IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner

v.

CARDWARE INC.,
Patent Owner

IPR2025-01513
Patent 10,339,520

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

Page

I. Introduction 1

II. The '520 Patent 5

III. Petitioner's Alleged Prior Art 7

A. Law 7

B. Gomez 13

C. Gill 19

D. Smith 23

E. Kay 26

IV. Level of Ordinary Skill in the Art 27

V. Claim Construction 27

A. Static Device Account Number 27

VI. The Petition Fails to Establish a Reasonable Likelihood of Success as to Any Challenged Claim 28

A. Petitioner Fails to Show a Reasonable Likelihood of Success for Grounds 1A-1B. 28

1. The Petition Does Not Comply with 37 C.F.R. § 42.104(b)(3) Because Petitioner Does Not Explain Why it is Taking Different Claim-Construction Positions In Its IPR Petition and District Court or Using Patent Owner's Alleged Constructions.. 28

2. A POSITA Would Not Have Substituted Gomez's EPIC Payment Account Number into Law's System Because It Would Reduce Security Measures of Law and Leave Law Vulnerable to "Replay Attacks" and Other Unauthorized Access Attempts 39

3. Petitioner Fails to Meet its Burden of Showing that its Proposed Combination has a "Static *Device* Account Number" that is Wirelessly Received as Required by Limitations [10.d] and [10.g]. 49

B. Petitioner Fails to Show a Reasonable Likelihood of Success for Ground 2A. 59

1. Petitioner's Ground 2A Rehashes the Same Four-Reference Combination Used in a Recently Denied Petition Challenging the Same Claims. 59

2. Petitioner Fails to Show That It Would Have Been Obvious to Combine Gill, Smith, and Kay. 60

3. Petitioner Fails to Show That It Would Have Been Obvious to Add Gomez to the Gill-Smith-Kay Combination. 67

VII. Conclusion 71

TABLE OF AUTHORITIES

Page(s)

Cases

Am. Airlines, Inc. v. Intell. Ventures I LLC,
IPR2025-01055, Paper 11 (PTAB Nov. 11, 2025) 33, 34

AT&T Servs., Inc. v. Innovative Sonic Ltd.,
IPR2024-01143, Paper 15 (PTAB Feb. 11, 2025) 41

CardWare Inc. v. Google LLC,
Case No. 7:24-cv-00278 (W.D. Tex.) 34, 35, 37

In re Gurley,
27 F.3d 551 (Fed. Cir. 1994) 63

Precision Cancer Techs. Inc. v. Oncoustics Inc.,
IPR2025-00242, Paper 7 (PTAB June 3, 2025) 40

Revvo Techs., Inc. v. Cerebrum Sensor Techs., Inc.,
IPR2025-00632, Paper 20 (Director Nov. 3, 2025) ..... *passim*

Tesla, Inc. v. Intell. Ventures II LLC,
IPR2025-00340, Paper 18 (Director Nov. 5, 2025) ..... *passim*

TQ Delta, LLC v. Cisco Sys., Inc.,
942 F.3d 1352 (Fed. Cir. 2019) 63

Xerox Corp. v. Bytemark, Inc.,
IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022) 41

Regulations

37 C.F.R. § 42.11 33

37 C.F.R. § 42.100(b) 32

37 C.F.R. § 42.104(b)(3) ..... *passim*

83 Fed. Reg. 51,340 (Oct. 11, 2018) 31

PATENT OWNER'S UPDATED EXHIBIT LIST

No.	Exhibit Description
2001	Memorandum for Memorandum for Director Institution of AIA Trial Proceedings, dated October 17, 2025
2002	Interim Director Discretionary Process *available at* https://www.uspto.gov/patents/ptab/interim-director-discretionary-process
2003	First Agreed Scheduling Order in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2004	Complaint in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2005	Order and Advisory in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Nov. 5, 2024)
2006	Order Denying Defendants' Motion to Stay in *Quantum Imaging, LLC v. Sony Interactive Entm't Inc.*, No. 1:23-cv-1212-ADA-DTG (W.D. Tex. Dec. 4, 2024) (Gilliland)
2007	Agreed Scheduling Order in *CardWare Inc. v. Apple Inc.*, No. 1:25-cv-00446-ADA (W.D. Tex. May 20, 2025)
2008	Complaint in *CardWare Inc. v. Apple Inc.*, No. 1:25-cv-00446-ADA (W.D. Tex. Nov. 4, 2024)
2009	Standing Order Governing Proceedings (OGP)—Patent Cases for cases before Judge Albright (dated Mar. 5, 2025)
2010	Report and Recommendation Denying The Defendants' Motion to Dismiss in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Aug. 15, 2025)
2011	Order Adopting Report and Recommendation Denying The Defendants' Motion to Dismiss in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Sept. 3, 2025)
2012	Order Denying the Defendant's Motion to Transfer Venue to the Northern District of California in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Aug. 7, 2025)
2013	Claim Construction Order in *CardWare Inc. v. Apple Inc.*, No. 1:25-cv-00446-ADA (W.D. Tex. Aug. 29, 2025)
2014	Email from counsel for Petitioner to counsel for Patent Owner, dated Sept. 4, 2025
2015	Defendant Google LLC's Invalidity Contentions in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Apr. 3, 2025)

No.	Exhibit Description
2016	Exhibit I to Defendant Google LLC's Invalidity Contentions in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Sept. 18, 2025)
2017	DocketNavigator Time to Trial Statistics for Patent Cases in the Western District of Texas
2018	Defendants' Notice of Subpoena to Google in *CardWare Inc. v. Samsung Elecs. Co., Ltd.*, No. 2:22-cv-00141-JRG-RSP (E.D. Tex. Feb. 2023)
2019	Letter from CardWare, Inc. to Google LLC dated October 10, 2023 "RE: Patent Portfolio of CardWare Inc."
2020	Proof of Delivery to Apple Inc. for Letter from CardWare, Inc. to Google LLC dated October 10, 2023 "RE: Patent Portfolio of CardWare Inc."
2021	Petition for *Inter Partes* Review of Pat. 10,339,520 in IPR2023-00210, by Petitioner Samsung Electronics Co., Ltd.
2022	Notice of Order Denying Institution in IPR2025-01145, IPR2025-01146, IPR2025-01147, IPR2025-01148, IPR2025-01149, IPR2025-01150, IPR2025-01151, IPR2025-01152
2023	Defendant Google LLC's Objections to Claim Construction Memorandum and Order, Dkt. 105, filed in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. Sept. 11, 2025)
2024	Defendant Google LLC's Claim Construction Brief, Dkt. 58, filed in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. May 22, 2025)
2025	Joint Claim Construction Statement, Dkt. 85, filed in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. July 15, 2025)
2026 [*New*]	Petition for *Inter Partes* Review of Pat. 10,339,520 in IPR2025-01146, by Petitioner Apple Inc.
2027 [*New*]	Plaintiff CardWare Inc.'s Responsive Claim Construction Brief, Dkt. 63, filed in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. June 12, 2025)
2028 [*New*]	Defendant Google LLC's Reply Claim Construction Brief, Dkt. 71, filed in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. June 26, 2025)
2029 [*New*]	Plaintiff CardWare Inc.'s Sur-Reply Claim Construction Brief, Dkt. 83, filed in *CardWare Inc. v. Google LLC*, No. 7:24-cv-00278-DC-DTG (W.D. Tex. July 10, 2025)
2030 [*New*]	Decision Denying Institution of *Inter Partes* Review in *Samsung Elecs. Co., Ltd. v. CardWare, Inc.*, IPR2023-00210, Paper 13 (PTAB June 13, 2023)

I. INTRODUCTION

The Director should deny institution of the Petition (Paper 1) challenging claims 10-24 ("Challenged Claims") of U.S. Patent No. 10,339,520 (the "'520 Patent"). Petitioner both failed to comply with 37 C.F.R. § 42.104(b)(3) and to meet its burden of demonstrating a reasonable likelihood of success that its prior-art combinations render obvious any Challenged Claim.

For **Grounds 1A-1B** challenging independent claim 10 and dependent claims 11-17, Petitioner failed to comply with 37 C.F.R. § 42.104(b)(3) for two independent reasons. First, Petitioner is taking contradictory (and unexplained) claim construction positions in district court versus here. Petitioner asserts in district court that the scope of the claims cannot be ascertained with reasonable certainty and the claims are thus indefinite. Yet Petitioner asserts here that "any reasonable construction reads on the prior art" (Pet., 7) and its expert explains his "understand[ing] that claim terms, in the absence of an express definition or disclaimer, are given their ordinary and customary meaning, as would have been understood by a POSITA at the time of the alleged invention" and that he has "applied these principles in interpreting the Challenged Claims" (EX1003 ¶¶86-89). Petitioner (and its expert) then proceed—without any mention that anything is allegedly indefinite or that the claim scope allegedly cannot be determined—to apply the prior art to the claims. This is the same failure that led the Director to vacate

institution of an IPR in *Tesla, Inc. v. Intell. Ventures II LLC*, IPR2025-00340, Paper 18 (Director Nov. 5, 2025) (informative). Second, instead of proposing its own claim constructions, Petitioner purports to adopt Patent Owner's alleged interpretation for several claim limitations. This failure similarly led the Director to vacate institution of an IPR in *Revvo Techs., Inc. v. Cerebrum Sensor Techs., Inc.*, IPR2025-00632, Paper 20 (Director Nov. 3, 2025) (precedential).

Petitioner's **Grounds 1A-1B** also fail for other reasons. For example, Petitioner proposes to add Gomez's EPIC payment account number (alleged to be the claimed "static device account number") to Law's system. According to Petitioner, "Law does not expressly disclose that [its] funding card identifier is sent as part of the complete payment information when performing a payment transaction" but a POSITA would have nonetheless sought to apply Gomez's EPIC payment account number to Law due to alleged improved transaction security. Pet., 14-15. The problem for Petitioner is that, among other things, Law teaches that doing so would *reduce* security, as it would "leave behind" a static number and thereby risk "replay attacks." Indeed, that is why Law discloses to use a different PAN generated by a "new Kpan" with every transaction (instead of a static PAN or other static funding identifier): "A new Kpan is used to generate a different PAN from the previous transaction, and to also prevent against replay attacks." EX1032, [0145]; *see also, e.g.*, [0223], [0268].

Petitioner also asserts that Gomez's EPIC payment account number is the claimed "static *device* account number." But Gomez confirms that its EPIC payment account number is simply an account number and has nothing to do with any particular device at all. This is yet another reason Grounds 1A and 1B fail.

For **Ground 2A** challenging independent claim 18 and dependent claims 19-24, Petitioner relies on the same four reference combination (*Gill-Smith-Kay-Gomez*) that was part of another IPR petition filed by Apple that was recently denied. Petitioner's Ground 2A challenge fails for the same reasons.

For example, Petitioner fails to show a motivation to combine or reasonable expectation of success for several reasons. Initially, Petitioner's primary reference (Gill) teaches that ATM transactions involve entirely different considerations than non-ATM transactions such as point-of-sale ("POS") transactions. This 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). Gill 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.

Petitioner's fourth reference in the combination, Gomez, is used for what Petitioner couches as a more explicit disclosure of "dynamically generated limited-use number portion[s]." *E.g.*, Pet., 52, 69. 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 addresses these considerations, which further demonstrate its Ground 2A fails to show a reasonable likelihood of success.

For these reasons and those below, Patent Owner respectfully submits that Petitioner has failed to show a reasonable likelihood of success for any Challenged Claim. Institution should be denied.

II. THE ’520 PATENT

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 Challenged Claims of the ’520 Patent generally relate to methods for reducing fraud during payment transactions.

Independent claim 10 is illustrative for Petitioner’s Ground 1A and 1B challenges (to independent claim 10 and dependent claims 11-17). The claim is directed to a method of storing and generating payment information in an electronic device wherein the device can accept a user input of issued payment information (such as a traditional credit card number). EX1001, 17:8-33 (claim 10). The device has both device-specific and user-specific information and wirelessly receives a

"static device account number payment information for storage on the electronic device." EX1001, 17:18-20. 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 10 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 for making a payment transaction." EX1001, 17:24-33. 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, 1:30-33.

The Challenged Claims in Ground 2A (claims 18-24) 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

Patent Owner discusses below the references in Petitioner's Grounds relevant to showing in this POPR that Petitioner has failed to show a reasonable likelihood of success for any Challenged Claim.

A. Law

U.S. Patent App. Pub. No. 2015/0134540 ("Law") is directed to systems and methods "for facilitating contactless payment using cloud-based wallet containing payment credentials (e.g. Visa, Mastercard, American Express) using a near field communication (NFC)-capable device and payment gateway servers." EX1032, Abstract. Law discloses "[b]y way of background" a typical credit card (such as in Figure 2) including credit card number 204, which is also "referred to as a primary account number (PAN)." EX1032, [0043].

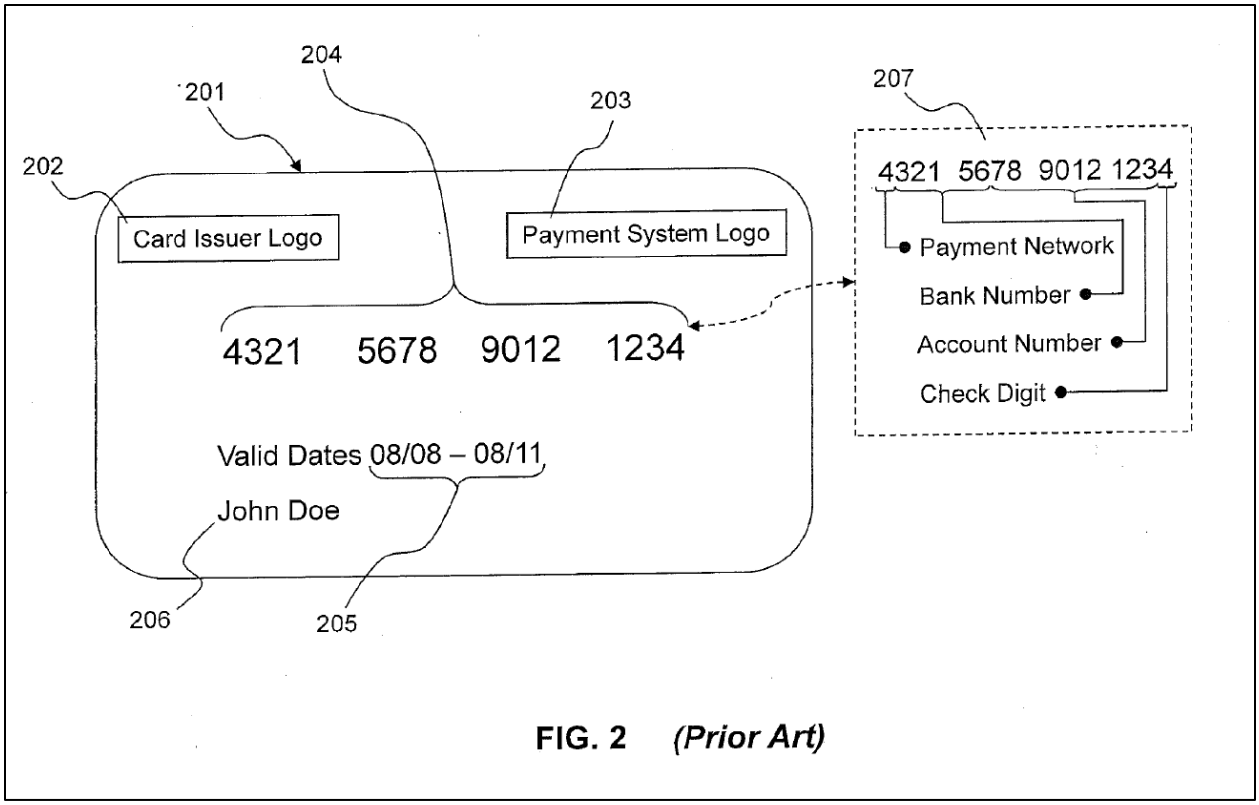


FIG. 2 ***(Prior Art)***

EX1032, FIG. 2. During a payment transaction the card is swiped such that the information (including the static PAN) is provided to the merchant for processing. EX1032, [0048]-[0059]. Law recognized that contactless transactions existed using a mobile device with NFC technology where the funding card can be loaded onto the device and the static card number (PAN) is transmitted along with other dynamic data. EX1032, [0061]-[0070]. However, such contactless transactions suffered from certain drawbacks, including storage, compatibility, coordination, and security issues. EX1032, [0071]-[0073]. Law thus explains in its Abstract to use a "virtual card" connected on the backend to the actual "funding card":

> A user can use their existing payment card, herein referred to as a funding card, for contactless payments. A second

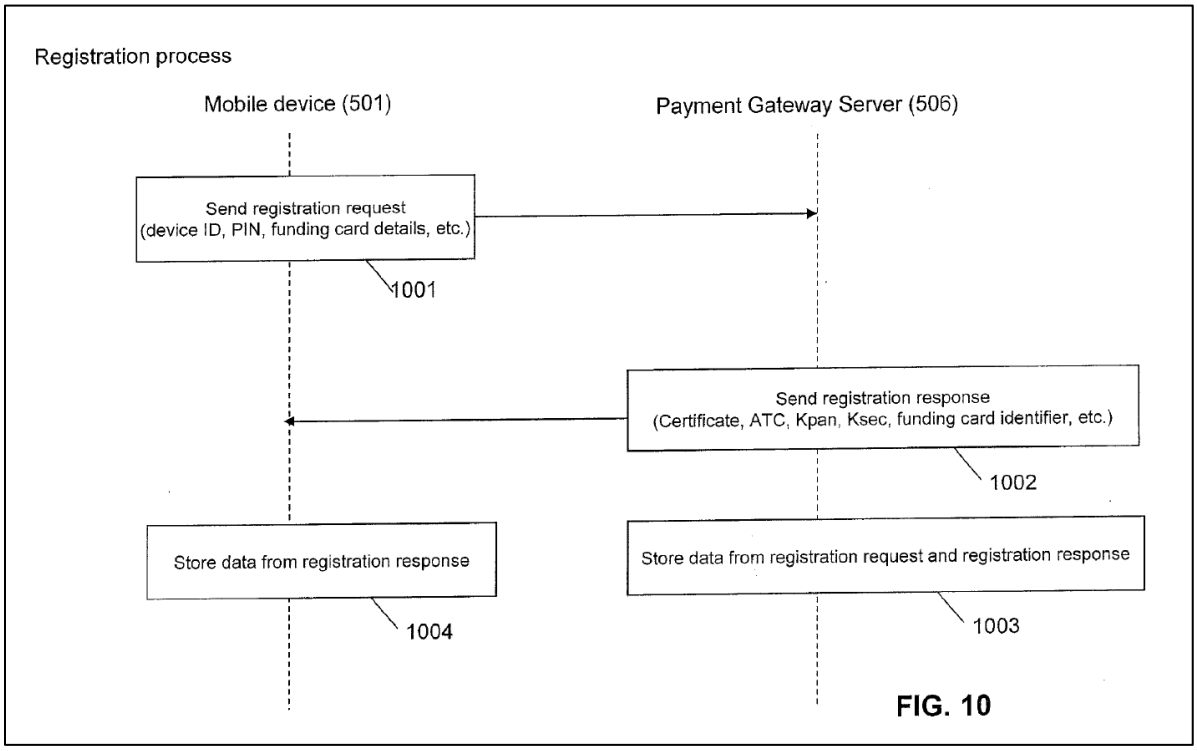
> payment card, herein referred to as a virtual card, is generated. The virtual card is associated with the funding card on a payment gateway server. The virtual card is used on a NFC-enabled mobile device. When a payment is initiated, the virtual card data is sent through the NFC system from a point of sale terminal. This information is sent to the payment gateway server, which retrieves the funding card to make the payment. The funding card, not the virtual card, is used to transfer the money to make payment.

EX1032, Abstract.

Law discloses how to register a virtual card with the virtual card data for use on a mobile device that includes, among other things, a "kPAN" (aka, a "key value") which changes with every transaction and is used to generate a new PAN for each transaction. This is explained, for example, in the context of Figures 10-12 and elsewhere in Law.

In Figure 10, Law discloses a registration process, whereby a registration request is sent from a mobile device and a response is then sent by a payment gateway server. EX1032, [0142]-[0143]. The response includes "a certificate, an Application Transaction Counter (ATC), *a key value (called Kpan) for generating a PAN*, a secure element key value (called KSec), and a funding card identifier that

identifies each registered funding card(s).” EX1032, [0142].[1] Both payment gateway server 506 and mobile device 501 store the registration response data (at blocks 1003 and 1004). EX1032, [0143].



EX1032, FIG. 10.

In Figure 11, Law discloses a process to compute a virtual card, whereby a request from the mobile device includes “the device ID, the identifier of the selected funding card, the Certificate and the stored Kpan,” which “stored Kpan can be from registration or from the previous transaction.” EX1032, [0144]. As Law explains, “[t]he payment gateway server 506 determines if the *received Kpan* and Certificate

[1] Unless noted, all emphasis and coloring have been added.

match the Kpan and Certificate stored on the payment gateway server (block 1102) associated with the DeviceID stored in the payment gateway server database." EX1032, [0145]. "If so, then the payment gateway server 506 sends a virtual card response to the mobile device 501 that includes a *new Kpan* (block 1103)," and "[a] *new Kpan* is used to generate a *different PAN* from the previous transaction, and to also prevent against replay attacks." EX1032, [0145]. This new Kpan is stored both at the mobile device and payment gateway server (at blocks 1105 and 1106) for "later use" as part of a transaction. EX1032, [0145]-[0146].

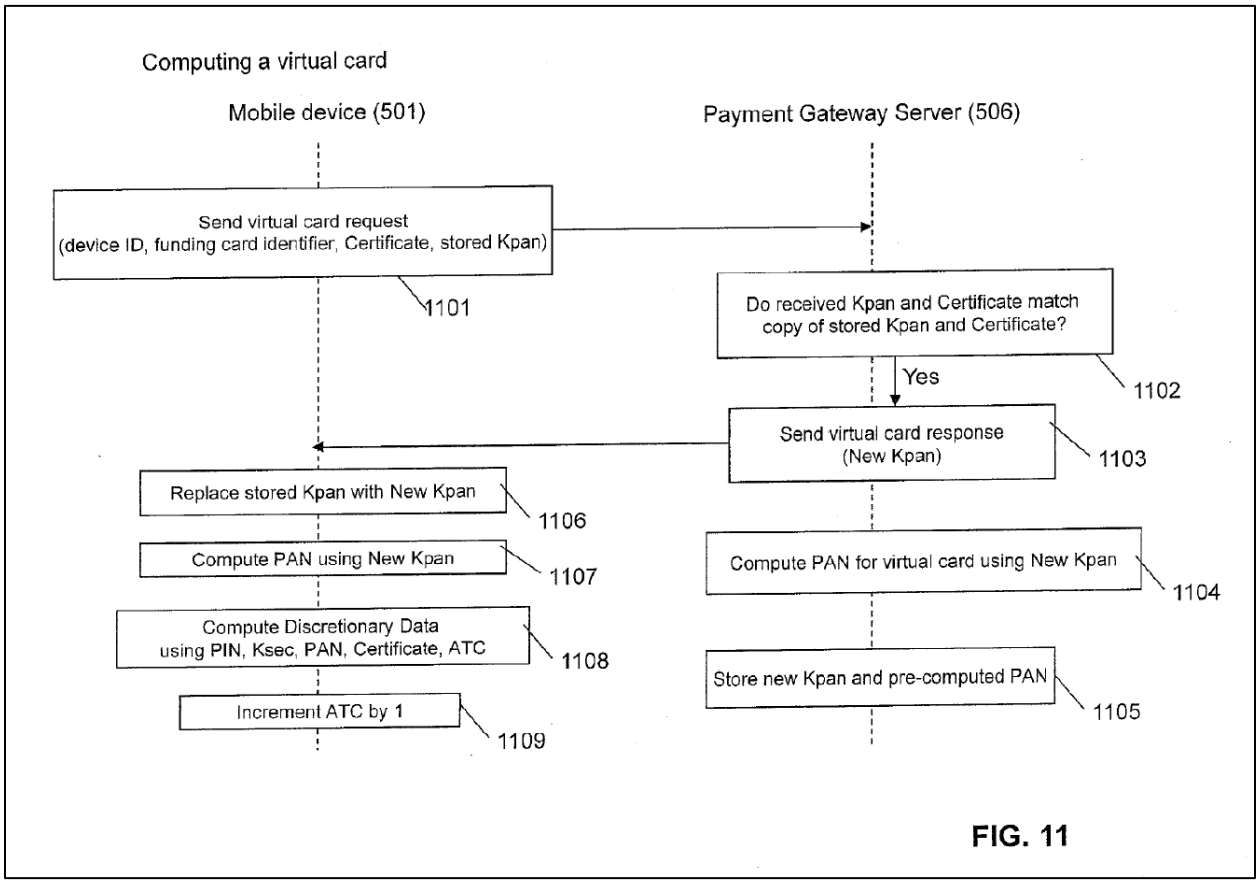


FIG. 11

EX1032, FIG. 11.

In Figure 12, Law depicts "an example embodiment of computer executable or processor implemented instructions [that] are provided for verifying virtual card data, and in particular the verification by the payment gateway server of the discretionary data (e.g. the dynamic data)." EX1032, [0156]. Figure 12 "can be used in combination with the principles described above for verifying the virtual card data" and as "a continuation of [Figure] 11." EX1032, [0156]. The mobile device sends a payment authorization request (block 1201) including a PAN (referencing to Figure 11, a new "different PAN" generated using the new Kpan) along with other data. EX1032, [0157], [0268]. The payment gateway server receives the request and compares the received PAN to stored PANs, "and if a match is found … then the stored data associated with that given precomputed PAN is considered the relevant stored associated data" and the payment gateway server continues to confirm the other data (*e.g.*, discretionary data) to verify the transaction. EX1032, [0278]. "[A]fter the data is successfully verified or not, the payment gateway server eventually respond[s] to the merchant by sending an authorisation response to the merchant (103,502) (block 1207)." EX1032, [0166]. Law discloses how to process a transaction using the data transmitted as part of the payment authorization request to retrieve the funding card details for use in completing the transaction. EX1032, [0077]-[0078], [0117], [0135], [0175], [0224], [0259].

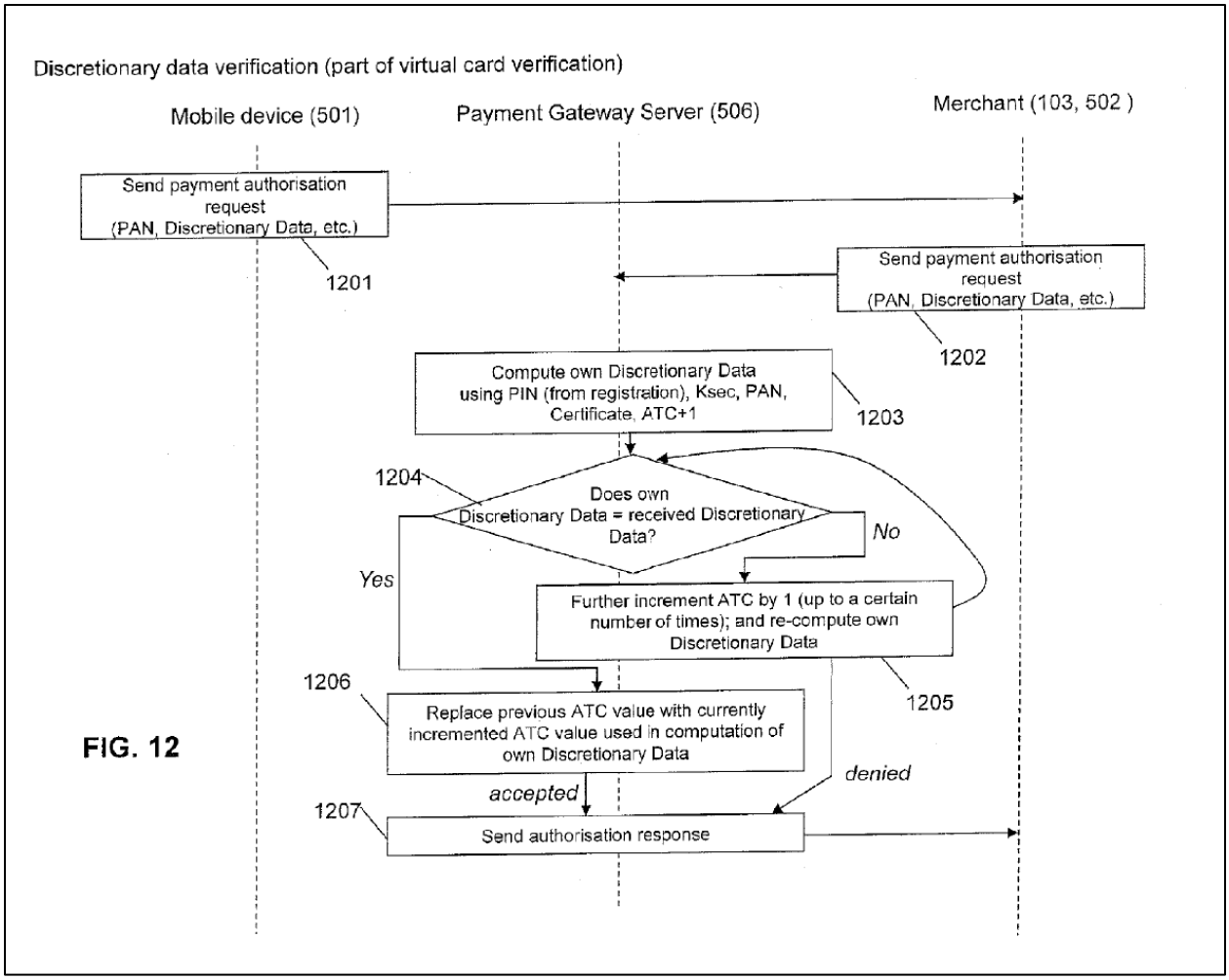


FIG. 12

EX1032, FIG. 12.

B. Gomez

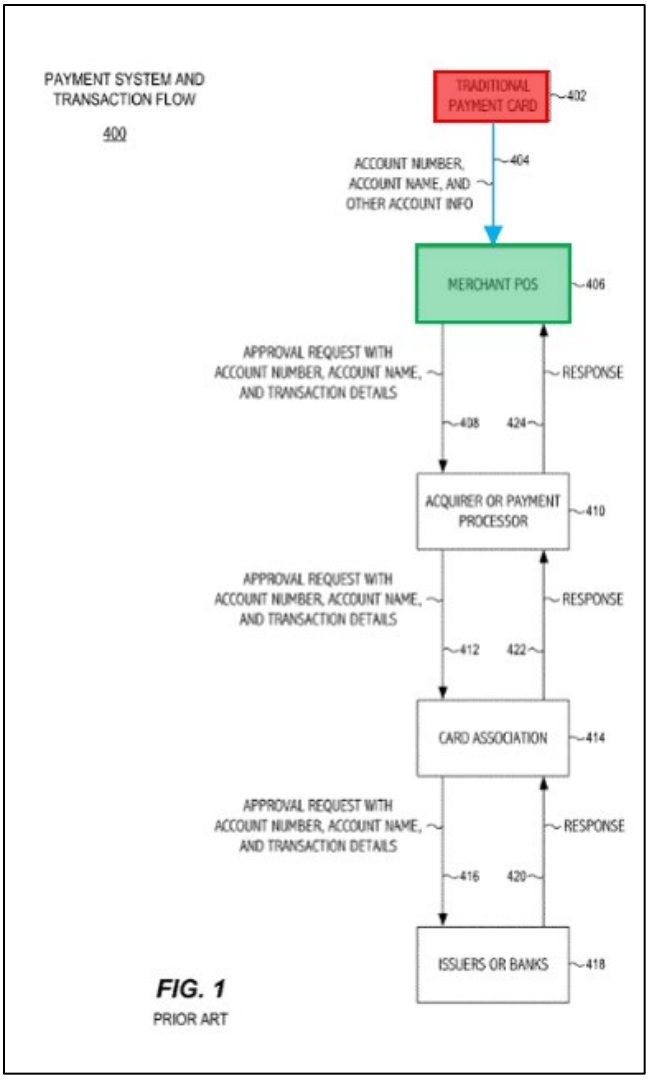
U.S. Patent No. 9,600,808 ("Gomez") is concerned with fraud risk associated with in-store payments at a point-of-sale ("POS") terminal or with a merchant present. EX1007, 4:64-5:2 ("[T]he risk is much higher regarding interactions with the merchant 406, whose employees may have access to the physical 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. EX1007, 1:58-63.

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" and may represent "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 the date/time of the attempted purchase." EX1007, 5:13-29. 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.

Gomez's system is specifically designed to work within a pre-existing traditional payment system infrastructure, such that "*[n]o changes* in the payment system infrastructure need be made by either the point-of-sale merchant or the card issuer." EX1007, 2:40-41; *see also, e.g.*, 2:42-45, 5:32-34, 5:67-6:2. "For example,"

Gomez explains that "such a payment card [the "EPIC" payment card discussed below] may use a programmable magnetic stripe or contactless technology to provide *total compatibility* with existing POS equipment." EX1007, 2:40-42. Gomez then discloses the "*traditional* payment system" in Figure 1 (EX1007, 3:65-67), which it labels "Prior Art" (*i.e.*, the pre-existing payment infrastructure that Gomez is expressly designed to work within, without any changes to the existing merchant POS or card issuer):



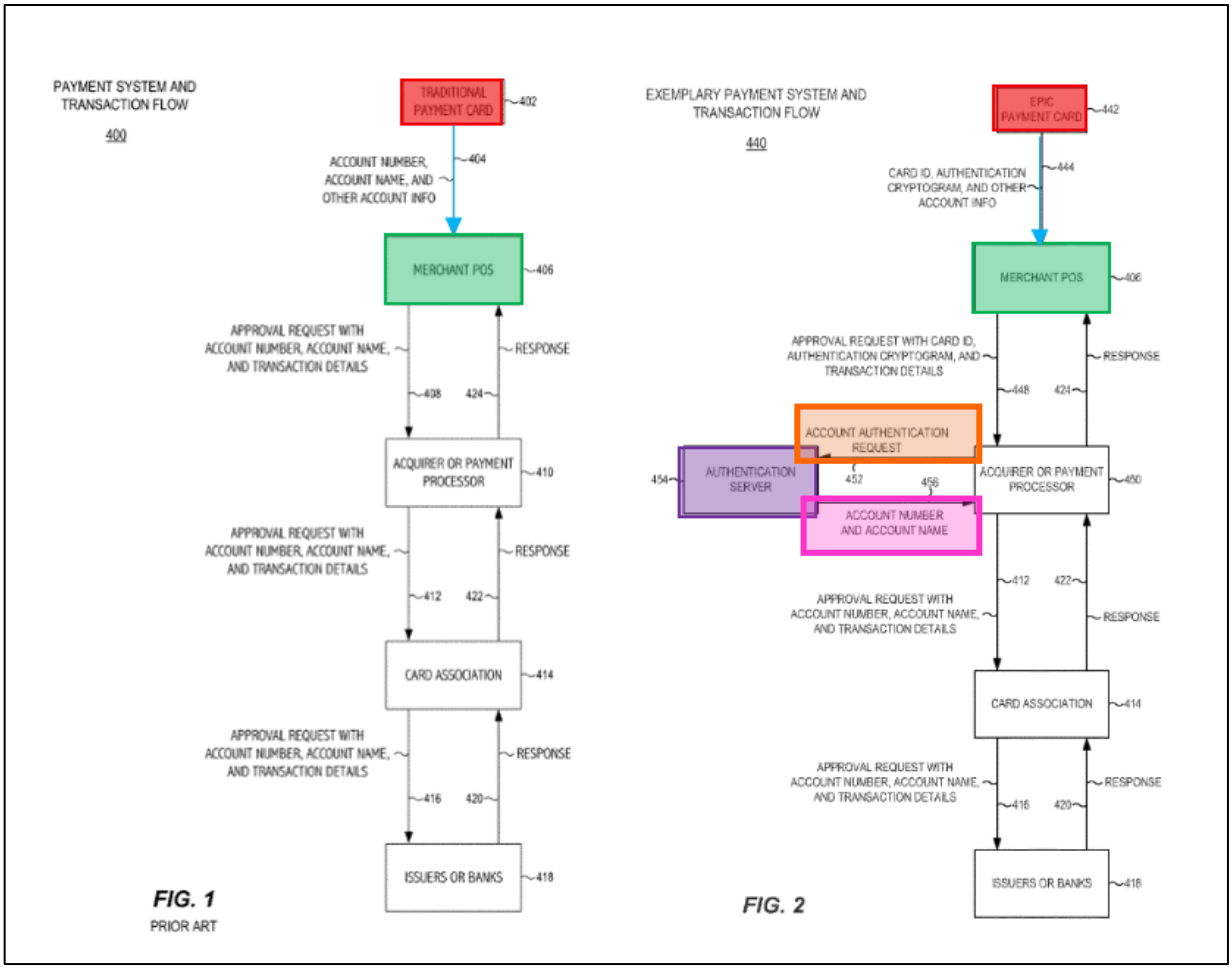
EX1007, FIG. 1. As shown in Figure 1, Gomez discloses a traditional "payment system and transaction flow," with a "**traditional payment card 402**" that transmits to "**merchant POS 406**" "**account information 404**" "including the account number, security code, account name, expiration date." EX1007, 3:65-4:7. Notably, this is a *one-way* communication, *i.e.*, the payment card transmits information to the merchant POS, while the merchant POS does not send anything to the card. This is further evident by the bi-directional communication elsewhere in the Figure (request 408, response 424, etc.). *See also, e.g.*, EX1007, 4:8-63. That is, in the "traditional payment system" and "transaction flow" disclosed by Gomez (and depicted in Figure 1), a payment card sends information to the merchant POS, but not vice versa.

In its system, Gomez specifically makes no modifications to the merchant POS or card issuer systems to implement its "EPIC payment card." Such EPIC payment card includes a rewritable magnetic stripe on which the static payment card identifying number may be encoded in the account number field and the authorization cryptogram may be encoded in the account name field. EX1007, 5:48-57, Abstract. The EPIC payment card may be swiped through a POS terminal "just like a traditional magnetic stripe payment card." EX1007, 5:29-34. Here too, Gomez teaches that "[s]ince all of the information is encoded using *standard* fields, a *traditional POS* terminal may be used *without any required changes* as a result of the encoding." EX1007, 5:67-6:2; *see also* 14:3-11. The information such as the

EPIC account number is "'left behind'" and "readily observable." EX1007, 5:32-40; *see also*, 13:63-65.

Account information communicated by swiping the card is sent by the merchant to a payment processor or "acquirer," which analyzes the account number to determine it corresponds to an EPIC account. EX1007, 5:64-6:12. The acquirer sends an account authentication request to an EPIC authentication server, which determines whether the cryptogram is valid and, if so, provides to the acquirer an actual payment card account number and account name to use for processing the transaction. EX1007, 6:23-27. The acquirer then uses that information to form an approval request to the card association corresponding to the actual payment card being used. EX1007, 6:39-47. The request is "essentially unchanged" from that used in a traditional payment system. EX1007, 3:65-67, 6:47-51.

Thus, as can be seen by comparing Figure 1 (a "traditional" "prior art" payment system) with Figure 2 (Gomez's system) the transaction flow is largely the same (and the exact same as to **the merchant POS** and card issuer); the only change is that the payment processor communicates with an additional **authentication server** to obtain the account number and account name. EX1007, 3:18-23, 3:65-67, 5:48-50, FIGs. 1-2.



EX1001, FIGs. 1-2.

In effect, Gomez's system adds a cryptogram into the account cardholder name field, and an associated substitute "account number" (the EPIC payment account number) into an otherwise traditional system. The EPIC number and the cryptogram are later authenticated by **EPIC authentication server 454**. EX1007, 6:7-37. An **account authentication request 452** is created, which includes "the EPIC account number, the date and time of the transaction, and the authentication cryptogram" and is sent to **EPIC authentication server 454**. EX1007, 6:12-22.

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 "accomplishe[d] … 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** communicated back to the acquirer 450." EX1007, 6:32-38.

C. Gill

U.S. Patent No. 9,098,846 ("Gill") describes systems and methods for performing contactless transactions at an ATM. "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." EX1034, Abstract.

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

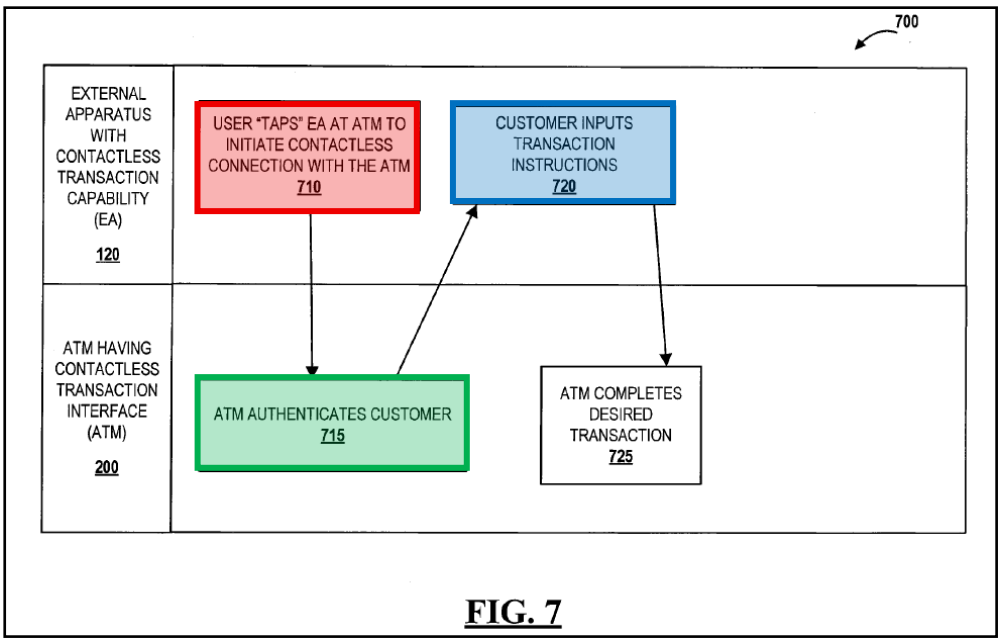


FIG. 7

EX1034, FIG. 7.

As shown in Figure 7, 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." EX1034, 14:1-8. At **block 715**, the ATM 200 "authenticat[es] the customer" by requiring the user to present a valid credential such as a PIN. EX1034, 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." EX1034, 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). EX1034, 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 technology[2] 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 generally limited as to the amount

[2] Gill claims priority to a non-provisional filed September 6, 2012 and provisional filed March 4, 2011. EX1034, Cover Page. That is before, for example, Smith (EX1035, Cover Page) and Gomez (EX1007, Cover Page).

> 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.

EX1034, 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*.

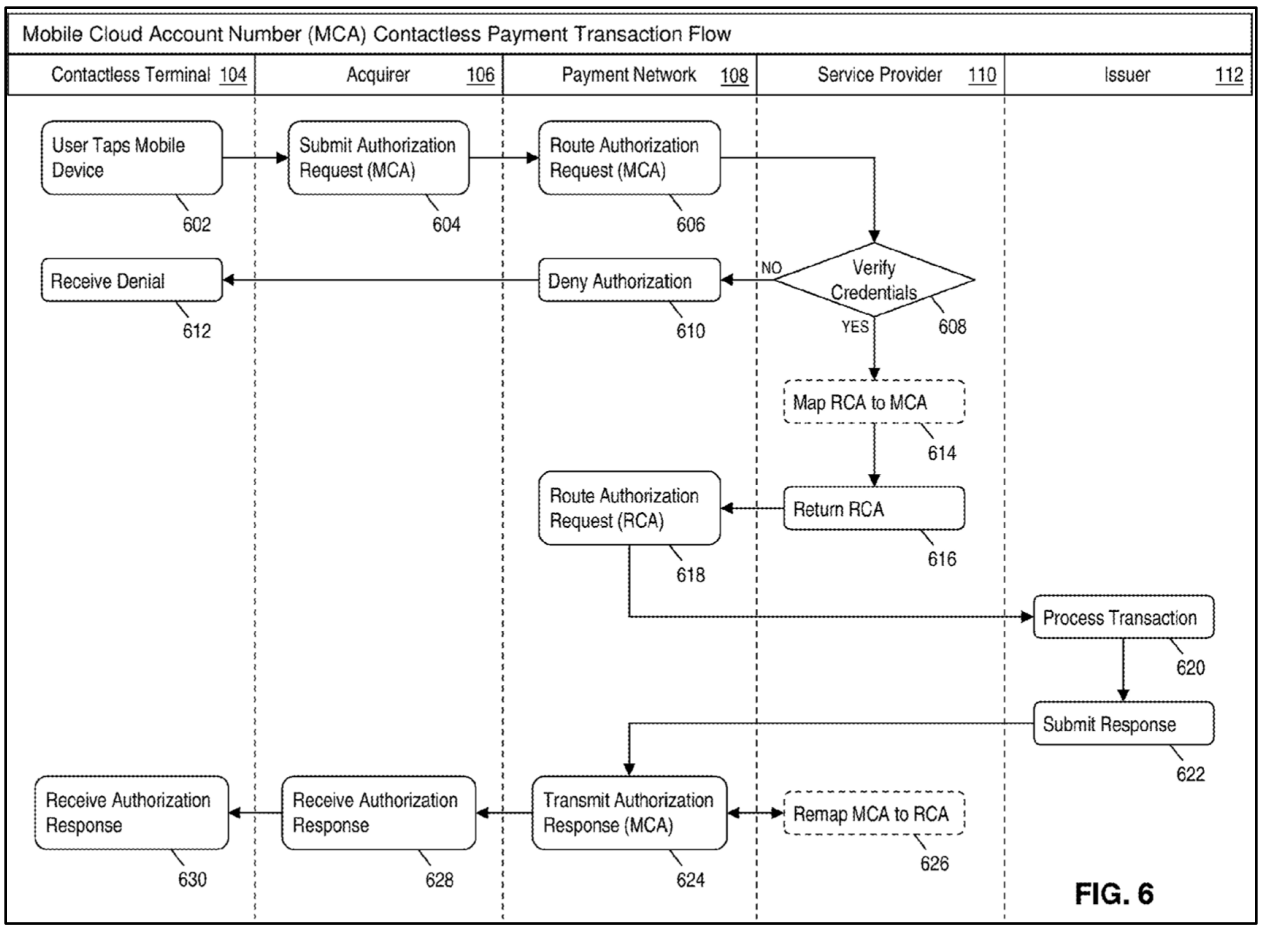
EX1034, 4:56-5:10.

Thus, per 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.

D. Smith

U.S. Patent App. Pub. No. 2013/0232083 ("Smith") describes techniques for conducting POS contactless payment transactions with a mobile device. EX1035, Abstract, [0002], [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. EX1035, [0032]-[0037]; *see also* [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)." EX1035, [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." EX1035, [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." EX1035, [0034].



EX1005, FIG. 6.

As shown in Figure 6, Smith discloses that a user initiates a POS contactless transaction by tapping his/her mobile device at a terminal. EX1035, [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." EX1035, [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." EX1035, [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. EX1035, [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." EX1035, [0072].

E. 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" and a financial transaction terminal. EX1036, [0004], [0017]. "[T]he 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. *See id*., [0038]-[0043].

Pet., 44.

IV. LEVEL OF ORDINARY SKILL IN THE ART

For purposes of this POPR only, Patent Owner does not dispute Petitioner's definition of a person of ordinary skill in the art (a "POSITA").

V. CLAIM CONSTRUCTION

A. Static Device Account Number

Claims 10-17 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 claim 10 (and others). In that proceeding, the Board denied institution on the merits because it determined that the petitioner (Samsung) failed to demonstrate that any of its references disclosed a "static device account number." EX2030 (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." EX2030, 14.

The Board did not specifically address the words "device" or "account," but it did determine that "static" modifies "number" and that the petitioner needed to show that the prior art disclosed such a "static" number. EX2030, 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.

VI. THE PETITION FAILS TO ESTABLISH A REASONABLE LIKELIHOOD OF SUCCESS AS TO ANY CHALLENGED CLAIM

A. Petitioner Fails to Show a Reasonable Likelihood of Success for Grounds 1A-1B.

Petitioner failed to comply with 37 C.F.R. § 42.104(b)(3). But regardless, a POSITA would not have sought to make the proposed combinations and the combinations are missing key limitations.

1. The Petition Does Not Comply with 37 C.F.R. § 42.104(b)(3) Because Petitioner Does Not Explain Why it is Taking Different Claim-Construction Positions In Its IPR Petition and District Court or Using Patent Owner's Alleged Constructions.

Petitioner "must set forth" in the Petition "[h]ow the challenged claim[s] [are] to be construed." 37 C.F.R. § 42.104(b)(3). The Director has explained that, to comply with Rule 42.104(b)(3), "when a petitioner advances different positions before the Board and a district court, that petitioner is *required* to explain why those different positions are warranted." *Tesla, Inc. v. Intell. Ventures II LLC*, IPR2025-00340, Paper 18 at 3 (Director Nov. 5, 2025) (informative) (emphasis in original and citing *Revvo Techs., Inc. v. Cerebrum Sensor Techs., Inc.*, IPR2025-00632, Paper 20

at 3-5 (Director Nov. 3, 2025) (precedential)). Petitioner has failed to do so, meaning its Grounds 1A-1B challenges necessarily fail.[3]

The situation here is analogous to both the Director's Order in *Tesla* Granting Director Review, Vacating the Decision Granting Institution, and Denying Institution of *Inter Partes* Review (IPR2025-00340, Paper 18), as well was the Director's Order in *Revvo* Vacating the Decision Granting Institution, and Remanding to the Board for Further Proceedings after *Sua Sponte* Director Review (IPR2025-00632, Paper 20).

Patent Owner explains below why Petitioner failed to comply with Rule 42.104(b)(3) for two independent reasons: (1) as in *Tesla*, Petitioner asserts in district court that the scope of certain terms cannot be ascertained with reasonable certainty and thus the claims are indefinite but asserts here that those same terms should be given their plain and ordinary meaning; and (2) as in *Revvo*, Petitioner

[3] Although Petitioner took these claim construction positions concerning Grounds 1A-1B, Patent Owner respectfully submits that it would be improper to institute on any Ground as Petitioner has failed to comply with Rule 42.104(b)(3) (necessitating denial) and Petitioner also could then potentially seek to continue to (improperly) pursue Grounds 1A-1B post-institution.

purports to adopt Patent Owner's claim constructions instead of proposing its own constructions for various claim terms in the Petition.

a. Analogous to *Tesla*, Petitioner Asserts in District Court that the Scope of the Claims Cannot be Ascertained with Reasonable Certainty But Has No Issue Doing So In Its IPR Petition

The situation here is akin to the Director's Order in *Tesla*, IPR2025-00340, Paper 18. In *Tesla*, the petitioner asserted in district court that a claim limitation (referred to as the "generating limitation") "recited in independent claim 1 is indefinite because a person of ordinary skill in the art would not be able to determine the meaning and scope of that limitation with reasonable certainty," which the patent owner opposed. *See id.* at 2-3. "In contrast, [the *Tesla* petitioner] argued in its Petition that the challenged claims should be given their plain and ordinary meaning." *Id.* The petitioner argued it complied with 37 C.F.R. § 42.104(b)(3) "by providing a construction for the generating limitation, and by explaining that the different claim construction positions at the Board and in district court are warranted because Petitioner is statutorily prohibited from raising indefiniteness challenges in an *inter partes* review." *Id.* at 2-3. The Director held that "Petitioner's statement that it cannot raise indefiniteness challenges in an *inter partes* review is not a sufficient explanation" and "[i]ndeed, the statement amounts to an assertion that a petitioner should be permitted to raise inconsistent invalidity challenges in the two forums." *Id.* at 3. In the Order vacating institution, the Director found that "[a]llowing a

petitioner to advance a claim construction before the Board when that petitioner has made inconsistent indefiniteness arguments in district court fails to further, but instead detracts from, the Office's goal of 'providing greater predictability and certainty in the patent system.'" *Id.* at 4 (quoting *Revvo Techs.*, IPR2025-00632, Paper 20 at 4-5 (quoting 83 Fed. Reg. 51,340, 51,342-43 (Oct. 11, 2018))).

The same thing (albeit worse) happened here.

Petitioner's District Court Positions. Petitioner asserts in district court that various "payment information" terms found in independent claim 10 (and by extension, dependent claims 11-17) have "no reasonably certain meaning" rendering the claims indefinite. EX2024, 3-10 (Petitioner's Opening Claim Construction Brief); EX2028, 2-7 (Petitioner's Reply Claim Construction Brief, asserting same); *see also* EX2025, 1 (Joint Claim Construction Statement confirming it was Petitioner that proposed to construe the terms and asserts they are indefinite). Patent Owner disagreed and explained that these terms should be given their "plain and ordinary meaning." EX2027, 3-10 (Responsive Claim Construction Brief); EX2029, 2-6 (Sur-Reply).

Petitioner's IPR Positions. In its IPR petition, Petitioner asserts that "any reasonable construction reads on the prior art." Pet., 7. Its expert notes his "understand[ing] that claim terms, in the absence of an express definition or disclaimer, are given their ordinary and customary meaning, as would have been

understood by a POSITA at the time of the alleged invention," and that "[i]n considering the meaning of the claims, however, … one must consider the language of the claims in light of 'the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.'" EX1003 ¶¶86-87 (quoting 37 C.F.R. § 42.100(b)). He also asserts that he "applie[s] these principles in interpreting the Challenged Claims for purposes of my analysis in this Declaration." EX1003 ¶88.[4]

Petitioner (and its expert) then proceed—without any mention that anything is allegedly indefinite or that the claim scope allegedly cannot be determined—to apply the prior art to the claims. *See* Pet. (Grounds 1A-1B).

While Petitioner attaches the magistrate judge's claim construction order and generically mentions it in passing (Pet., 7 (citing EX1046)), Petitioner omits that (i) it argues in district court that the claim scope cannot be ascertained rendering the claims indefinite, (ii) it is continuing to pursue its indefiniteness challenges in district court, and (iii) it has filed objections to the magistrate judge's order, asking the court to revisit the determination rejecting Petitioner's indefiniteness assertion for claims

[4] The expert also notes that he "understand[s] that Petitioner does not assert that any claim terms require express construction in this proceeding." EX1003 ¶89.

10-17. EX2023, 1-5.[5] Moreover, Petitioner has *not* withdrawn or otherwise agreed to not pursue its indefiniteness positions during the district court case or on appeal—further confirming that, regardless of the outcome of its IPR petition, it has (and will) continue to maintain entirely inconsistent and irreconcilable positions in parallel forums.[6]

And importantly, and even worse than in *Tesla*, Petitioner does ***not*** mention (let alone attempt to justify) that it has taken contradictory positions between forums. *See Am. Airlines, Inc. v. Intell. Ventures I LLC*, IPR2025-01055, Paper 11, 13 (PTAB Nov. 11, 2025) ("We also remind Petitioner's counsel of their duty of candor and good faith to the Office during the course of a proceeding pursuant to 37 C.F.R. § 42.11. Patent Owner should not have been the first party to inform the Board as to

[5] Petitioner's expert—in applying the "ordinary and customary meaning" to the claims—does not mention or address any indefiniteness issues. Although he states he reviewed and is familiar with the "exhibits to the Petition" (EX1003 ¶29), he never mentions or considers Petitioner's district-court claim construction positions or the magistrate judge's order (EX1046) in his declaration. *See generally* EX1003.

[6] Petitioner's statement in the Petition that it "reserve[s] all rights to raise claim construction and other arguments in other venues" (Pet., 7 n.5) is telling and systemic of Petitioner's ongoing inconsistent approaches across the forums.

Petitioner's different claim construction positions in the two forums."); *cf. Tesla*, IPR2025-00340, Paper 18 at 3 ("Here, Petitioner's statement that it cannot raise indefiniteness challenges in an *inter partes* review is not a sufficient explanation. Indeed, the statement amounts to an assertion that a petitioner should be permitted to raise inconsistent invalidity challenges in the two forums.").

Accordingly, because Petitioner has taken (and continues to take) irreconcilable and unexplained claim-construction positions in parallel forums—alleging in district court that the scope of certain terms cannot be ascertained and are thus indefinite while in its IPR Petition seeking to apply the plain and ordinary meaning for those same terms—Patent Owner respectfully submits that Petitioner has failed to comply with Rule 42.104(b)(3). *See Tesla*, IPR2025-00340, Paper 18 at 3; *Am. Airlines*, IPR2025-01055, Paper 11 at 11-13; *Revvo*, IPR2025-00632, Paper 20 at 3-5. Institution would thus be improper.

b. Analogous to *Revvo*, Petitioner Also Purports to Apply Patent Owner's District Court Positions

The situation here is also like the Director's Order in *Revvo*, IPR2025-00632, Paper 20. In *Revvo*, the petitioner "did not propose its own constructions for claim terms in the Petition, but instead accepted [the patent owner's] proposed constructions from the parties' district court litigation." *Id.* at 2. The petitioner asserted it complied with Rule 42.104(b)(3) "because Petitioner had adopted Patent Owner's proposed constructions from the district court litigation." *Id.* As the

Director stated, "[s]imply noting that the petitioner is adopting a patent owner's claim construction proposals from district court, however, is *not* a sufficient reason for advancing different positions in the two forums." *Id.* at 5. The Director found that the petitioner's bare statement that it "accepts Patent Owner's proposed constructions" fails to comply with Rule 42.104(b)(3). *Id.*

That is analogous to Petitioner's assertions here. Instead of applying the plain and ordinary meaning or explaining what Petitioner believes to the proper construction, Petitioner relies on Patent Owner's alleged interpretation—based in large part on a misrepresentation of Patent Owner's preliminary infringement contentions in the parallel case (EX1037)—to explain why the prior art allegedly teaches various claim limitations. This is exemplified in the following table:

Limitation	**Petitioner's Assertion**
[10.e]	"In its infringement contentions, Patent Owner identifies, among other things, a DPAN (or static number) as meeting [10.e]. *See* EX1037, 95. Applying that interpretation, the Law-Gomez combination discloses this limitation. EX1003, ¶¶144-145. Patent Owner also identifies 'a issuer provided payment information' as a 'PAN or associated expiration date or CVV.' *Id*. Applying that interpretation, the Law-Gomez combination discloses that limited-use numbers for limited-use by the device are used in place of at least a PAN (i.e., an actual credit card number). EX1032, [0082]; EX1033, [0052]; EX1003, ¶¶144-145." Pet., 28-29 n.9.

Limitation	Petitioner's Assertion
[10.e]	"This also aligns with Patent Owner's interpretation of the limitation which advances infringement contentions that identify a cryptogram, among other values, as [10.e]'s 'limited-use number' (in addition to [10.f]'s 'one-time limited use number'). EX1037, 95; *see also id*., 99. Thus, Gomez's disclosure of the EPIC number (i.e., 'a static device account number payment information') and an authentication cryptogram (i.e., 'a dynamically-generated one-time limited-use number') and the use of those values together align with Patent Owner's interpretation of the limitation. *Id.* Applying that interpretation, the combination of Law-Gomez would also provide the recited limited-use number for limited use by the device in place of a issuer provided payment information. EX1003, ¶¶144-145; *supra* IX.A.3." Pet., 29-30.
[10.a]	"Law's disclosure of user input of an expiry date and/or static security code would constitute at least [10.a]'s 'an issuer provided payment information.' *See* EX1037, 71-78; EX1003, ¶135." Pet., 20.
[10.c]	"The Law-Gomez disclosure of issuer provided payment information communicated wirelessly aligns with Patent Owner's interpretation of limitation [10.c]. In its infringement contentions, Patent Owner identifies a Wi-Fi or cellular network communication as [10.c]'s wireless communication. *See* EX1037, 81." Pet., 23 n.7.
[10.d]	"The Law-Gomez disclosure of wirelessly receiving a static device account number payment information for storage on the electronic device aligns with Patent Owner's interpretation of limitation [10.d]. In its infringement contentions, Patent Owner identifies the reception

Limitation	Petitioner's Assertion
	of a tokenized account number over a wireless connection as meeting [10.d]. *See* EX1037, 88-95." Pet., 26 n.8.

As the above table shows, in multiple instances across independent claim 10, Petitioner does not purport to rely on what it believes to be the plain and ordinary meaning, but rather on what it believes Patent Owner's construction to be (as allegedly reflected in EX1037).

Petitioner's expert confirms that he also used "Patent Owner's reading of the claims in forming [his] opinions" on "occasion[]":

> I am aware that the parties are engaged in contemporaneous litigation styled *CardWare Inc. v. Google LLC*, Case No. 7:24-cv-00278 (W.D. Tex.) (the "Litigation"). In the Litigation, Patent Owner has accused Petitioner's mobile phones as infringing the Challenged Claims, despite the fact that the Patent does not disclose any mobile phone invention, but instead is drawn to a payment card that can be read by a magnetic stripe reader. *This accusation has compelled Patent Owner to interpret various claim terms in a manner that is at odds with the intrinsic evidence.* ***I have therefore made occasional use of Patent Owner's reading of the claims in forming my opinions***.

EX1003 ¶30.

Petitioner's expert—at the request of Petitioner's counsel—then does just that for certain limitations in independent claim 10, where he was "asked to assume

[Patent Owner's alleged interpretation] applies to [the] limitation" and then provides his opinion "[i]f that interpretation applies." For example:

- "I understand from counsel that Patent Owner has identified a Wi-Fi or cellular network communication as [10.c]'s wireless communication. ***I have been asked to assume that interpretation applies to this limitation***. ***If that interpretation applies***, the Law-Gomez disclosure of issuer provided payment information communicated wirelessly aligns with Patent Owner's interpretation of limitation [10.c]." EX1003 ¶140 n.2.
- "I understand from counsel that Patent Owner has identified the reception of a tokenized account number over a wireless connection as meeting [10.d]. ***I have been asked to assume that interpretation applies to this limitation***. ***If that interpretation applies***, the Law-Gomez disclosure of wirelessly receiving a static device account number payment information for storage on the electronic device aligns with Patent Owner's interpretation of limitation [10.d]." EX1003 ¶143 n.3.
- "I understand from counsel that Patent Owner has identified, among other things, a DPAN (or static number) as meeting [10.e]. ***I have been asked to assume that interpretation applies to this limitation. If that interpretation applies***, the Law-Gomez combination discloses this limitation. I also understand that Patent Owner has identified 'a issuer provided payment information' as a 'PAN or associated expiration date or CVV.' Applying that interpretation, the Law-Gomez combination discloses that limited-use numbers for limited-use by the device

> are used in place of at least a PAN (i.e., an actual credit card number). EX1032, [0082]; EX1033, [0052].” EX1003 ¶144 n.4.

See also EX1003 ¶145 (using “Patent Owner’s interpretation of the limitation” for [10.e]).

As is apparent from the above, Petitioner and Petitioner’s expert (at counsel’s request) use Patent Owner’s alleged claim interpretations throughout the analysis of independent claim 10. That is improper and fails to comply with Rule 42.104(b)(3). Accordingly, Patent Owner respectfully submits that Petitioner has failed to comply with Rule 42.104(b)(3) for the additional reasons explained in this Section V.A.1.b. *See Revvo*, IPR2025-00632, Paper 20 at 3-5.

2. A POSITA Would Not Have Substituted Gomez’s EPIC Payment Account Number into Law’s System Because It Would Reduce Security Measures of Law and Leave Law Vulnerable to “Replay Attacks” and Other Unauthorized Access Attempts

Petitioner’s rationale for using Gomez’s EPIC payment account number with Law’s system[7] is premised on its assertions that (i) “Law does not expressly disclose that the funding card identifier is sent as part of the complete payment information

[7] As explained in this Section VI.A.2, and further in Section VI.A.3, Petitioner’s obviousness theory is premised on adding Gomez’s EPIC payment account number into Law’s system.

when performing a payment transaction," (ii) Gomez describes an "EPIC" payment account number (also referred to a "static payment card identifying number") used in a transaction along with an authentication cryptogram, and (iii) "[m]ultiple reasons would have led a POSITA to apply Gomez's suggested use of a static payment card identifying number in combination with an authentication cryptogram with Law before the Critical Date of the '520 patent." Pet., 14. Petitioner's "reasons" to add the EPIC account number boil down to an alleged increase in security in "preventing fraudulent use of a substituted or incorrect account number," "requiring both a tokenized static number and authentication cryptogram as part of the complete payment information [would result in] an additional layer of security [being] realized to prevent unauthorized actors from exploiting any compromised portion of the payment," and allegedly enabling "a payment processing authority [to] more easily identify the user's actual account number for processing a transaction with the presence of the user's tokenized static account number in the payment information because that tokenized static account number is linked to the user's actual account." Pet., 14-15.

Its expert says the same thing, without any additional evidence or analysis. EX1003 ¶¶127-28. Such testimony should be given little to no weight. *See, e.g.*, *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., Inc. v. Innovative Sonic Ltd.*, IPR2024-01143, Paper 15, 28, 38 (PTAB Feb. 11, 2025).

Notwithstanding, there are multiple problems with Petitioner's conclusory assertions (and its expert's parroting of the same).

First, transmitting a static number as part of payment transactions is exactly what Law teaches ***not*** to do. Law relies on a one-time use "Kpan" that is intentionally used to generate a ***new, different*** PAN with ***every*** transaction. EX1032, [0145], [0223], [0249], [0268], [0270].[8] This is critical in Law because it "prevent[s] against replay attacks":

[8] The use of Law's Kpan underlies Petitioner's obviousness theory. Pet., 26-29 (relying on Kpan as limited-used payment information including to assert that "[t]he newly received Kpan is used to compute a different PAN (i.e. limited-used payment information) from the previous transaction for the virtual card"), 30 (relying on Kpan regarding dynamically generated one-time limited-used number).

> The payment gateway server 506 determines if the received Kpan and Certificate match the Kpan and Certificate stored on the payment gateway server (block 1102) associated with the DeviceID stored in the payment gateway server database. If so, then the payment gateway server 506 sends a virtual card response to the mobile device 501 that includes a ***new Kpan*** (block 1103). A ***new Kpan is used to generate a different PAN from the previous transaction, and to also prevent against replay attacks***.

EX1032, [0145]; *see also* [0268] (same); [0223] ("Sending a key value may be safer, should an attacker intercept the key value."); [0249] (Law explaining to "send[] a key value (called Kpan) that the mobile device can use to generate an identical virtual card PAN as computed by the payment gateway server 506"); [0270] ("the PAN keep[s] changing with ***each*** transaction").

Spodak (a reference relied upon by Petitioner in Ground 2A) further confirms why a POSITA would not have sought to repeatedly use Gomez's static EPIC account number (rather than Law's one-time-use Kpan to generate a new, different PAN) in a payment transaction. Spodak explains that the former is vulnerable to replay attacks known to be a problem in contactless transactions such as in Law: "Another example of using the non-standardized portions of the tracks includes using a dynamic authentication value to authenticate the transaction. To *prevent*

fraudulent transactions, traditional contactless cards can generate dynamic data every time they are read. Dynamic data generation per read *provides logical security and inhibits fraudulent replay* of contactless card data that may have been previously read." EX1009, [0094].

Yet Petitioner never addresses how its proposed combination would "prevent against replay attacks," which are a problem in contactless transactions, like in Law (as opposed to traditional magnetic swipes which are the focus in Gomez). Thus, using Gomez's static EPIC account number would leave vulnerable that information (and Law's system in general) if "compromised," rather than "prevent unauthorized actors from exploiting any compromised portion of the payment" or "prevent[] fraudulent use of a substitute or incorrect account number" as Petitioner incorrectly asserts (Pet., 14-15).

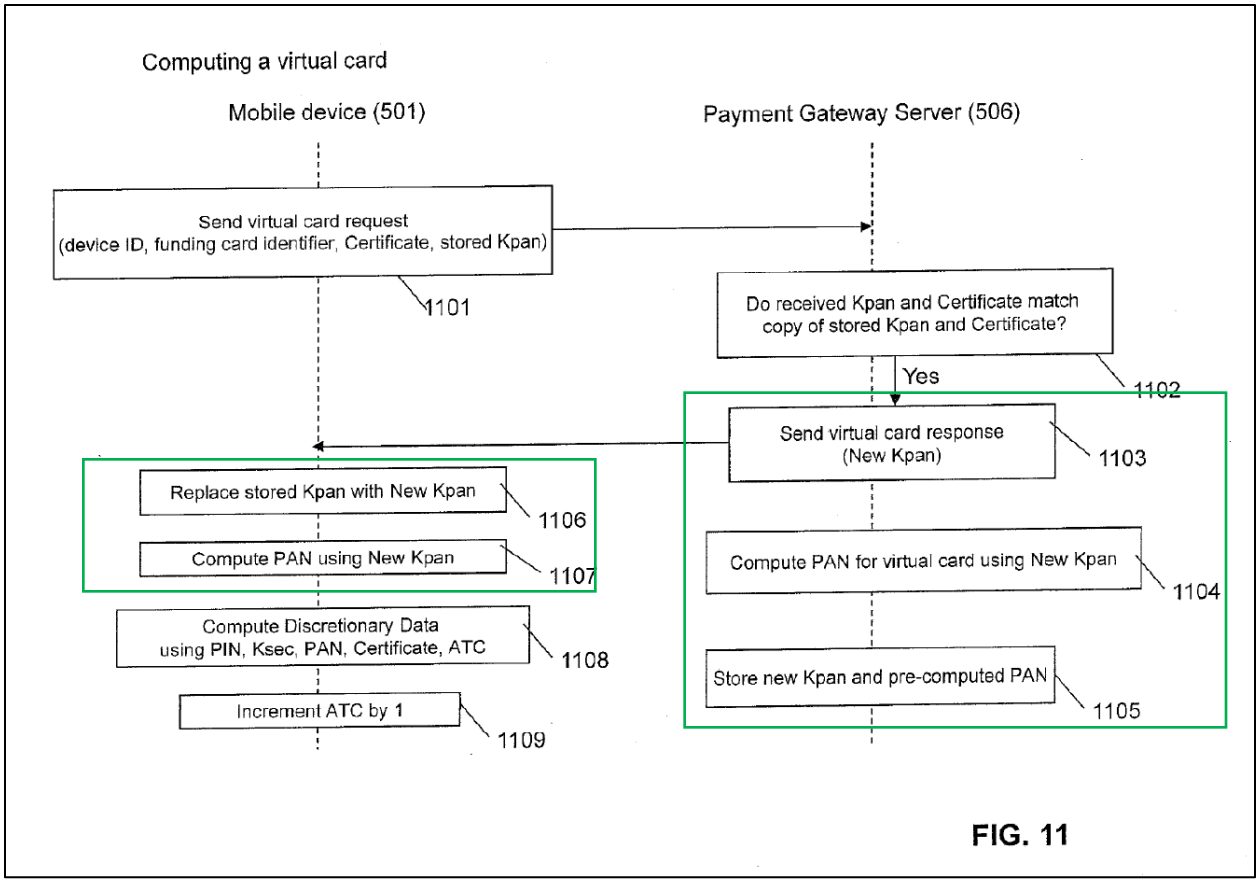
Second, Petitioner's assertion that using Gomez's EPIC account number would enable "a payment processing authority [to] more easily identify the user's actual account number for processing a transaction with the presence of the user's tokenized static account number in the payment information because that tokenized static account number is linked to the user's actual account" (Pet., 15) is both wrong and unnecessary in view of Law's teachings. In support, Petitioner points to Law (EX1032, [0082]), but that paragraph does not support Petitioner's position, as it says nothing about how the payment processor in Law identifies the user's actual

account number. Nor does Petitioner's other citation to Gomez (EX1007, 5:13-18) support the assertion. That portion of Gomez discloses only that "an EPIC payment card uses a fully static payment card number, but generates an authentication cryptogram for each attempted transaction only after the card holder successfully presents a credential, such as a fingerprint or PIN number, into the payment card." EX1007, 5:13-18. Its expert repeats the same thing, verbatim. EX1003 ¶128.

There is no support for Petitioner's conclusory assertion. But more importantly: it is contradicted by Law. There is no need to use an EPIC account number because Law teaches to use a *different* PAN (generated for each payment transaction using a *new* Kpan) transmitted from the mobile device to the payment gateway server during each transaction, at which point the payment gateway server computes and matches that PAN using its own stored Kpan (as well as discretionary data, etc.) to confirm the transaction is valid and should proceed. EX1032, [0156]-[0165]; *see also* [0223], [0249], [0268], [0270].

For example, Law teaches in Figures 11 and 12 (the latter being a continuation of the former (EX1032, [0156])) to compute a different PAN using the new Kpan as part of each transaction. Figure 11 of Law, below, depicts "an example embodiment of computer executable or processor implemented instructions are provided for computing virtual card data." EX1032, [0144]. "The request includes the device ID, the identifier of the selected funding card, the Certificate and the stored Kpan,"

which "stored Kpan can be from registration or from the previous transaction." EX1032, [0144]. "The payment gateway server 506 determines if the ***received Kpan*** and Certificate ***match the Kpan*** and Certificate stored on the payment gateway server (block 1102) associated with the DeviceID stored in the payment gateway server database." EX1032, [0145]. "If so, then the payment gateway server 506 sends a virtual card response to the mobile device 501 that includes a ***new Kpan*** (block 1103)," whereby "[a] ***new Kpan*** is used to generate a ***different PAN*** from the previous transaction, and to also prevent against replay attacks." EX1032, [0145]. This new Kpan is stored both at the mobile device and payment gateway server (at blocks 1105 and 1106) for "later use" (*i.e.*, for use as part of computing a different PAN transmitted during a payment transaction as in Figure 12). EX1032, [0145]-[0146]. Law explains "[i]f the conditions and data are correct, although the mobile device computes the PAN independently of the payment gateway server, the PAN computed by the mobile device should be ***identical*** to the PAN computed by the payment gateway server." EX1032, [0146]. In other words, the "new" Kpan at the mobile device and payment gateway server are identical (as reflected in **green** below) and then used to compute the new "different PAN" transmitted and used as part of each new payment transaction (as in Figure 12).



EX1032, FIG. 11.

Turning to Figure 12 of Law, below, Law depicts "an example embodiment of computer executable or processor implemented instructions … provided for verifying virtual card data, and in particular the verification by the payment gateway server of the discretionary data (e.g. the dynamic data)." EX1032, [0156]. Figure 12 "can be used in combination with the principles described above for verifying the virtual card data" and as "a continuation of [Figure] 11" (*i.e.*, above describing verification using the new Kpan in each payment transaction). EX1032, [0156]. As part of the process, the mobile device sends a payment authorization request (block

1201) including a PAN (referencing to Figure 11, a new "different PAN" generated using the Kpan) along with discretionary data. EX1032, [0157]. The payment gateway server receives the request and compares the received PAN to stored PANs, "and if a match is found … then the stored data associated with that given precomputed PAN is considered the relevant stored associated data" and the payment gateway server continues to confirm the other data (e.g., discretionary data) to verify the transaction. EX1032, [278]. "[A]fter the data is successfully verified or not, the payment gateway server eventually respond[s] to the merchant by sending an authorisation response to the merchant (103,502) (block 1207)." EX1032, [0166]. As Law explains, "[i]f successfully verified, the funding card details associated with the virtual card are retrieved and sent to the funding card issuer server via the payment network to complete the payment authorization transaction." EX1032, [0077]; *see also* [0117] ("payment gateway server retrieves the funding card data that is associated with the virtual card data card" after successful validation); [0175]. In other words, Law teaches exactly how to process a transaction using the data transmitted as part of the payment authorization request; adding additional data in the form of Gomez's EPIC account number, as proposed by Petitioner, would not be unnecessary and redundant (as well as less secure).

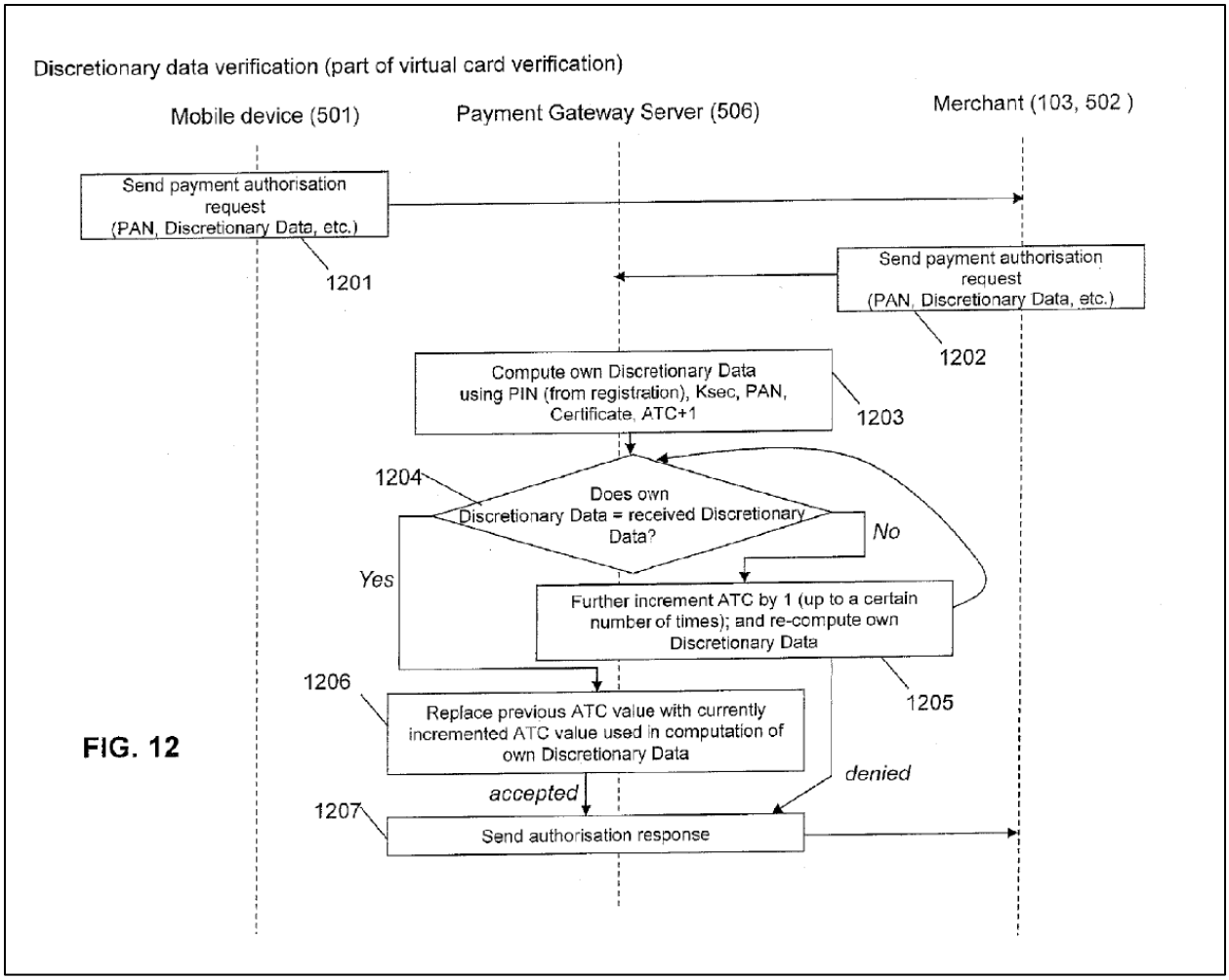


FIG. 12

EX1032, FIG. 12.

Third, Law's system specifically does "*not* rely on having a software payment card stored on the secure element on the mobile device to facilitate contactless payment transaction." EX1032, [0167]. Per Law, "[t]his is because the PAN, and the other card data elements of the funding card are *not* stored on in the mobile device" and "[i]nstead the PAN and expiry date of the funding card is stored on a secure server (e.g. the payment gateway server)." EX1032, [0167]. Law also discloses that "[t]he virtual card data is *only* sent at the time of making the payment, and can *only*

be used once," and that "*only* the server can validate the virtual card data." EX1032, [0167]. "In other words," as Law explains, "there is *nothing* for an adversary to access via brute force on the mobile device without being detected." EX1032, [0167]. In Petitioner's proposed combination, however, all these advantages would be lost, as static information would be stored on and transmitted by the mobile device—exactly what Law teaches not to do. This too would leave the system vulnerable to various attacks by an adversary.

In short: there is no reason why a POSITA would have sought to include Gomez's EPIC account number in Law's system, and in fact, doing so would be at odds with and unnecessary in Law.

3. Petitioner Fails to Meet its Burden of Showing that its Proposed Combination has a "Static *Device* Account Number" that is Wirelessly Received as Required by Limitations [10.d] and [10.g].

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;" and
- [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."

Petitioner's obviousness theory is premised on the assertion that Gomez's "EPIC *payment account* number" corresponds to the claimed "status *device* account number." While for limitation [10.d], Petitioner appears to assert either Law's "funding card identifier" or Gomez's "EPIC payment account number" could be the "static device account number" (Pet., 23-26), for limitation [10.g] Petitioner relies *exclusively on Gomez* (Pet., 31-34). For example, in its obviousness combination assertion for limitation [10.g] Petitioner equates Gomez's EPIC number as being the "static device account number": "As taught in Gomez, the payment device of the Law-Gomez combination renders obvious use of the EPIC number, or static payment card identifying number (i.e., the static device account number) and authentication cryptogram (i.e., the dynamically generated one-time limited-use number) in making a payment transaction." Pet., 31-32. Nowhere does Petitioner mention (let alone rely on) Law's "funding card identifier" as part of its assertion for limitation [10.g]. The exclusive reliance on Gomez is also consistent with Petitioner's alleged motivation to combine Law and Gomez to apply Gomez's EPIC account number to Law. *See* Pet., 14-15. Thus to meet its burden, Petitioner must show that Gomez's EPIC payment account number is a "static *device* account number" and in its combination would be received wirelessly for storage on the electronic device. Petitioner has failed on both accounts.

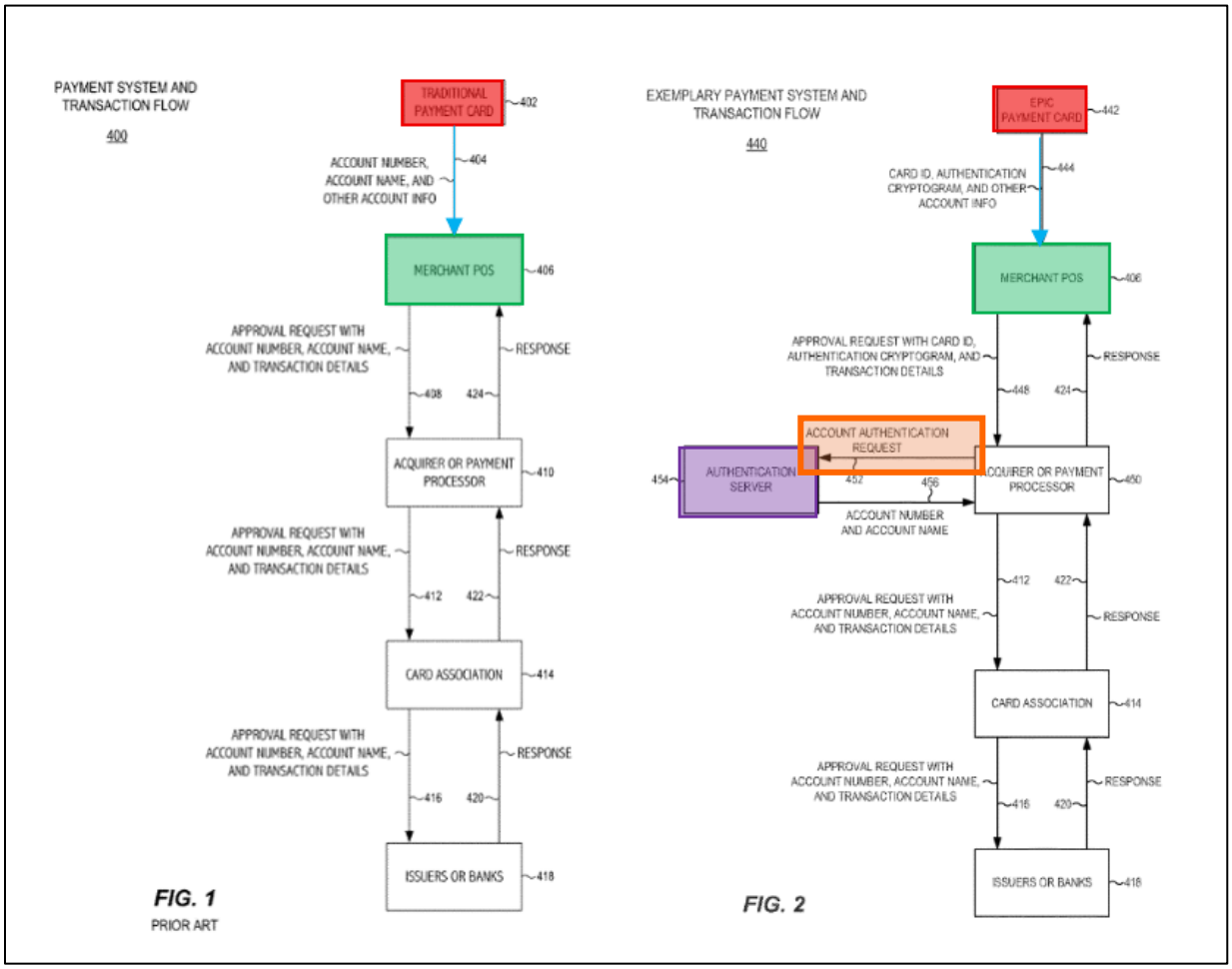
a. Gomez's EPIC payment account number is not a "static device account number"

Petitioner equates Gomez's EPIC payment account number with the claimed "static device account number." That is wrong; Gomez confirms that its EPIC payment account number is simply an account number and has nothing to do with any particular device at all.

To begin, Gomez discloses an EPIC account number, which per Gomez is "an identifying number for an EPIC *account*" that is, in turn, "linked [to] one or more live payment card accounts." EX1007, 5:7-24, 6:7-22, Abstract.[9] 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 EPIC number is "'left behind'" and "readily observable." EX1007, 5:32-39; *see also* 13:63-65 ("the payment card identif[ication] number [is] visible to merchant employees and left behind after a transaction").

[9] Gomez briefly mentions that the number could be a "live" account number, but Petitioner does not (and cannot) rely on this part of the disclosure.

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, FIGs 1-2.



EX1007, FIGs. 1-2.

As Gomez explains, in its EPIC system, "*[n]o changes* in the payment system infrastructure need be made by either the point-of-sale merchant or the card issuer." EX1007, 2:40-41; *see also, e.g.*, 2:42-45, 5:32-34, 5:67-6:2, 10:8-17, 14:3-11. That is, Gomez specifically makes no modifications to the merchant POS or card

issuer systems to implement its "EPIC payment card." Such **EPIC payment card 442** includes a rewritable magnetic stripe on which the EPIC card number may be encoded in the account number field and the authorization cryptogram may be encoded in the account name field—akin to **traditional payment card 402** of the prior art system in Figure 1. EX1007, 5:48-57, Abstract. **EPIC payment card 442** may be swiped through a POS terminal "just like a traditional magnetic stripe payment card." EX1007, 5:29-34.

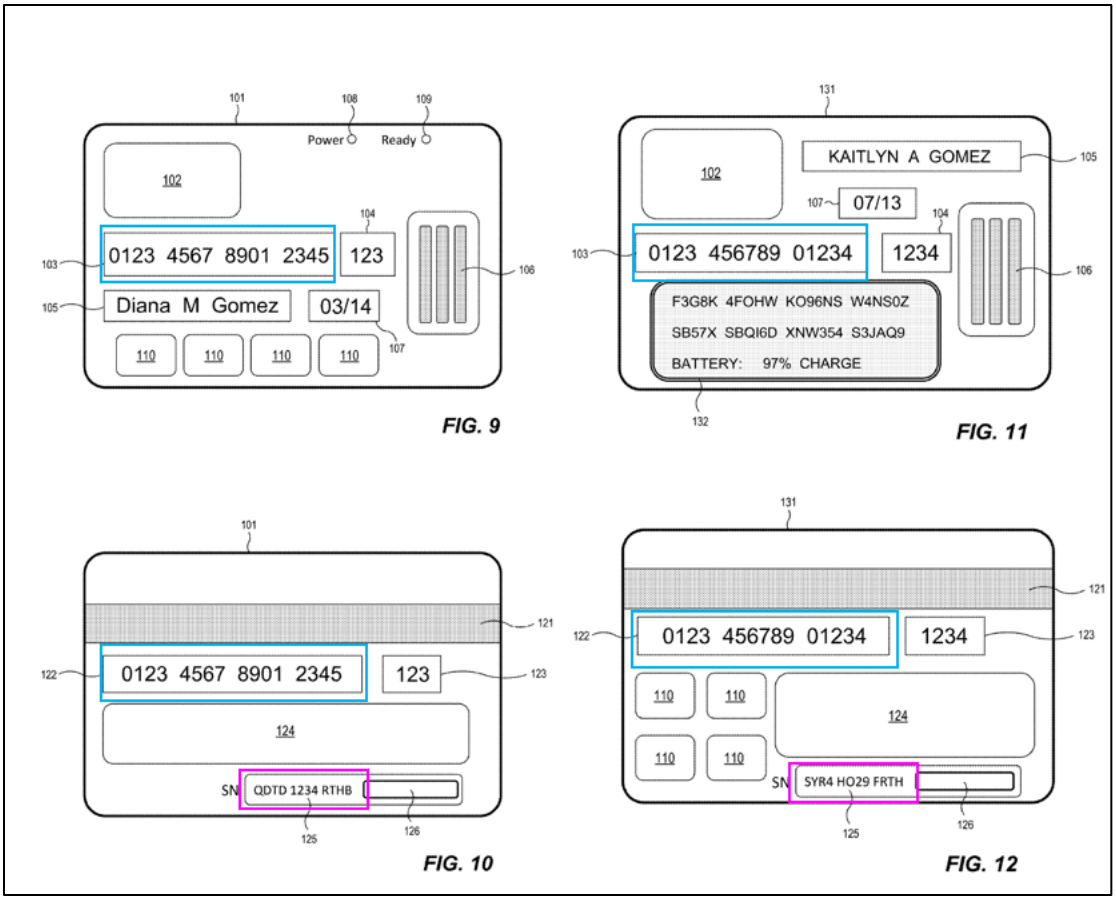
Indeed, the only change in Gomez's EPIC system (Figure 2) relative to the "prior art" system (Figure 1) is that the payment processor communicates with an additional **authentication server** to obtain the account number and account name. EX1007, 3:18-23, 3:65-67, 5:48-50, FIGs. 1-2. This can be seen in comparing Figures 1 and 2 and the corresponding disclosure. In Figure 2, the "**account information 444**"—including the EPIC account number and cryptogram—are provided via a traditional "swiping [of] the payment card" through a "traditional POS terminal." EX1007, 5:61-67; *see also* 5:67-6:2 ("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.").

According to Gomez, "as before" (*i.e.*, as in the prior art), **merchant 406** combines **account information 444** and the transaction information which is sent to the acquirer 450 and also "[a]s before, the acquirer 450 analyzes the *account*

number [i.e., the EPIC account number] conveyed in the inbound approval request 448 to determine the appropriate card association or entity to next process the transaction approval request." EX1007, 6:7-10 "[T]he *account* number would be recognized as an EPIC *account* number (or at least the first portion of an EPIC account number)." EX1007, 6:10-12. An "**account authentication request 452**" is created, which includes "the EPIC *account* number, the date and time of the transaction, and the authentication cryptogram" and is sent to **EPIC authentication server 454**. EX1007, 6:13-22. **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," such determination being "accomplishe[d] … 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, 6:23-32. "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 communicated back to the acquirer 450." EX1007, 6:32-38. That

is, the EPIC account number has nothing to do with a device; it is simply a user's account number linked to one or more actual "live" credit card account numbers.

Further confirming the EPIC account number is not a "static *device* account number," and rather just an account number generally, Gomez depicts various fronts and backs of its EPIC cards in, *e.g.*, Figures 9-12 (below with fronts depicted in Figures 9 and 11 and backs in Figures 10 and 12). The EPIC account numbers are shown in **blue** boxes, below, "as with many traditional payment cards." EX1007, 11:19-27, 11:63-66, 12:41-45, 13:5-10, 13:14-19, 13:34-39. "A fully static (16-digit) account number and (3-digit) security code," as with traditional cards, "are preferably utilized." EX1007, 13:49-52. In other words, the EPIC account number is hard-encoded onto the payment card.



EX1007, FIGs. 9-12.

As shown in Figures 10 and 12 (above), the cards include a "**serial number**" (element 125) on the back of the card. If a card is lost, stolen, etc. and a replacement card is issued, a new serial number is generated for the replacement card, which "allows these two cards [the lost, stolen, etc. card and the replacement card] to be distinguished…." EX1007, 12:24-40. Indeed, Gomez specifically adds a serial number to the card, so that in the event a card is lost or stolen, the new and old cards can be distinguished:

> A **serial number region 125** provides space to include a serial number printed on the card. This is particularly useful since the card memory contains information which is not discernable from the front or back face of the card…. [I]f that given payment card is lost, stolen, damaged, or otherwise compromised, ***a replacement card associated with that particular payment card account*** may contain a different seed value than the seed value in the compromised card. ***A serial number allows these two cards to be distinguished without compromising the security of the payment card***.

EX1007, 12:24-36.

Gomez includes a serial number to distinguish a new and old card because the EPIC account number stays the same (as necessarily and obviously preferable so that a user does not have to change their account information, re-link live credit card accounts to a new number, or update information for auto payment schedules, such as for utility bills). Indeed, despite disclosing a change of serial numbers, Gomez never discloses—nor would it make sense in Gomez—that the EPIC account number is ever changed. Moreover, the EPIC account number is printed right on the face of the card (*e.g.*, as in Figures 9-12, above); if a new card had a different number, there would be no reason for a serial number at all. A user could distinguish the cards just by the EPIC numbers if they changed from card to card.

In contrast, when Gomez wanted to indicate that a number was device-specific or unique, Gomez said so. The "seed value" is such an example; Gomez repeatedly explains that it is "unique" for each payment card. *See, e.g.*, EX1007, 7:27-28 ("Th[e] seed value is unique for each payment card…"), 16:66-17:1 ("In some embodiments, each payment card may utilize a unique, static seed value for that card…"). The customer key is another example, albeit unique to a customer. EX1007, 7:35-36 (referring to "customer specific information, such as a unique customer key"). Gomez *never* refers to the EPIC number as unique to anything.

In reality, the EPIC number is purely an account number—it is not a "static device account number"—and has nothing to do with any particular device at all. Thus, Petitioner's Grounds 1A and 1B challenges fail.

b. Gomez's EPIC payment account number would not have been received wirelessly

Petitioner asserts that Gomez describes communicating payment card information via NFC, which is wireless. Pet., 25 (citing EX1007, 7:49-54). This is a *one-way* communication *from* the card *to* the merchant POS, where the payment card *transmits* data to the merchant POS. *See also* Section III.B above (Gomez overview).

That is the opposite of the data flow claimed for limitation [10.d], which requires "*receiving* wirelessly a static device account number payment information for storage on the electronic device." Petitioner never explains how (or why) an EPIC payment account number (the alleged "static device account number") would

be received wirelessly for storage on the device, when the only disclosure in Gomez is that it *transmitted from the payment card*. Moreover, there is no need in Gomez to receive wirelessly the EPIC account number, because as explained in Section VI.A.3.a, above, it comes hard-encoded onto the card.

The same would apply to Law, and for good reason. As both Law and Spodak disclose (and as explained in Section VI.A.2, above), a POSITA would *not* have transmitted wirelessly a static account number and then used that same number in a transaction because, among other problems, it would leave the system vulnerable to replay attacks and interception. *See also* EX1032, [0145], [0223], [0249], [0268], [0270]; EX1009, [0094].

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

Petitioner's Ground 2A asserts that claims 18-24 are obvious over a four-reference combination of Gill, Smith, Kay, and Gomez. This combination fails because Petitioner has not met its burden of proof to demonstrate a POSITA would have sought to make the proposed combination for multiple reasons.

1. Petitioner's Ground 2A Rehashes the Same Four-Reference Combination Used in a Recently Denied Petition Challenging the Same Claims.

Petitioner relies on the *same* four reference combination (*Gill-Smith-Kay-Gomez*) that was part of another IPR petition filed by Apple that was recently denied. EX2026, 55-65 (Apple's IPR Petition in IPR2025-01146 challenging claims 18-24

of the '520 Patent using the same combination). Patent Owner explains below exemplary problems with Petitioner's Ground 2A including that (i) it would not have been obvious to combine Gill, Smith, and Kay, and (ii) it would not have been obvious to further add Gomez to the Gill-Smith-Kay combination.

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., 44-51. 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 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.C 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* EX1034, Fig. 1, *with* EX1035, Fig. 1; *see supra* Sections III.C-D. As Gill explains (and

summarized above in Section III.C), 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 technology[10] 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

[10] Again, Gill claims priority to a non-provisional filed September 6, 2012, and a provisional filed March 4, 2011. EX1034, Cover Page. Smith claims priority to a non-provisional filed March 1, 2013, and a provisional filed March 1, 2012. EX1035, Cover Page.

> 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.

EX1034, 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. EX1034, 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." EX1034, 4:56-5:20. 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." EX1034, 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)." EX1034, 4:35-55.

Petitioner's proposed combination does not account for *any* of Gill's teachings distinguishing between ATM and POS transactions (discussed in this Section V.B.2, as well as in Section III.C 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 a motivation to combine, or reasonable expectation of success in combining, Smith and Gill. *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., 46), 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., 47. However, Gill explains that ATM transactions require "security verification," whereas POS transactions, like in Smith, do not. EX1034, 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* EX1034, 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* EX1035, [0034] (explaining that Smith's

mobile device does not store the real card account number, which "reduc[es] the potential for fraud."). 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., 47); 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 is not explicit in describing 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., 45), 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., 45. 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 [account] information to the ATM terminal via a contactless/wireless connection when a user 'taps' the mobile device at the ATM." Pet., 56 (citing EX1034, 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., 56. 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., 56 (citing EX1034, 13:41-46; emphasis added). 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 "[i]ntegrating Smith's suggested use of payment credentials, including at least an MCA and payment cryptogram, in ATM transactions like Gill's would have amounted to an obvious application of known techniques to improve a similar system in substantially the same way as described in Smith, and would have achieved merely predictable results (e.g., more

secure transactions)" (Pet., 48), is not sufficient to explain how or why a POSITA would want to look to Smith (a non-ATM reference), and much less how or 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.B.2 and in Section III.C.

Therefore, for these reasons, Petitioner has failed to meet its burden to show a reasonable likelihood of success for claims 18-24 in Ground 2A.

3. Petitioner Fails to Show That It Would Have Been Obvious to Add Gomez to the Gill-Smith-Kay Combination.

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., 52-64.

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., 52. 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 itself 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.B.2. 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., 52-54. 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., 53-54, 70), 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.C, V.B.2), are vastly different from ATM transactions. Thus, for the same reasons as explained above in Sections III.C. and V.B.2, 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*."); 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.").

Thus, Petitioner has failed to show a reasonable likelihood of success for claim 18-24 in Ground 2A for these additional reasons.

VII. CONCLUSION

Petitioner has failed to show a reasonable likelihood of success for any Challenged Claim. Institution should be denied.

Dated: December 15, 2025

Respectfully submitted,

/Matthew G. Berkowitz/

Matthew G. Berkowitz (Reg. No. 57,215)
mberkowitz@reichmanjorgensen.com
REICHMAN JORGENSEN
LEHMAN & FELDBERG LLP
Lead Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE

I hereby certify that this paper complies with the type-volume limitation of 37 C.F.R. §42.24 (as determined by the Microsoft Word word-processing system used to prepare this paper) because it contains 13,979 words, excluding the parts of the paper exempted by 37 C.F.R. §42.24(a).

Dated: December 15, 2025 */Matthew G. Berkowitz/*

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

CERTIFICATE OF SERVICE

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

Naveen Modi (Reg. No. 46,224)
Daniel Zeilberger (Reg. No. 65,349)
Robert Laurenzi (Reg. No. 45,557)
Jason Mikus (Reg. No. 71,911)
Alexa Lowman (*pro hac vice* to be filed)
Maksim Mints (Reg. No. 78,507)
PH-Google-Cardware-IPR@paulhastings.com
naveenmodi@paulhastings.com
danielzeilberger@paulhastings.com
robertlaurenzi@paulhastings.com
jasonmikus@paulhastings.com
alexalowman@paulhastings.com
maksimmints@paulhastings.com

Dated: December 15, 2025

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