the authentication cryptogram” and is sent to an “EPIC authentication server 454.” EX1007, 6:13-22 (annotated). The EPIC authentication server 454 “determines whether the authentication cryptogram is valid for the transaction, and if so, provides to the acquirer 450 an actual payment card account number and account name to use for processing the transaction.” EX1007, 6:23-27. Such determination is “accomplish[ed] by independently generating a ‘reference’ authentication cryptogram based upon the seed value corresponding to the EPIC account number, and based upon the date/time of the transaction (or other temporal signal value...).” EX1007, 6:27-32. “If the server-calculated reference authentication cryptogram matches the received authentication cryptogram generated by the EPIC card and provided to the merchant 406, then the authentication server 454 provides an actual payment card account number and account name to use for the transaction, and conveys this information in a response 456 [(in purple)] communicated back to the acquirer 450.” EX1007, 6:32-38 (annotated).

In addition, *Gomez* is not the smartphone / PDA type of device claimed in the ’520 Patent. *Gomez* makes no attempt to merge the features of a card and a smartphone, as does the ’520 Patent, such as the use of gestures to maintain security and avoid unwitting use, in order not to change the traditional point-of-sale infrastructure. *See, e.g.*, EX1007, 5:32-34 (“The card holder then swipes the payment

card through a POS terminal at the merchant *just like a traditional magnetic stripe payment card.*)” (emphasis added); 5:64-6:2 (“This account information 444 is communicated to the merchant 406 by swiping the payment card 442 through a magnetic card reader on a point-of-sale (POS) terminal (not shown). Since all the information is encoded using *standard fields*, a traditional POS terminal may be used without any required changes as a result of the encoding.”) (emphasis added). This is a specific teaching to a POSITA not to combine *Gomez*’s teaching with teachings relating to smartphone / PDA references. In other words, *Gomez* does not disclose (and teaches away from) a mechanism to use the disclosed system with a non-traditional POS terminal (including an ATM). For example, *Gomez* does not address *Gill*’s ATM-specific approach that “the actual financial institution account is identified such that information specific to that account can be displayed and debit account transactions performed on the particular account.” See EX1004, 4:56-5:20.

E. Petitioner’s Proposed Combinations

Petitioner’s proposed obviousness combination for both of its Grounds 1 and 2 is based on a combination of *Gill*, *Smith*, and *Kay* (additionally with *Gomez* in Ground 2).

Relevant to this Preliminary Response and as further discussed below, as best that Patent Owner can discern, Petitioner proposes that *Gill* is the primary reference for Ground 1, including its methods for performing contactless transactions at an

ATM, including interactions with an external apparatus. Pet., 16. Petitioner then proposes that it would have been obvious to “[a]pply[] Smith’s proposed use of payment credentials—including an MCA and payment cryptogram—in Gill’s system.” Pet., 18-27. Petitioner further proposes that it would have been obvious to apply the teachings of *Kay* for several user interface-related limitations. Pet., 31-40. For Ground 2, Petitioner further proposes that *Gomez* is further applied to the *Gill-Smith-Kay* combination, “such that the payment cryptogram would be generated using a temporal signal and cryptographic methods like those described in *Gomez*.” Pet., 58-66.

IV. LEVEL OF ORDINARY SKILL IN THE ART

For the purposes of this Preliminary Response only, Patent Owner does not dispute Petitioner’s definition of a person of ordinary skill as of the Critical Date (a “POSITA”).

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

A. Petitioner Fails to Show a Reasonable Likelihood of Success Regarding Ground 1.

Petitioner’s Ground 1 asserts that claims 18-21 and 24 are obvious over a combination a three-reference combination of *Gill*, *Smith*, and *Kay*. This combination fails because Petitioner has not met its burden of proof that limitation 18(h) in independent claim 18 is disclosed in these prior art references and further fails to demonstrate a motivation to combine *Gill* with *Smith*. Each of these is

dispositive of Petitioner’s Ground 1.

1. The *Gill-Smith-Kay* Combination Fails To Disclose A Dynamically Generated Number, As Required By Limitation 18(h).

Claim limitation 18(h) recites: “*wherein the identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions.*” Petitioner relies exclusively on *Smith* as disclosing this limitation, arguing that “[b]ased on *Smith*, it would have been obvious for the wireless exchange to involve transmission of a mobile card account number (MCA) and a payment cryptogram (*identification and authorizing information*) from a mobile device to a terminal.” Pet., 45 (emphasis in original); *see also* Pet., 45-48 (relying only on *Smith*). Petitioner further contends that *Smith*’s “MCA is a *statically generated limited-use number portion*,” Pet., 45 (emphasis in original), and that “according to *Smith*, the payment cryptogram (*dynamically generated limited-use number portions*) can be a ‘dynamic card validation code’ or an ‘authorization request cryptogram,’ either of which a POSITA would have understood and found obvious to be a dynamically generated limited-use numbers portion of the payment credentials.” Pet., 45 (emphasis in original).

However, *Smith* fails to disclose anything about this cryptogram, including whether and to what extent it is a “limited-use number” as required by limitation 18(h).

First, at best, *Smith* only discloses that the “payment cryptogram” can be a “dynamic card validation code.” EX1005, [0067], [0096], [0103]. *Smith* says nothing more about this “code”; it does not say *how* it is generated, whether and to what extent it changes from one transaction to another, or, for that matter how it could be validated via the claimed ATM machine to authorize a transaction.

Petitioner concedes (in Ground 2) that “Smith does *not* expressly disclose all details as to how the payment cryptogram would be made to change across transactions or how the cryptogram would be calculated.” Pet., 56 (emphasis added). Nonetheless, Petitioner asserts (in Ground 2) that “the use of dynamic cryptograms in electronic transaction systems had been known for many years before the Critical Date of the ’520 Patent.” Pet., 56. In other words, Petitioner effectively concedes that *Smith* does *not* literally disclose that the cryptogram of Smith is a “dynamically generated limited-use number portion” (despite seemingly doing so in Ground 1).²

All that *Smith* discloses is a “cryptogram,” or “dynamic card validation code, generated based on at least a portion of the mobile cloud account data stored in the secure element.” EX1005, [0067]. *Smith* does not say whether or to what extent this

² For ease of understanding that Petitioner’s arguments concerning *Smith* regarding limitation 18(h), Patent Owner discusses in this Section Petitioner’s assertions regarding *Smith* as to both Grounds 1 and 2.

is limited-use. Nor can Petitioner’s expert fill the gap. Indeed, the cited portion of Petitioner’s expert’s declaration consists of a single conclusory sentence that lacks any citation to evidence or a prior art reference. Pet., 56; EX1003 ¶194.

Smith also does not enable its disclosure of a “dynamic card validation code,” meaning it is insufficient as a matter of law to render claim 18 obvious. *In re Kumar*, 418 F.3d 1361, 1368 (Fed. Cir. 2005) (“Although published subject matter is ‘prior art’ for all that it discloses, in order to render an invention unpatentable for obviousness, the prior art must enable a person of ordinary skill to make and use the invention.”). Indeed, Petitioner includes Ground 2 entirely for this reason—to address perceived holes with *Smith*’s purported disclosure of “dynamically generated limited-use number portions.”

Second, and notwithstanding the above, Petitioner cites paragraph [0067] in *Smith* and wrongly argues (in Ground 1) that “Smith specifically explains that the payment cryptogram is ‘generated’ for each transaction, ‘based on mobile cloud account data’ (*limited-use*)—in contrast to the MCA which is read from memory of the device.” Pet., 46 (purporting to quote EX1005, [0067]; emphasis in original). But the cited paragraph in *Smith* does not support Petitioner’s contention. See EX1005, [0067]. Petitioner’s expert asserts the same thing, verbatim, without additional evidence or analysis. EX1003 ¶177. Such unsupported, conclusory testimony should be afforded little, if any, weight. See, e.g., *Precision Cancer Techs. Inc. v. Oncoustics*

Inc., IPR2025-00242, Paper 7, 15-16 (PTAB June 3, 2025); *AT&T Servs. Inc. v. Innovative Sonic Ltd.*, IPR2024-01143, Paper 15, 27, 38 (PTAB Feb. 11, 2025); *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15-17 (PTAB Aug. 24, 2022) (precedential); *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)).

Not only does Petitioner misquote *Smith* at paragraph [0067], but this paragraph states, in full (emphasis added to show the sentence that Petitioner misquotes):

In step 602, the user 302 may “tap” the contactless terminal 104 using the mobile device 102 with payment credentials loaded into the mobile cardlet in the secure storage 210. The term “tapping” may refer to the transmission of payment credentials via near field communication from the mobile device 102 to the contactless terminal 104 due to the close proximity of the mobile device 102 to the terminal 104, which sometimes may result in the mobile device 102 physically tapping the terminal 104. ***The payment credentials may include a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code, generated***

based on at least a portion of the mobile cloud account data stored in the secure element 210. The contactless terminal 104 may forward the payment credentials, including the MCA and payment cryptogram, to the acquirer 106, who may then submit an authorization request including the MCA and payment credentials to the payment network 108 in step 604.

EX1005, [0067] (emphasis added).

As made plain from the above excerpt, all paragraph [0067] actually discloses is that the payment credentials (1) may include a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code, and (2) are generated based on at least a portion of the mobile cloud account data stored in the secure element. EX1005, [0067]. *Smith* does not say how frequently the code is updated, or whether it is “limited-use” as required by limitation 18(h) of claim 18.

Perhaps recognizing this failure, Petitioner, relying solely on expert opinion, argues (for Ground 1) that “[t]he significance of the cryptogram having a dynamic, limited-use would have been apparent to a POSITA, as it was commonly understood that updating the cryptogram, such as a dynamic validation code, on a frequent basis (e.g., with each transaction or some other period of time) protects against the risk of payment credentials (including the MCA and cryptogram) from a prior transaction being reused by an illicit actor to conduct a fraudulent transaction with the same credentials.” Pet., 47 (citing EX1003 ¶178). Petitioner’s expert cross-references

another section of his declaration that generally discusses certain other references that are *not* included, discussed, or cited as part of the Petition (EX1003 ¶178),³ which amounts to an improper incorporation by reference. *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)). Accordingly, Patent Owner respectfully submits that Petitioner’s reliance on its expert for arguments and evidence not in the Petition should be disregarded. *See id.* (“We decline to sift through [the expert’s] declaration in order to find the arguments that may support Petitioner’s challenge.”). But regardless, such alleged general knowledge is not only conclusory, it fails to “specify where each element of the claim is found *in* the prior art patents or printed publications relied upon” (namely, that *Smith* discloses limitation 18(h)). *See* 37 C.F.R. §42.104(b)(4) (emphasis added); *cf.*

³ Petitioner never discusses or cites any such reference (or the corresponding paragraphs from its expert’s declaration) in its 13,197-word Petition (which is one of two parallel Petitions Petitioner filed challenging the ’520 Patent). *See also Apple Inc. v. CardWare Inc.*, IPR2025-01145, Paper No. 1 (PTAB filed Jun. 24, 2025) (13,267-word Petition challenging claims 1-17).

Memorandum entitled “Enforcement and Non-Waiver of 37 C.F.R. § 42.104(B)(4) and Permissible Uses of General Knowledge in Inter Partes Reviews” (July 31, 2025).⁴

2. Petitioner Fails To Show That It Would Have Been Obvious To Combine *Gill*, *Smith*, and *Kay*.

Petitioner argues that it would have been obvious to combine *Gill*, *Smith*, and *Kay*. Pet., 21-27.⁵ Not so. As discussed below, it would not have been obvious for a POSITA to add the teachings of *Smith* to *Gill* for at least three reasons. First, *Gill*—which focuses on ATM transactions—explicitly teaches away from using art related to POS transactions, like *Smith*. Second, *Gill* includes a security layer, as it requires a user to complete a verification step (*e.g.*, entering a PIN code); thus, a POSITA would not seek to add an additional layer of security by using *Smith*’s cryptograms that require a significantly more complicated payment network. Third, contrary to

⁴ Patent Owner acknowledges that this Memorandum applies to “any petition for IPR filed on or after September 1, 2025,” but respectfully submits that the underlying principles and rule on which it is based are nonetheless applicable even without the specific Memorandum.

⁵ Petitioner applies the same reasoning to both Grounds 1 and 2. Thus, Petitioner’s failure—as explained in this Section V.A.2 is dispositive of both Grounds. *See also* Section V.B below (noting same).

Petitioner’s arguments that there are gaps in *Gill* that would urge a POSITA to look to *Smith*, no such gaps exist.

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

First, as summarized in Section III.A above, *Gill* teaches away from, and expressly discourages, the combination of *Gill* and *Smith*. As explained above, *Gill* focuses on ATM transactions, whereas *Smith* focuses on POS transactions. Compare EX1004, Fig. 1, with EX1005, Fig. 1; see *supra* Section III.A-B. As *Gill* explains (and summarized above in Section III.A), there are critical distinctions between ATM transactions, on the one hand, and POS contactless payment transactions, on the other.

To begin, *Gill* explains differences in the security associated with ATM and POS transactions resulting in “presently known” POS contactless payment technology⁶ being “ineffective for use with an ATM”:

As a general matter, automated teller machine (ATM) users have not enjoyed the benefits of contactless transactions, while numerous point-of-sale (POS) contactless payment terminals have been made available. This unavailability of

⁶ Again, *Gill* claims priority to a non-provisional filed September 6, 2012, and a provisional filed March 4, 2011. EX1004, Cover Page. *Smith* claims priority to a non-provisional filed March 1, 2013, and a provisional filed March 1, 2012.

contactless ATMs is largely due to security issues (actual and perceived) as well as systematic problems relating to the type of data that must be wirelessly relayed to an ATM as opposed to a simple payment terminal. *For instance, regarding security issues, in contrast to ATM transactions, POS contactless transactions do not require the entry of a personal identification number (PIN).* Indeed, generally, there is *no* personal account verification at all with the POS contactless payment terminals (e.g. no signature required). As a result (of zero verification), contactless payments are generally limited as to the amount the transaction may be (e.g., generally \$100 or less). *As such, the POS contactless payment technology presently known is ineffective for use with an ATM.* Indeed, financial institutions (and their customers) do not wish to institute contactless ATM terminals that do not utilize any security verification prior to providing access to financial funds and personal financial records.

EX1004, 4:35-55 (emphases added).

Gill further explains that ATM and POS transactions are very different from one another, requiring “vastly different” data to be transmitted and processed and have vastly different security issues. EX1004, 4:56-5:10. As *Gill* notes, “the type of data transmitted (or the way the data is processed), an ATM transaction is *vastly different* than a simple POS payment transaction.... Thus, the information processed and manner of processing in a debit account transaction is *substantially different* than

a simple determination of whether the card is a valid major credit card.” EX1004, 4:56-5:20 (emphasis added). *Gill* further explains that unlike a POS, “not only must an ATM be capable of receiving the account information, it must also be capable of processing the information in a manner such that the actual financial institution account is identified such that information specific to that account can be displayed and debit account transactions performed on the particular account.” EX1004, 4:56-5:20. And with respect to the differences in security challenges between ATM and POS transactions, *Gill* explains that “in contrast to ATM transactions, POS contactless transactions do *not* require the entry of a personal identification number (PIN).” EX1004, 4:35-55 (emphasis added).

Petitioner’s proposed combination does not account for *any* of *Gill*’s teachings distinguishing between ATM and POS transactions (discussed in this Section V.A.2, as well as in Section III.A above) and instead assumes (without any analysis or evidence) that a POSITA would have sought to apply *Smith*’s POS contactless payment transaction teachings to *Gill*’s ATM transaction system. There is simply no reason that a POSITA would have done so—especially considering that *Gill* expressly teaches the problems and incompatibility of doing so, none of which are addressed by Petitioner. Accordingly, Petitioner has failed to show motivation to combine, or reasonable expectation of success in combining, *Smith* and *Gill*, and its proposed combination thus fails. *See also, 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.”); *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994) (“A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.”).

Second, Petitioner’s argument that *Smith*’s combination with *Gill* would allow a POSITA to “realize predictable security improvements,” Pet., 23-24, is based on a false premise, and therefore also fails. In support, Petitioner argues that “security enhancements stemming from use of both an MCA and a cryptogram in contactless ATM transactions (*e.g.*, credit/debit transactions at an ATM) would have furthered *Gill*’s objectives of providing for secure transactions with an ATM.” Pet., 25-26. However, *Gill* explains that ATM transactions require “security verification,” whereas POS transactions, like in *Smith*, do not. EX1004, 4:35-55. Thus, *Gill* is concerned with conveying a PIN code to an ATM securely, which provides a security verification for the transaction, whereas *Smith* is concerned with hiding a real card number from a POS terminal precisely because there is no security verification at a POS terminal. *Compare* EX1004, 4:35-55 (*Gill* distinguishing ATM transactions

from POS transactions on the basis that “POS contactless transactions do not require the entry of a personal identification number (PIN),” and explaining that “financial institutions (and their customers) do not wish to institute contactless ATM terminals that *do not utilize any security verification prior to providing access to financial funds* and personal financial records”), with EX1005, [0034] (explaining that *Smith*’s mobile device does not store the real card account number, which “reduc[es] the potential for fraud.”) (emphasis added). Thus, while both *Gill* and *Smith* are concerned about security of transactions, each reference takes a strikingly different approach—*Gill* focuses on security verifications whereas *Smith* focuses on obscuring the real card number from the POS. Petitioner fails to explain why a POSITA would find *Gill*’s security verification step insufficient such as to warrant combining it with *Smith*, which would require a significantly more complicated payment network.

Moreover, in an attempt to buttress this obviousness argument, Petitioner argues that “cryptograms in payment devices were common,” Pet., 25; but this only makes the invention less obvious. Since cryptograms were around long before the invention, *Gill* would have included them if it was an obvious and useful addition, in the context of ATM transactions. That *Gill* failed to include cryptograms demonstrates that the combination of *Gill* and *Smith* is *not* obvious.

Third, Petitioner’s argument that it would have been obvious for a POSITA to combine *Gill* and *Smith* because “Gill does not provide much detail about the

specific information conveyed by the mobile device in a transaction request, or how such information might be secured and deployed to identify a desired payment account,” Pet., 22, also fails. Based on this alleged gap, Petitioner contends that “[i]t would have been obvious to a POSITA to consider references with additional implementation details and modify Gill in view of Smith such that the mobile device in Gill would be adapted to convey to the ATM at least ‘payment credentials’ for a requested transaction,” to fill gaps in *Gill*’s disclosure. Pet., 22. Not so. There is no gap in *Gill*’s disclosure, and no reason for a POSITA to look to *Smith*. In fact, Petitioner relies on these alleged gaps in *Gill*’s disclosure in its Petition. For example, the Petition argues that *Gill*’s “mobile device provides ‘payment vehicle data’ to the ATM terminal via a contactless/wireless connection when a user ‘taps’ the mobile device at the ATM.” Pet., 18 (citing EX1004, 5:11-20). Petitioner also string cites a series of quotes from *Gill* to assert that *Gill* discloses the user’s “account information, for example, account number, name, expiration date, debit/credit, etc.).” Pet., 18 (emphasis omitted). Moreover, as Petitioner also notes, *Gill* discloses that “typical content to be transferred from the external apparatus 120 includes *data identifying the financial account associated with the external apparatus*.” Pet., 18 (citing EX1004, 13:41-46; emphasis in original). Thus, *Gill* has no gap; rather, *Gill* describes a *complete* set of information needed to initiate an *ATM* transaction, and as such, there would have been no reason for a POSITA to look to a

POS reference like *Smith*. Moreover, Petitioner’s argument that *Gill* and *Smith* “operate in highly similar contexts,” Pet., 22, is not sufficient to explain why a POSITA would want to look to *Smith* (a non-ATM reference), and much less why a POSITA would want to combine *Gill* and *Smith*. And regardless, it is contradicted by the express disclosure in *Gill* discussed above in this Section V.A2 and in Section III.A.

Therefore, for these reasons, Petitioner has failed to meet its burden on claim 18 and Ground 1. This is dispositive of Ground 1, as the remaining Challenged Claims depend from independent claim 18.

B. Petitioner Fails to Show a Reasonable Likelihood of Success Regarding Ground 2.

Petitioner’s second ground asserts that claims 18-24 are obvious over a combination of *Gill*, *Smith*, *Kay*, and *Gomez*. This ground is unavailing for the same reasons as Ground 1, and further for the reasons set forth below.

In this ground, Petitioner argues that it would have been obvious to modify the cryptogram in the *Gill-Smith-Kay* combination to change temporally based on *Gomez*’s “temporal signal.” Pet., 56-60. As an initial matter, a POSITA would not have combined *Gill*, *Smith*, and *Kay* for the reasons set forth above. *See supra* V.A.2. Thus, the *Gill-Smith-Kay-Gomez* combination fails for the same reasons.

Moreover, as discussed below, it would not have been obvious for a POSITA to add the teachings of *Gomez* to the *Gill-Smith-Kay* combination for at least three

reasons. First, the *Gill-Smith-Kay* combination has two layers of security, and a POSITA would not have been motivated to add a third layer of security through *Gomez*. Second, just like *Smith*, *Gomez* is directed to a POS payment system, whereas *Gill* is directed to an ATM payment system, and those two systems are vastly different, as *Gill* itself indicates. Third, *Gomez* is directed to a smart payment card in a traditional format, whereas *Gill*, *Smith*, and *Kay* are all directed to mobile device payment systems, and Petitioner makes no attempt to explain why, or how, a POSITA would consider modifying the three-reference *Gill-Smith-Kay* combination directed to conducting payments on a smartphone with the teachings of *Gomez* directed to a traditional payment card.

Patent Owner addresses these issues below.

First, Petitioner argues that a POSITA would have known many ways in which a cryptogram like *Smith*'s could be generated so as to provide a unique value for each transaction. Pet., 56. However, Petitioner's argument fails to explain *why* a POSITA would have been motivated to seek out an additional reference to modify *Smith*'s cryptograms to change temporally, or how this change would have been implemented.

Assuming that the *Gill-Smith-Kay* combination was obvious (which it is not), a POSITA would have a system that has two layers of security: (i) a security verification, such as a PIN code, and (ii) an obscured real card number. *See supra*

Section V.A. Petitioner fails to explain why a POSITA would then trade increased complexity for a third layer of security by making the cryptogram change based on *Gomez*'s "temporal signal." Pet., 58-59. While Petitioner argues that a "POSITA would have sought to use a dynamically changing temporal signal in calculation of the cryptogram (along with a cryptographic technique such as hashing) to ensure that the cryptogram produced in each transaction would vary from prior cryptograms in an unpredictable manner, thereby frustrating the ability of illicit actors to exploit an MCA and cryptograms from prior transactions to later consummate a fraudulent transaction," Pet., 59, this fails to explain why a POSITA would seek this additional layer of security beyond the specific context of *Gomez*, which is focused entirely on the fraud risk *at the point-of-sale location*.

Specifically, *Gomez* relies on an authorization server to validate the cryptogram and the EPIC payment account number. EX1007, 6:23-28. *Gomez*'s system works because the same entity controls both the smart payment card and the authorization server such that the cryptograms and EPIC payment account information provided by the payment card can be synced and validated by the authorization server without further intervention; they are both able to "know" the same seed value, temporal signal, and cryptographic algorithm. EX1007, 6:23-28. Thus, adding *Gomez* to the *Gill-Smith-Kay* combination would require an authentication server for syncing and validating *Gomez*'s cryptogram. As such, there

is no easy solution or modification for Petitioner’s re-imagined mobile phone based on the four- reference combination that would purportedly be obvious to a POSITA and used to conduct an ATM transaction. This alone shows that the four-reference, *Gill-Smith-Kay-Gomez* combination is the product of impermissible hindsight and must be rejected.

Second, even if a POSITA wanted to add an additional layer of security to *Gill*, a POSITA would not look to *Gomez*. Just like *Smith*, *Gomez* is concerned with POS transactions, which as explained in *Gill* (*supra* Sections III.A, V.A), are vastly different from ATM transactions. Thus, for the same reasons as explained above in Sections III.A. and V.A., *Gill* teaches away from, and expressly discourages, the combination of *Gill* and *Gomez* (like *Smith*, another POS transaction reference). Moreover, *Gomez* is also an already-complete solution that depends upon a *Gomez*-specific authorization server.

Third, Petitioner makes no attempt to explain why, or how, a POSITA would consider modifying the three-reference *Gill-Smith-Kay* combination directed to conducting payments on a smartphone with the teachings of *Gomez* directed to a traditional payment card. *See, e.g.*, EX1007, 5:32-34 (“The card holder then swipes the payment card through a POS terminal at the merchant *just like a traditional magnetic stripe payment card.*”) (emphasis added); 5:64-6:2 (“This account information 444 is communicated to the merchant 406 by swiping the payment card

442 through a magnetic card reader on a point-of-sale (POS) terminal (not shown). Since all the information is encoded using standard fields, *a traditional POS terminal may be used without any required changes* as a result of the encoding.”) (emphasis added).

Therefore, for these reasons, Petitioner has failed to meet its burden on claim 18, which is dispositive of Ground 2.

VI. 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 7,027 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

I hereby certify that the foregoing Patent Owner's Preliminary Response and Exhibits listed on the List of Exhibits were served on October 10, 2025, via electronic mail upon counsel of record for Petitioner at the following email addresses:

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)