

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner

v.

CARDWARE INC.,
Patent Owner

Case No. IPR2025-01344
Patent No. 10,810,579

CARDWARE’S PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The '579 Patent.....	5
III.	Petitioner's Alleged Prior Art.....	7
	A. Royyuru	7
	B. Phillips	10
	C. Gomez.....	11
	D. Amacker.....	16
IV.	Level of Ordinary Skill in the Art.....	19
V.	The Petition Fails to Establish a Reasonable Likelihood of Success as to Any Challenged Claim	19
	A. Grounds 1A-1F: The "Royyuru"-Based Grounds.....	19
	1. Royyuru Does Not Teach Limited-Use Payment Information for Use "in Place of" Card Issuer Payment Information	19
	2. A POSITA Would Not Have Combined Royyuru with Phillips34	
	B. Grounds 2A-2E: The "Gomez"-Based Grounds	42
	1. Gomez Does Not Teach Limited-Use Payment Information for Use "in Place of" Card Issuer Payment Information	43
	a. Petitioner's Theory Relies on Gomez's "Manual" Embodiment, But This Embodiment Requires Use of the Actual (Real) Payment Card Information, as Petitioner Effectively Admits in Another IPR Petition.....	44
	b. If Gomez Does Not Teach How the Selected Credit Card Number is Used Throughout the "Manual" Process, Petitioner's Proposed Combination is Inoperative, Unworkable, and Unexplained	51

2.	A POSITA Would Not Have Sought to Modify Gomez with Amacker to Receive an NFC Transaction Payment Request; Gomez Teaches Away from and Expressly Discourages the Proposed Combination	54
VI.	Conclusion	71

TABLE OF AUTHORITIES

Page(s)

Cases

<i>AT&T Servs., Inc. v. Innovative Sonic Ltd.</i> , IPR2024-01143, Paper 15 (PTAB Feb. 11, 2025).....	38, 50, 54, 69
<i>Chemour Co. FC, LLC v. Daikin Indus., Ltd.</i> , 4 F.4th 1370 (Fed. Cir. 2021)	66
<i>DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.</i> , 567 F.3d 1314 (Fed. Cir. 2009).....	66
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016).....	39
<i>PayPal, Inc. v. IOENGINE, LLC</i> , IPR2019-00930, Paper 16 (PTAB Oct. 29, 2019)	50, 54
<i>Precision Cancer Techs. Inc. v. Oncoustics Inc.</i> , IPR2025-00242, Paper 7 (PTAB June 3, 2025).....	38, 69
<i>Samsung Elecs. Co. Ltd. v. Mojo Mobility Inc.</i> , IPR2023-01100, Paper 11 (PTAB Feb. 12, 2024).....	50, 54
<i>Solus Advanced Mat’ls Co. Ltd. v. SK Nexilis Co., Ltd.</i> , IPR2024-01462, Paper 14 (PTAB Apr. 25, 2025).....	39
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022)	38, 69

PATENT OWNER’S UPDATED EXHIBIT LIST

No.	Exhibit Description
2001	Memorandum for Interim Processes for PTAB Workload Management, dated March 26, 2025
2002	Interim Director Discretionary Process <i>available at</i> https://www.uspto.gov/patents/ptab/interim-director-discretionary-process
2003	First Agreed Scheduling Order in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2004	Complaint in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2005	Order and Advisory in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Nov. 5, 2024)
2006	Order Denying Defendants’ Motion to Stay in <i>Quantum Imaging, LLC v. Sony Interactive Entm’t Inc.</i> , No. 1:23-cv-1212-ADA-DTG (W.D. Tex. Dec. 4, 2024) (Gilliland)
2007	Agreed Scheduling Order in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. May 20, 2025)
2008	Complaint in <i>CardWare Inc. v. Apple Inc.</i> , 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 <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Aug. 15, 2025)
2011	Claim Construction Memorandum and Order in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Aug. 28, 2025)
2012	Order Denying the Defendant’s Motion to Transfer Venue to the Northern District of California in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Aug. 7, 2025)
2013	Claim Construction Order in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Aug. 29, 2025)
2014	Email from counsel for Petitioner to counsel for Patent Owner, dated Aug. 21, 2025
2015	Defendant Google LLC’s Invalidity Contentions in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Apr. 3, 2025)
2016	Exhibit I to Defendant Google LLC’s Invalidity Contentions in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Sept. 18, 2025)

No.	Exhibit Description
2017	DocketNavigator Time to Trial Statistics for Patent Cases in the Western District of Texas
2018	Defendants’ Notice of Subpoena to Google in <i>CardWare Inc. v. Samsung Elecs. Co., Ltd.</i> , 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 <i>Inter Partes</i> Review of Pat. 10,339,520 in IPR2023-00210, by Petitioner Samsung Electronics Co., Ltd.
2022	Petition for <i>Inter Partes</i> Review of Pat. 10,810,579 in IPR2023-00196, by Petitioner Samsung Electronics Co., Ltd.
2023	Order Adopting Report and Recommendation Denying The Defendants’ Motion to Dismiss in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Sept. 3, 2025)
[New] 2024	U.S. Patent App. Pub. No. 2015/0134540 to <i>Law</i> (Exhibit 1032 to Petitioner’s Petition in IPR2025-01361)
[New] 2025	Petitioner’s Petition for <i>Inter Partes</i> Review in IPR2025-01361 (Paper 1)

I. INTRODUCTION

On July 24, 2025, Google LLC (“Google” or “Petitioner”) filed a Petition requesting *inter partes* review of claims 1-23 (“Challenged Claims”) of U.S. Patent No. 10,810,579 (“the ’579 Patent”) (EX1001), entirely on obviousness Grounds. Paper 1 (“Petition” or “Pet.”). On August 7, 2025, the Board issued a Notice of Filing Date Accorded for the Petition and set the time for filing Patent Owner’s Preliminary Response. Paper 5.

The Board should deny institution because Petitioner fails to meet its burden of demonstrating that its prior art references render obvious any of the Challenged Claims. Petitioner’s Grounds 1A through 1F (which rely on Royyuru as the primary reference), and Grounds 2A through 2E (which rely on Gomez as the primary reference), are missing key limitations and regardless, a POSITA would not have sought to combine the references as proposed by Petitioner.

First, for **Grounds 1A-1F**, Petitioner fails to show the proposed combinations disclose using generated limited-use payment information “in place of” card issuer payment information, as in elements [1.i], [15.d], and [19.k]. For this limitation, Petitioner relies exclusively on Royyuru. But Royyuru doesn’t disclose replacing card issuer payment information with generated limited-use payment information. Instead, Royyuru simply teaches an improved process for more securely encrypting the card issuer payment information (*i.e.*, the real primary account number (“PAN”))

that is still used throughout the transaction (initially sending it in encrypted form and then decrypting after receipt).

Second, also for **Grounds 1A-1F**, Petitioner fails to show how a POSITA would have combined Royyuru with Phillips while retaining the features of each system that Petitioner relies upon. For example, Royyuru's system, including its use of an Institution Key Card Variant ("IKCV"), is designed to have a single account from a single issuer per payment card or device, whereas Phillips' system, including its features for selecting from among different payment cards, is designed for multiple accounts from multiple issuers on a single device. Petitioner fails to show how the proposed Royyuru and Phillips combination would work when re-imagining Royyuru as a multi-card and multi-issuer device. Petitioner's theory also rests on conclusory expert testimony, lacking in evidentiary support. And Petitioner's expert glosses over as "minor" that the proposed combination would require, *e.g.*, increased storage. While Petitioner entirely omits from the Petition this alleged "minor increase," the record shows that it (and other problems) are anything but minor. Rather, they are fundamental considerations in utilizing mobile devices for payment transactions that further demonstrate Petitioner has failed to meet its burden.

Third, for **Grounds 2A-2E**, Petitioner's proposed combinations fail to disclose using generated limited-use payment information "in place of" issued payment information in connection with the payment transaction, as in elements

[1.i], [15.d], and [19.k]. Petitioner relies exclusively on Gomez for this requirement. Petitioner's challenge, however, mixes and matches Gomez's "manual" and "automatic" embodiments. The "manual" embodiment of Gomez is critical to Petitioner's position regarding elements [1.f], [15.c], and [19.j] (and overall obviousness theory) because it is the only Gomez embodiment meeting that limitation requiring that issued payment information is "display[ed]" and "select[ed]." But, unlike the "automatic" embodiment, Gomez never explains what information is transmitted to a merchant in connection with the "manual" embodiment, including whether that is actual payment information or something "in place of" it. In a co-pending IPR Petition, Petitioner admits this, stating that Gomez "describes how a user may manually choose which of the actual credit/debit cards to use at the moment of a transaction" but "does not explicitly disclose how the selected actual credit/debit card payment information is communicated to the merchant and EPIC authentication server during a transaction." EX2025, 53-54. All indications from Gomez suggest that in "'Manual' mode," the *actual* payment information is transmitted in connection with the payment transaction (and nothing is "in place of" it). But regardless, Petitioner has failed to meet its burden on elements [1.i], [15.d], and [19.k] and does not offer any reason why (or how) a POSITA would combine the Manual and Automatic mode disclosures from Gomez.

Lastly, for **Grounds 2A-2E**, Petitioner fails to show that a POSITA would have modified Gomez with Amacker to receive a request for transaction payment via an NFC interface. Gomez discloses a payment card designed to work with a traditional payment infrastructure and transaction flow including a magnetic stripe whereby “[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. Yet, Petitioner’s proposed combination ignores all this and requires the exact changes Gomez teaches against. Petitioner reimagines Gomez’s payment card as either a mobile device or super-charged payment card complete with touchscreen and other capabilities. But the mobile device would not work because Gomez envisions that the payment instrument would maintain magstripe swiping capabilities. And Petitioner’s super-charged payment card is pulled from thin air; Amacker does not say anything about this (or any card for that matter), and does not provide any disclosure that might teach a POSITA how to build out the EPIC card in the way that Petitioner imagines. For example, Petitioner imagines that the new payment card would receive a transaction payment via an NFC interface. Gomez says nothing about this (and regardless, such a change would require a change in the transaction flow at the merchant POS, which Gomez teaches against). Amacker also says nothing about this—not one thing. It is entirely made up with hindsight reconstruction by its expert.

Both the Royyuru-based and Gomez-based combinations fail to disclose all of the claim limitations, the proposed combinations are otherwise unworkable, and a POSITA would not have sought to make such combinations. Accordingly, Patent Owner respectfully submits that Petitioner has failed to show a reasonable likelihood of success for any Challenged Claim and that institution should thus be denied.

II. THE '579 PATENT

The '579 Patent is generally directed to “multi-function electronic devices or smart cards and, more particularly, ... methods of smart tokenizing payment cards and devices.” EX1001, 1:23-27. The '579 Patent recognizes that “[s]ecurity is an area of concern for credit card holders, as the small form factor makes theft quite easy, and additionally there are many ways for a malicious third-party to record the account number of a credit card in order to later make fraudulent transactions on the account.” EX1001, 9:9-13. The claimed invention “address[es] security concerns of a credit card owner on several fronts.” EX1001, 9:13-15.

For example, the '579 Patent teaches that security may be enhanced by “locking” the credit card to prevent use until, for example, an identified valid user input is entered. EX1001, 9:14-19. The user activates or “primes” the device to perform a transaction by providing an input such as a password or a gesture. EX1001, 9:40-48, 15:16-32.

As another example, the device produces a “limited-duration credit card number” and uses it for performing transactions. EX1001, 10:4-7. In contrast to traditional credit cards that displayed and used a completely static number in transactions, the credit card device of the ’579 Patent may have “no fixed number,” such that “[o]nly the number generated at the instant of the credit card transaction matters.” EX1001, 10:49-56. “The limited-duration credit card number is able to be generated according to the selected account, a timestamp, a transaction amount, an indicated merchant, user key or secrets, on-card unique hardware secrets, credit card authority key or secrets, user input from the card interface, and other information associated with the transaction.” EX1001, 7:12-18.

The ’579 Patent also teaches that a single device can conveniently be used for multiple banks or financial institutions “instead of carrying a separate credit card for each account.” EX1001, 6:49-54. The accounts stored on the device may be displayed, and the user selects an account, such as by keypad or touch sensor array. EX1001, 6:57-7:4.

Claim 1, for example, recites a method of performing a transaction that includes many of these features. Claim 1 recites receiving a “priming operation” of the electronic device; displaying “a card issuer payment method selection”; and generating “a limited-use payment information” and using it “in place of ... card issuer supplied payment information.”

III. PETITIONER’S ALLEGED PRIOR ART

Petitioner presents two sets of grounds: (i) Grounds 1A through 1F, based on Royyuru in combination with two or more additional references and (ii) Grounds 2A through 2E, based on Gomez in combination with two or more additional references.¹ As summarized below, Royyuru and Gomez—alone and in combination with other references—are fundamentally different than the inventions claimed in the ’579 Patent and fail to disclose key limitations, such as generating a limited-use payment information for use “in place of” card issuer payment information. Additional reasons why the Grounds fail are also provided below.

A. Royyuru

U.S. Patent App. Pub. No. 2010/0185545 (“Royyuru”) is directed to “methods and systems for utilizing dynamic cryptograms in a financial transaction.” EX1004, [0001]. Royyuru specifically sought to address certain problems resulting from attacks on encrypted forms of a real primary account number (“PAN”) that was transmitted and received during a payment transaction, including problems resulting from common and card-level keys being exposed. EX1004, [0004].

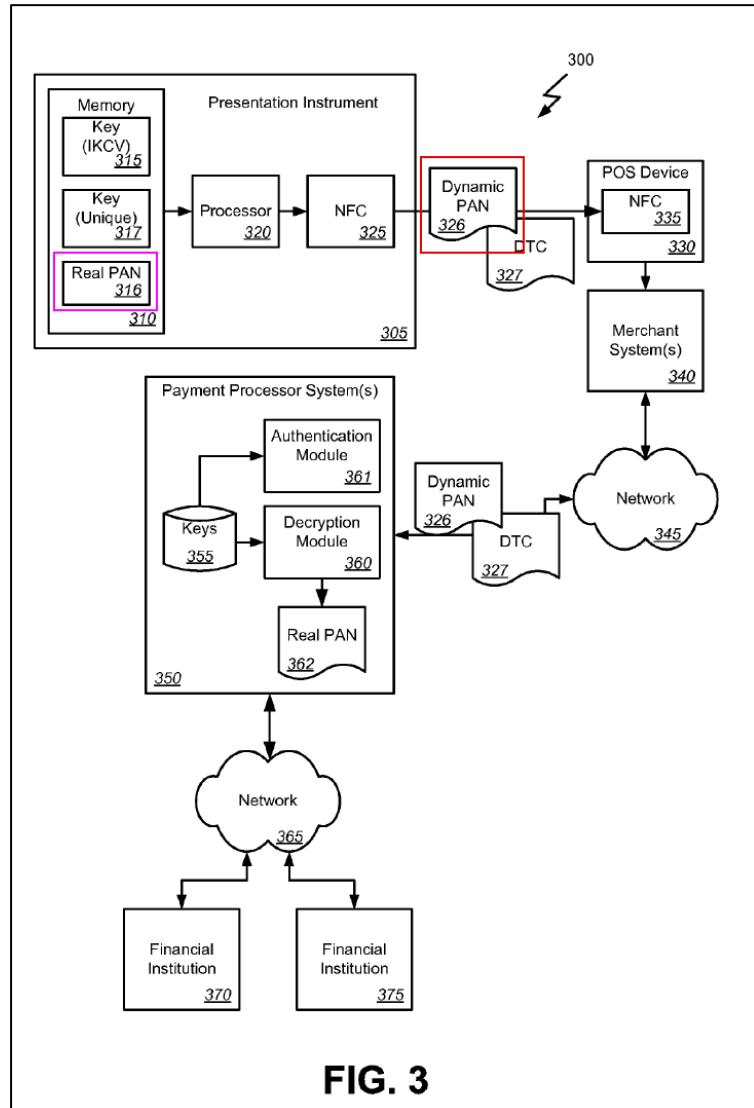
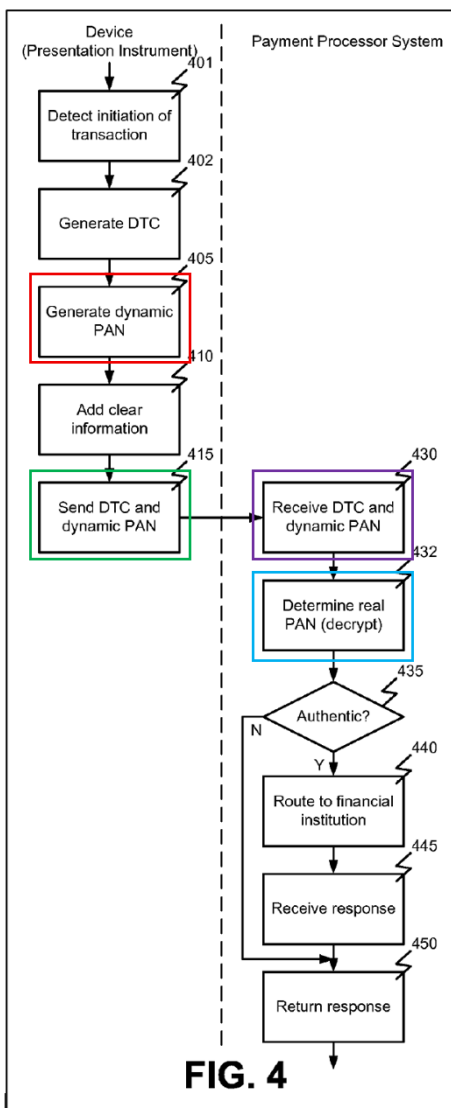
¹ Only the references relevant to arguments in this Preliminary Response are summarized here.

To do so, the device of Royyuru may generate (i) a “Dynamic Transaction Cryptogram (DTC)” and (ii) a “dynamic PAN” that comprises “an encrypted form of a real PAN of the financial account,” for use in financial transactions. EX1004, [0005]. The device stores information, including “a real Primary Account Number (PAN) for the financial account” and keys, such as an Institution Key Card Variant (IKCV), that are used to generate the DTC. EX1004 [0009]. “The IKCV can be generated when each card (device) is being customized,” and is based on the digits of the “card number (PAN).” EX1004, [0057].

As shown in Figure 4, reproduced below left, the device of Royyuru may provide the DTC and “dynamic PAN” (*i.e.*, an encrypted form of a real PAN) to a point-of-sale (POS) device, which then provides it to a payment processor system. EX1004, [0054] (steps 415 and 430). The payment processor system decrypts the dynamic PAN to obtain the “real PAN” (step 432); the “real PAN” can then be sent to a financial institution as part of completing the transaction. EX1004, [0055]. That is, as illustrated, “[a] dynamic PAN can also be generated **405** at the device,” where “the dynamic PAN can comprise an *encrypted form of a real PAN*....” EX1004, [0054].² “The DTC and dynamic PAN can be provided **415** by the device for use in the transaction[s]” and “[t]he payment processor system can receive **430** the DTC

² Unless noted all emphasis and coloring has been added.

and dynamic PAN from the device, e.g., from the POS device or merchant system....” EX1004, [0054]-[0055]. “The real PAN of the financial account can then be then determined **432** at the payment processor system” where “determining **432** *the real PAN can comprise decrypting the dynamic PAN using an institution key* of the issuer of the presentation instrument maintained by the payment processor system and corresponding to the IKCV of the device.” EX1004, [0055].



EX1004, FIGs. 3-4.

In Figure 3, above right, **real PAN 316** is stored in memory 310 of presentation instrument 305. EX1004, [0046]-[0047]. “Passing or tapping the presentation instrument near the POS device 330 can trigger the processor 320 of the presentation instrument 305 to read the IKCV 315, the unique card-level key 317 and **real PAN 316** from memory 310.” EX1004, [0047]. “Based on this information, the processor can *encrypt* the **real PAN 316** using the IKCV 315 and one or more factors from the payment device or the POS reader such as unpredictable numbers or counters, e.g., a time of day etc., to generate a **dynamic PAN 326**,” which “can be considered a dynamic, i.e., good for one use, cryptogram that represents but *hides* the **real PAN 316**.” EX1004, [0047].

B. Phillips

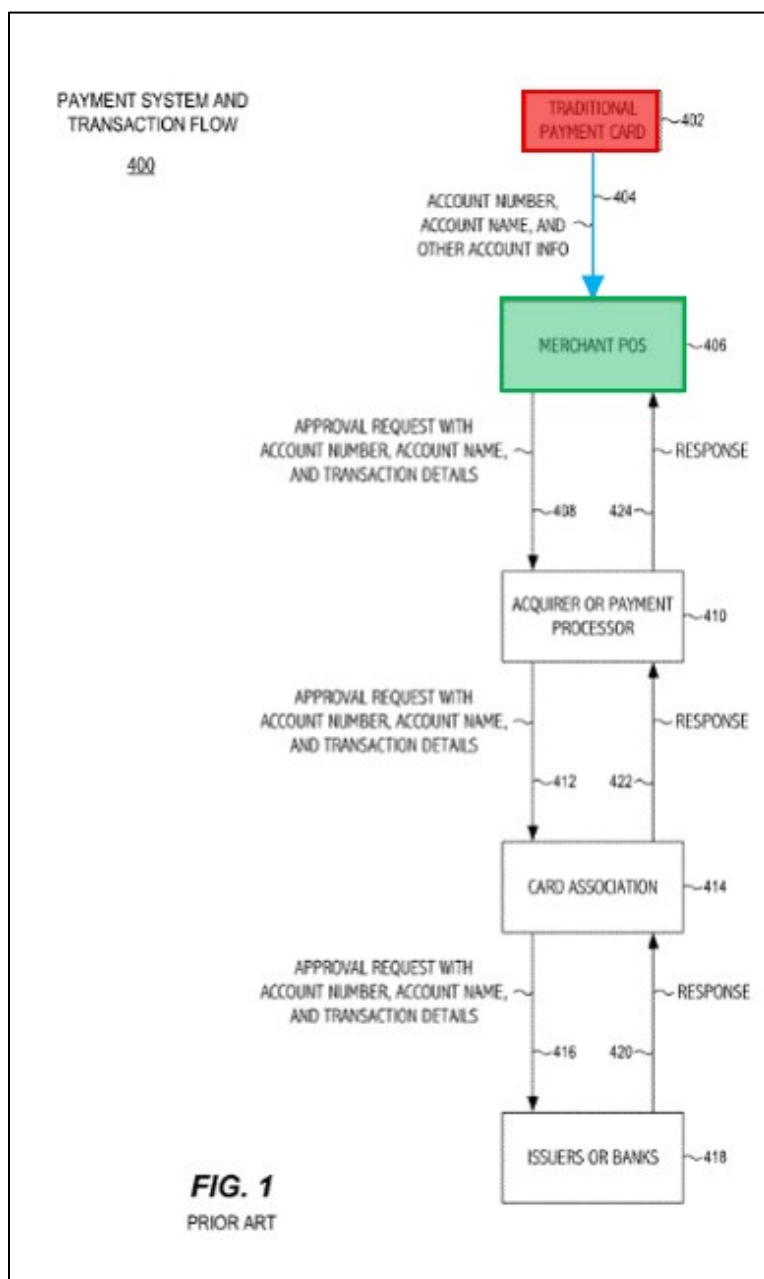
U.S. Patent App. Pub. No. 2012/0310760 (“Phillips”) is directed to “the automatic selection of a payment card account for use in a purchase transaction,” where “a user configures her mobile device so that it will automatically select a particular payment card account when certain predefined criteria are met.” EX1005, Abstract. A “payment circuit” on the device may store one or more card account numbers corresponding to payment card accounts that have been issued to the device owner. EX1005, [0023]. The payment card account numbers and related information are downloaded to the device from an issuer financial institution or service provider. EX1005, [0040].

C. Gomez

U.S. Patent No. 9,600,808 (“Gomez”) is directed to a more secure “payment card system” that can function within a pre-existing traditional payment system. *See, e.g.*, EX1007, Abstract, 1:58-2:44, 5:32-34, 5:67-6:2, FIGs. 1-2. Gomez, in its “Background,” recognizes that “problems of fraud and identity theft that result from the use of payment cards, such as credit and debit cards, are increasing throughout the world.” EX1007, 1:31-33. In its “Summary of Embodiments of the Invention,” Gomez discloses that “[p]ayment card transaction theft and fraud may be greatly reduced, if not virtually eliminated, in a payment card system that utilizes a secure authentication cryptogram which is generated uniquely for each attempted use of the payment card, and which expires within a short period of time thereafter.” EX1007, 1:58-63.

Gomez’s system is thus specifically designed to work within a pre-existing traditional payment system infrastructure, such that “[*n*]o *changes* in the payment system infrastructure need to be made by either the point-of-sale merchant or the card issuer.” EX1007, 2:40-41; *see also, e.g.*, EX1007, 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, 2:43-45. 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 can be seen 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, 4:7-63. 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.

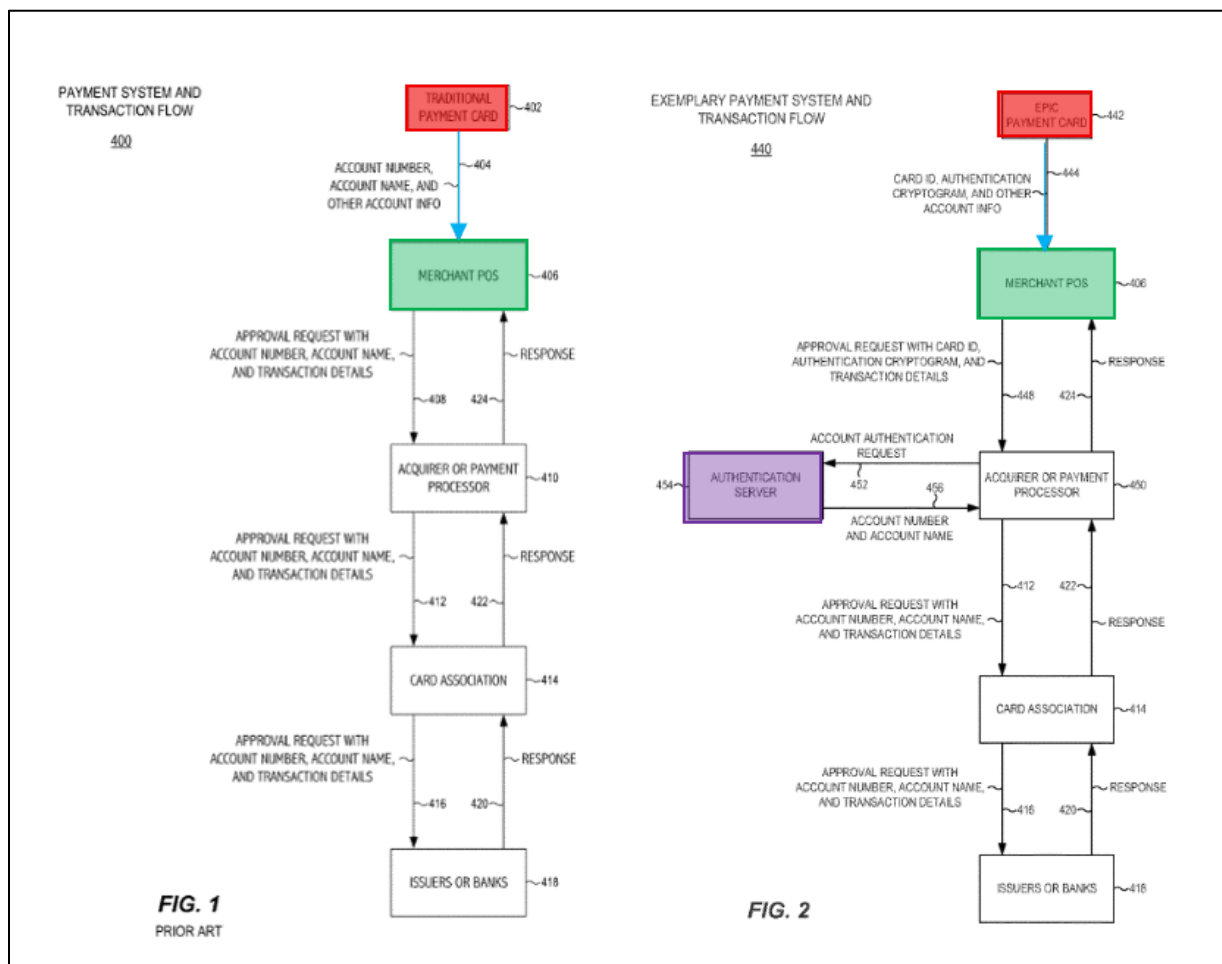
In its system, Gomez specifically makes no modifications to the merchant POS or card issuer systems to implement its “EPIC payment card.” Such EPIC payment card includes a rewritable magnetic stripe on which the static payment card identifying number may be encoded in the account number field and the authorization cryptogram may be encoded in the account name field. EX1007, 5:48-57, Abstract. It may additionally include NFC transmission. EX1007, 7:50-57, 14:3-11. The static number may be a “live” credit card number or may be “an identifying number for an EPIC account which is not itself a live payment card account, but to which are linked one or more live payment card accounts.” EX1007, 5:13-24. 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.

Account information communicated by swiping the card is communicated 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 (the system of Gomez), reproduced below, 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. That is, as noted above, and shown in the comparison of the two figures below, there are “[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.



EX1001, FIGs. 1-2.

Gomez describes two alternative ways to configure and set up an EPIC account: “manual” and “automatic.” EX1007, 20:1-62. “The ‘Automatic’ option means that during a purchase transaction, the EPIC system defaults to the major credit card selection flow established by the customer.” EX1007, 20:15-18. “[I]f the currently selected credit card fails to authorize payment, the EPIC system will

automatically move to the next available credit card for payment authorization of the same purchase transaction.” EX1007, 20:23-27. On the other hand, the “‘Manual’ option provides a customer with the opportunity to manually select the actual credit card that he/she wishes to use during a purchase transaction.” EX1007, 20:30-32. Per Gomez, “[t]his [manual] option is useful, for example, for a customer having a corporate credit card who needs the ability to choose which card to use at the moment of the transaction.” EX1007, 20:33-35. To enable the manual option, the EPIC card is fitted with a display and selection capability, such as a “membrane switch to scroll through available card accounts.” EX1007, 20:37-39. Importantly, Gomez does not say how a merchant, or, for that matter, the EPIC server, would know which underlying credit card is selected in manual mode. After all, the EPIC card itself does not have long-range communication capabilities (just NFC), and cannot communicate over a network. *See, e.g.*, EX1007, 21:5-12 (online payments only work when a vendor has “Epic Pay” on its website). The only possible explanation is that in Manual mode, the EPIC payment card transmits the real active credit card number.

D. Amacker

U.S. Patent No. 8,423,462 (“Amacker”) discloses a “mobile wallet server,” which refers to a user’s mobile device that hosts a “wallet server” (or simply “wallet”) storing personal information such as payment card information, usernames

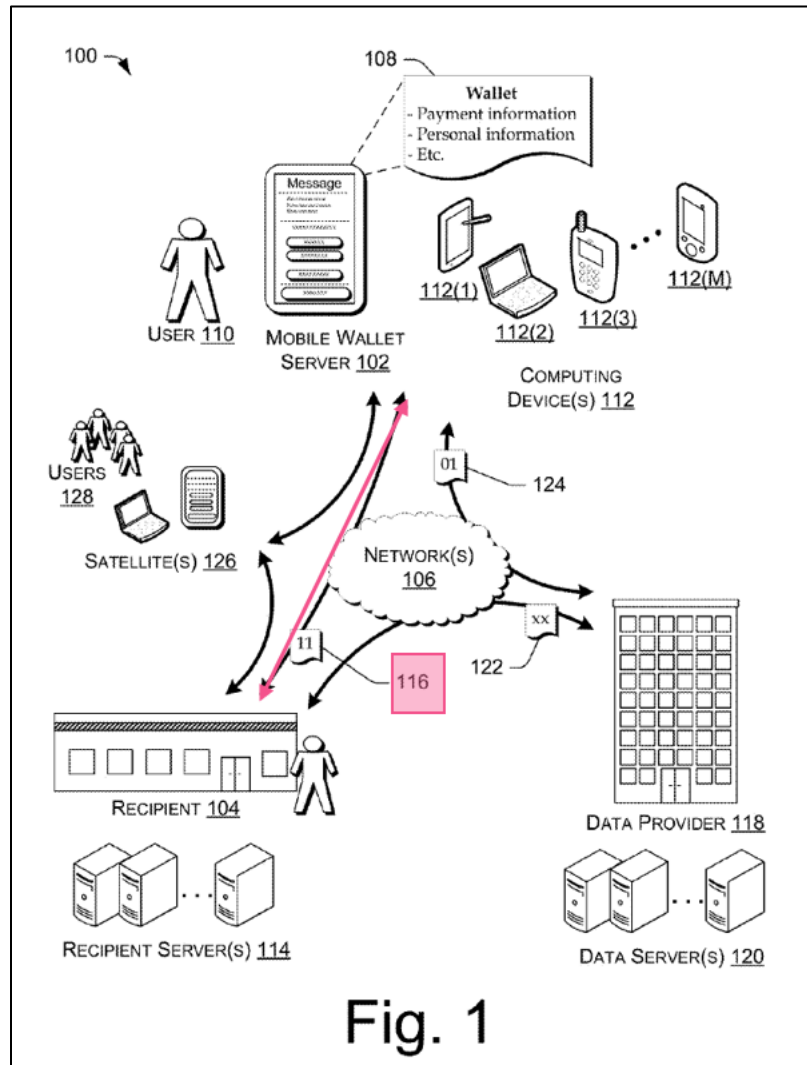
and passwords, contact information, etc. EX1008, 2:13-25, 3:4-13, 3:23-27. The wallet may enable the user to transmit data from the wallet to trusted recipients. EX1008, 3:13-15.

To transmit information to a recipient, the user provides an identifier (e.g., a telephone number or IP address) that enables the recipient to connect to the mobile wallet server. EX1008, 2:37-40, 6:49-53. The recipient then transmits a request for information to the mobile wallet server, which the user may choose to accept or reject. EX1008, 2:40-46, 6:52-61. If approved by the user, the mobile wallet server may transmit the requested information to the recipient. EX1008, 2:46-49.

Amacker teaches that its system enables a user to “complete a complicated transaction ... by transmitting payment and personal information ... while avoiding timely manual entry of the information and while reducing dissemination of the personal information to additional storage locations (e.g., an entity server used to store personal account information).” EX1008, 2:49-57.

As shown in Figure 1, below, Amacker discloses bi-directional communication between the “MWS 102” and the “recipient server(s) 114” which servers “may host a POS (point of sale) transaction system.” EX1008, 3:58-4:6. Amacker explains that “[u]sing the MWS 102, the user 110 may transmit personal information from the wallet 108 to the recipient server(s) 114[,] [f]or example, the recipient server(s) 114 may exchange **data 116** via the network 106,” where “[t]he

data 116 may include a request transmitted *from* the recipient server(s) 114 *to* the MWS 102 via the network 106.” EX1008, 3:62-4:1. Then “[a] response may be returned to the recipient server(s) from the MWS in the form of an approval that includes associated personal information from the wallet 108,” or [i]n the alternative, the user 110 may optionally reject the request from the recipient server(s) 114 and not disperse personal information from the wallet 108.” EX1008, 4:1-6.



EX1008, FIG. 1.

IV. LEVEL OF ORDINARY SKILL IN THE ART

For the purposes of this Preliminary Response only, Patent Owner does not dispute Petitioner’s definition of a person of ordinary skill in the art at the time of the invention of the ’579 Patent (a “POSITA”).

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

A. Grounds 1A-1F: The “Royyuru” -Based Grounds

For Grounds 1A-1F, Petitioner relies on a base combination of Royyuru, Phillips, and U.S. Patent No. 8,255,323 (“Casey”) (with several Grounds relying on additional references). However, as explained below, Royyuru, and the combination as a whole, fails to teach using limited-use payment information “in place of” card issuer payment information as required by all of the challenged claims. In addition, Petitioner fails to show that a POSITA would have made the asserted combination of Royyuru with Phillips.

1. Royyuru Does Not Teach Limited-Use Payment Information for Use “in Place of” Card Issuer Payment Information

Petitioner’s Royyuru-based grounds (Grounds 1A-1F) do not teach or render obvious generating limited-use information for use “in place of” card issuer payment information as recited in elements [1.i], [15.d], and [19.k]. Although each of

independent claims 1, 15, and 19 uses slightly different terminology, for purposes of this POPR, each incorporates substantially the same “in place of” requirement:

- Element [1.i]: “generating, by the processor, a limited-use payment information, and using said limited-use payment information *in place of* said card issuer supplied payment information”
- Element [15.d]: “generating a limited-use number at said electronic device, and using said limited-use number *in place of* at least a portion of selected account issuer payment information”
- Element [19.k]: “responsive to receiving an NFC transaction payment request, generating a limited-use payment information for use *in place of* card issuer payment information”

For this requirement, Petitioner relies on Royyuru alone. *See* Pet., 23-24, 35, 41.³ Petitioner argues that Royyuru “provides at least two examples of the claimed ‘limited-use payment information,’” namely, (1) the “dynamic PAN” and (2) the

³ Although Petitioner also relies on Phillips for element [19.k], Phillips is cited for additional requirements in element [19.k] of generating the limited-use payment information in “response to receiving an NFC transaction payment request.” Pet., 39-40. With respect to using the limited-use payment information “in place of” card issuer supplied payment information, Petitioner relies on Royyuru alone. Pet., 39.

“dynamic transaction cryptogram (DTC).” Pet., 23-24. However, Petitioner fails to show that either the dynamic PAN or the DTC, or the combination of the two, is used “in place of” card issuer payment information as required by the Challenged Claims.

Petitioner’s argument fails at the outset because, in the system of Royyuru, the PAN (*i.e.*, the “primary account number”) is still used in the transaction (just in an “encrypted” form). The PAN (*i.e.*, a credit card number) is issued by the financial institution and constitutes “card issuer supplied payment information” (as in element [1.i]), “account issuer payment information” (as in element [15.d]), and “card issuer payment information” (as in element [19.k]). Petitioner agrees. Pet., 24 (correlating the real PAN to same and asserting the dynamic PAN and DTC are used in place of the real PAN). The Challenged Claims therefore require that generated limited-use payment information be used “in place of” such issuer information (here the real PAN), which does not happen in Royyuru as the real PAN is still transmitted and used throughout the transaction (in encrypted and then decrypted form).

That is, Royyuru does not teach using some other, generated payment information “in place of” the card issuer payment information (*i.e.*, the real PAN) but rather still uses the real PAN throughout the transaction flow. Specifically, Royyuru teaches using a “dynamic PAN” that is “an *encrypted form* of [the] real

PAN of the financial account that varies with each use of the device.” EX1004, [0005].

That the real PAN is used throughout makes sense, as Royyuru is directed to more securely encrypting a real PAN that is transmitted during a payment transaction. Royyuru begins by explaining problems with existing systems that rely on a “common key” or a “card level key” for the encryption of a card account number (the real PAN) which can lead to problems if exposed or compromised:

In an effort to prevent such attacks, encryption is sometimes used to protect the account number on the card or device. Such encryption utilizes an encrypted account number on the card or device or an encryption key that is loaded into the card or device that is derived from an institution level key (i.e., it applies to many cards) and the card number. However, ***using a common key can lead to a compromise of a large number of cards if the institution’s encryption key is exposed.*** A common defense against this risk is to derive ***a card level key*** using the common institution level key and some card level attributes such as the Primary Account Number (PAN), though this technique has exposure risk as well. This key exposure can result from a failure in business processes of the issuer to protect the key or an assault on a single chip, e.g., using electron-microscopy to expose the derived key followed by a DES assault to derive the institution’s key. ***If the institution key is compromised, all transactions for all cards or devices with this institution's key***

are potentially exposed. Therefore, a new key must be created and a possibly large number of cards re-issued.

EX1004, [0004]. According to Royyuru, as a result of these problems, “there is a need in the art for improved methods and systems for securely handling a financial transaction.” EX1004, [0004].

Royyuru then seeks to build a more secure encryption design for transmitting the real PAN used in a payment transaction through what it terms a “dynamic PAN” sent together with a “DTC.” Importantly, however, the real PAN is *always* still transmitted (in encrypted form) and then decrypted once received. The difference between the prior art that Royyuru discloses in its Background (EX1004, [0002]-[0004]) and its improved system is the form of the encryption (being dynamic in nature); the process otherwise is still sending an encrypted PAN after which it is decrypted.

In Royyuru’s system, the real PAN is first encrypted to create a “dynamic PAN” which comprises “an encrypted form of a real PAN of the financial account that varies with each use of the device.” EX1004, [0005]. The dynamic PAN (along with the DTC) “can be provided by the device for use in the transaction” and “can be sent or provided from the POS device to a payment processor system.” EX1004, [0006]. The payment processor system then determines the real PAN by decrypting the dynamic PAN, and the decrypted PAN is then sent to a financial institution to

process the transaction. EX1004, [0006]. Thus, again, Royyuru does not replace the PAN, as required by the Challenged Claims, but simply encrypts the PAN during transmission from the device to the payment processor system.⁴ In each transaction of Royyuru, the real PAN (*i.e.*, card issuer supplied payment information) is sent, albeit in its encrypted form (otherwise, it could not be decrypted later).

This is made evident by Royyuru’s specification, which consistently describes this encryption/decryption process, whereby the real PAN is sent in encrypted form (using an “Institution Key Card Variant” (“IKCV”)), and then it is decrypted using that IKCV after being received to determine the “real PAN.” For example, Royyuru summarizes its process as follows:

The dynamic PAN can comprise *an encrypted form of a real PAN* of the financial account that varies with each use of the device. *Generating the dynamic PAN can be based on the real PAN and an Institution Key Card Variant (IKCV) stored on the device....* The DTC and the dynamic PAN can be provided by the device for use in the transaction. For example, providing the DTC and the

⁴ The analysis is no different for element [15.d], which requires “using said limited-use number in place of *at least a portion of* selected account issuer payment information,” because Petitioner does not identify any portion of issuer information that limited-use information is used “in place of.” Indeed, Petitioner makes no additional argument for element [15.d]. Pet., 38.

dynamic PAN from the device for use in the transaction can comprise providing the DTC and dynamic PAN to a Point-of-Sale (POS) device. In such cases, the DTC and the dynamic PAN can be sent or provided from the POS device to a payment processor system. ***The real PAN of the financial account can be determined at the payment processor system.*** The transaction can be authenticated at the payment processor system or at the financial institution based on the DTC. For example, ***determining the real PAN can comprise decrypting the dynamic PAN using a key maintained by the payment processor system and corresponding to one of the card-level keys of the device (e.g., the, IKCV).*** The real PAN can be sent from the payment processor system to a financial institution to affect processing of the transaction. Authenticating the transaction at the payment processor can comprise validating the DTC using a key maintained at the DTC validation system (e.g., the payment processor system or the financial institution), corresponding to the unique card level key on the payment device. According to another embodiment, ***dynamic PAN decryption to real PAN can be done by the payment processor*** and the DTC authentication can be done by the Financial Institution.

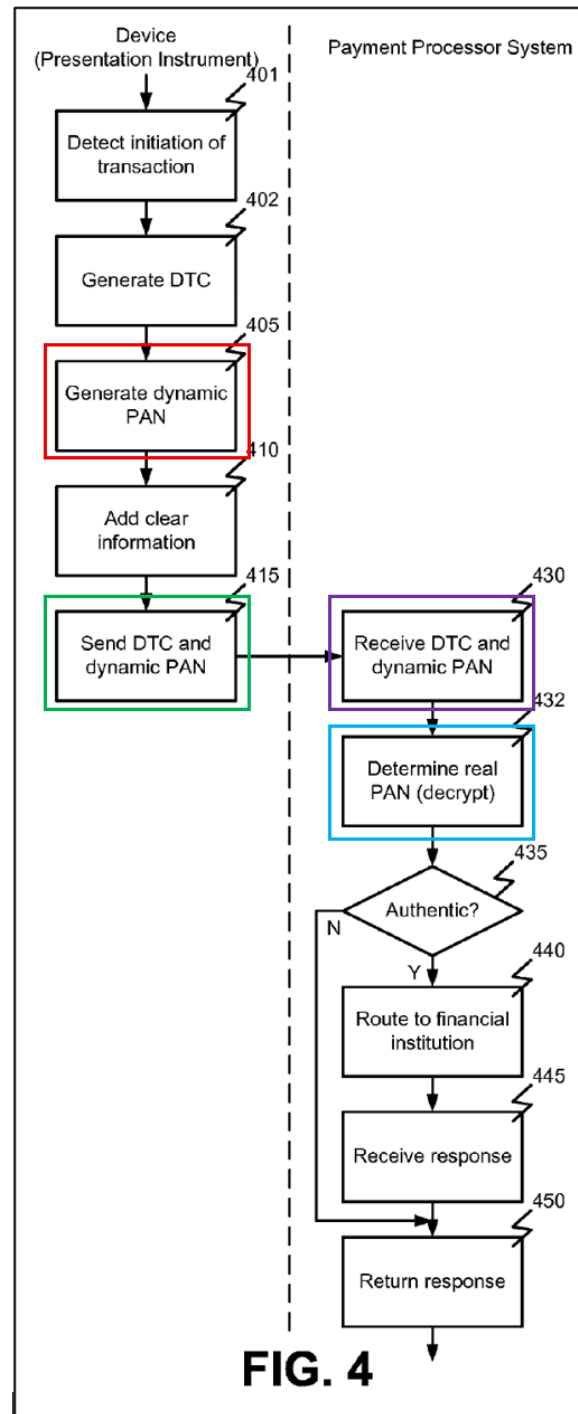
EX1004, [0005]-[0006]; *see also, e.g.,* EX1004, Abstract (“A Dynamic Transaction Cryptogram (DTC) and a dynamic PAN can be generated at the device. The DTC can be used to authenticate the transaction and the dynamic PAN can comprise ***an encrypted form of a real PAN*** of the financial account that is valid for a single transaction”); EX1004, [0010] (“the payment processor system can maintain an

institution key for an issuer of the financial account and can *determine the real PAN by decrypting the dynamic PAN using the institution key.*"); EX1004, cl. 1 ("generating a dynamic PAN at the device, the dynamic PAN comprising an encrypted form of the real PAN"); EX1004, cl. 13 ("The method of claim 11, further comprising determining the real PAN of the financial account at the payment processor system"); EX1004, cl. 14 ("The method of claim 13, wherein determining the real PAN comprises decrypting the dynamic PAN using an institution key of an issuer of the financial account.").

This improved encryption/decryption process whereby the real PAN is still used throughout the transaction is further depicted in Figure 4, reproduced below, which "is a flowchart illustrating processing of a financial transaction utilizing dynamic cryptograms." EX1004, [0014]. As illustrated, "[a] dynamic PAN can also be generated **405** at the device," where "the dynamic PAN can comprise an *encrypted form of a real PAN....*" EX1004, [0054]. "The DTC and dynamic PAN can be provided **415** by the device for use in the transaction[s]" and "[t]he payment processor can receive **430** the DTC and dynamic PAN from the device, e.g., from the POS device or merchant system...." EX1004, [0054]-[0055]. "The real PAN of the financial account can be then determined **432** at the payment processor system" where "determining **432** *the real PAN can comprise decrypting the dynamic PAN using an institution key* of the issuer of the presentation instrument maintained by

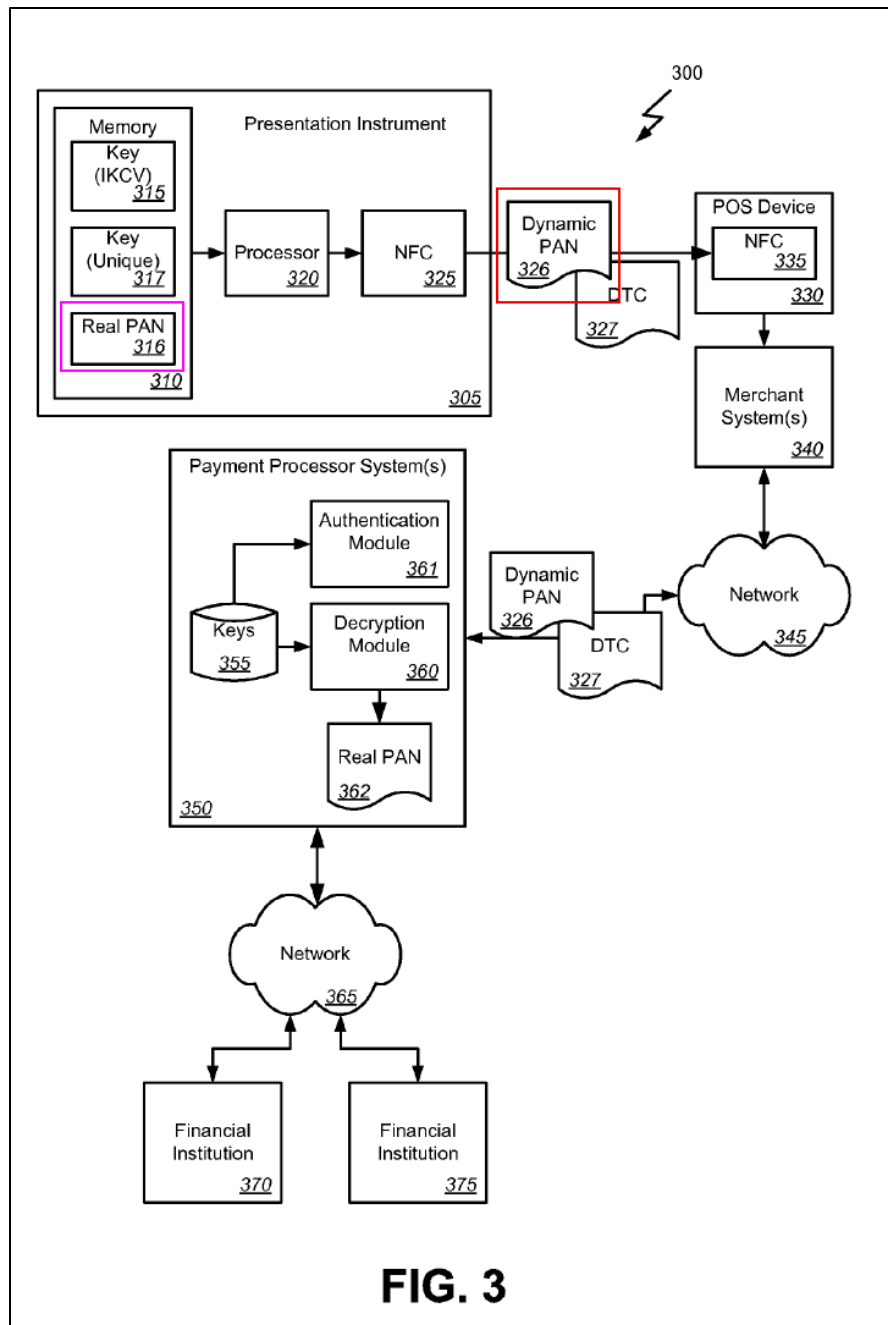
the payment processor system and corresponding to the IKCV of the device.”

EX1004, [0055].



EX1004, FIG. 4.

Similarly, Figure 3, below, which “is a block diagram illustrating, at a high level, a system for processing a financial transaction utilizing dynamic cryptograms according to one embodiment of the present invention,” (EX1004, [0044]), further confirms that the real PAN is used throughout. **Real PAN 316** is stored in memory 310 of presentation instrument 305. EX1004, [0046]-[0047]. “Passing or tapping the presentation instrument near the POS device 330 can trigger the processor 320 of the presentation instrument 305 to read the IKCV 315, the unique card-level key 317 and **real PAN 316** from memory 310.” EX1004, [0047]. “Based on this information, the processor can *encrypt* the **real PAN 316** using the IKCV 315 and one or more factors from the payment device or the POS reader such as unpredictable numbers or counters, e.g., a time of day etc., to *generate* a **dynamic PAN 326**,” which “can be considered a dynamic, i.e., good for one use, cryptogram that represents but *hides* the **real PAN 316**.” EX1004, [0047].



EX1004, FIG. 3.

Petitioner does not address that Royyuru is simply trying to build a more secure encryption process for transmitting a real PAN. Nor does Petitioner address the overall teachings of Royyuru's improved process, including its mirror image

encryption/decryption process of the real PAN that is transmitted (as a “dynamic PAN”) in encrypted form and then decrypted after being received by the payment processor system. Instead, Petitioner’s argument that the dynamic PAN is used “in place of” the PAN is based on a handful statements in Royyuru. Pet., 24 (citing EX1004, [0005], [0057], [0007], [0032], [0006]-[0010]). None support Petitioner’s interpretation when Royyuru is read in context (and most of the statements address only the “dynamic” nature of the dynamic PAN and DTC and have nothing to with the claimed “in place of” requirement). At best, these statements simply describe the encryption process for the real PAN that is sent. But, of course, it would be impossible to then decrypt the encrypted real PAN (that is, the dynamic PAN) to determine the real PAN if the real PAN was not actually sent in the first place.

Petitioner’s Dynamic PAN Assertions. Petitioner begins (at page 24 of the Petition) by quoting a portion of a sentence from Royyuru’s paragraph [0005] to assert that “[s]imilarly, the dynamic PAN is generated by the user device ‘based on the real PAN and an Institution Key Card Variant (IKCV) stored on the device.’” This does not show anything being used “in place of” anything else. Rather, when in read in context—including the immediately preceding sentence of paragraph [0005] that Petitioner omits—it shows that Royyuru is referring to an encrypted form of the real PAN: “The dynamic PAN can comprise ***an encrypted form of a real PAN*** of the financial account that varies with each use of the device. Generating ***the***

dynamic PAN can be based on the real PAN and an Institution Key Card Variant (IKCV) stored on the device.” EX1004, [0005]. Generation of “*the* dynamic PAN” in the second sentence is an example of generating the “encrypted form of a real PAN” from the first sentence, which, as explained above, is sent in encrypted form and then decrypted later. *See also* EX1004, [0005]-[0006], [0054]-[0055], FIG. 4.

Petitioner continues (also at page 24 of the Petition) with “another example,” citing from paragraph [0057] in Royyuru, to assert that “the dynamic PAN is ‘computed by the device for each transaction by combining the digits from the card number with the ATC and with the unpredictable number sent by the RFID or NFC reader and then encrypting these digits with the IKCV.’” Here too, the card number (real PAN) is still used; it is just in encrypted form (using the IKCV) after which it is sent and then later decrypted.

Petitioner then relies on paragraph [0037] to assert the dynamic PAN is valid for a single transaction, but, as the Petition notes, that goes to “limited-use,” (Pet., 24), not the “in place of” requirement.

Lastly, Petitioner highlights a stray statement to assert that “[t]he dynamic PAN or ‘Pseudo-PAN can be sent in place of the real PAN.’” Pet., 24 (citing

EX1004, [0057], [0007], [0032]); *see also id.* (citing [0006]-[0010]).⁵ But although the words Petitioner highlights (found in paragraph [0057] of Royyuru) in isolation suggest a substitution of the real PAN with something else, the rest of Royyuru makes clear that Royyuru simply sends an encrypted version of the real PAN, not information used “*in place of*” the real PAN. Indeed, as discussed above, Royyuru consistently discloses an improved encryption/decryption process of the real PAN, confirming that the real PAN is still used (just in encrypted form). That does not meet the claim requirement “using said limited-use payment information in place of said card issuer supplied payment information” in claim 1 (and similar in independent claims 15 and 19). Moreover, using the PAN (whether encrypted or unencrypted) is antithetical to the teachings of the ’579 Patent, which describes that it “addresses security concerns of a credit card owner,” including the “many ways for a malicious third-party to record the account number of a credit card in order to later make fraudulent transactions on the account.” EX1001, 9:9-15. That concern still exists if a real PAN is sent in encrypted form because if the encryption is hacked, the hacker would then have the real PAN. Claim 1 (and the other independent claims)

⁵ As discussed above, Royyuru at paragraphs [0006]-[0010] disclose the encryption/decryption process for the real PAN, not using anything in place of anything else.

of the '579 Patent prevent all this by generating limited-use information that is used in place of, *e.g.*, the PAN (whether encrypted or decrypted). By arguing that an encrypted PAN meets the “in place of” limitation of claim 1, Petitioner ignores the teachings of the '579 Patent (as well as the full disclosure in Royyuru).

Petitioner’s DTC Assertions. The second alleged limited-use information that Petitioner relies on, the DTC, also does not meet elements [1.i], [15.d], and [19.k]. First, Petitioner does not address how the DTC meets the “in place of” requirement at all. Petitioner merely quotes Royyuru’s teachings of how the DTC is generated and argues that “therefore the DTC is limited in use to the specific user device.” Pet., 24. But even if true, this does not show that the DTC is used *in place of* issuer information. Indeed, as just explained, Royyuru continues to use the real PAN (*i.e.*, issuer information) in connection with the transaction (in encrypted form). At most, the DTC is used together with, but not in place of, the PAN (or encrypted PAN), or any other issuer information.⁶ *See also, e.g.*, EX1004, [0005]-[0006], [0054]-[0055],

⁶ This is even more true for element [1.i], which requires using the limited-use payment information “in place of said card issuer supplied payment information.” The phrase “said card issuer supplied information” refers to “a card issuer supplied account number of a payment card” in element [1.f]. Thus, element [1.i] requires

FIG. 4 (disclosing and depicting that a dynamic PAN, *i.e.*, an encrypted real PAN, is sent together with the DTC).

Thus, because Royyuru does not teach using limited-use payment information “in place of” issuer information as required by elements [1.i], [15.d], and [19.k], which are present by dependency in every claim, Petitioner has failed to show there is a reasonable likelihood that it will prevail as any challenged claim in its Grounds 1A-1F.

2. A POSITA Would Not Have Combined Royyuru with Phillips

Petitioner relies on the combination of Royyuru with Phillips, and asserts that a POSITA would have re-imagined Royyuru as re-imagined multi-account and multi-issuer device. But Royyuru and Phillips are completely incompatible references, and a POSITA would never have simply added their features to each other.

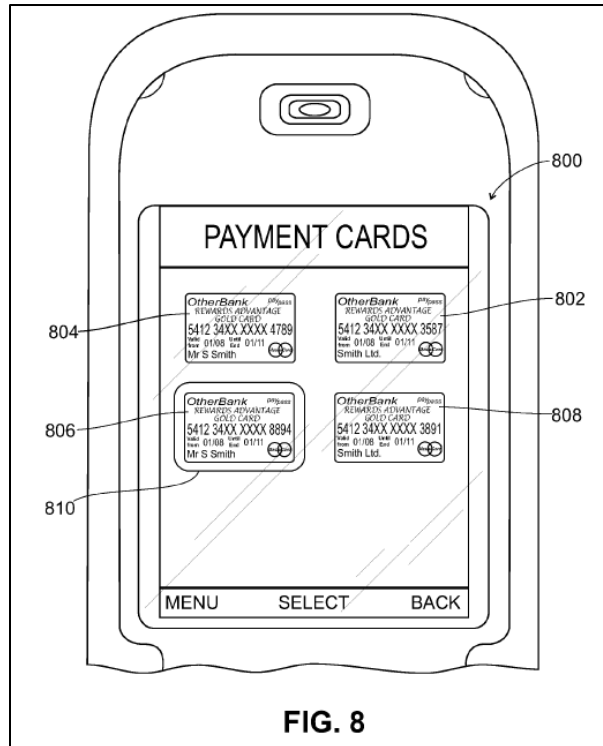
Royyuru is configured for a *single* account per card/device. Importantly, that is an express purpose of Royyuru—to build an improved system for more securely encrypting a single account per card/device. EX1004, [0003]-[0004]. In Royyuru, the IKCV and other information (such as a unique card key, CK) is “generated *when*

limited use information be used specifically “in place of” an account number (*e.g.*, PAN), which is exactly what Royyuru does *not* do.

each card (device) is being customized.” EX1004, [0057]. In fact, the DTC is generated using the unique card key or keys that are particular to each card. EX1004, [0047] (stating in reference to Figure 3, “[t]he processor 320 can also generate a dynamic transaction cryptogram (DTC) 327 based on the unique card-level key 317....”), [0032] (“routing of the transactions using this new prefix results in the transaction being delivered to a payment processor with the keys and capability to decrypt the dynamic PAN to the real PAN”), [0039] (“The repository of enabling data 145 can include a wide variety of information related to financial transactions related to the consumer and/or specified by different entities such as merchants, financial institutions, third-party advertisers, etc. For example, the enabling data 145 can include a set of keys, i.e., private keys held by the payment processor and/or financial institution and relating to the card-level keys of the individual cards, and that can be used to decrypt the dynamic PAN to determine the real PAN”).

In contrast, Phillips contemplates a *multi-account and multi-issuer* configuration where a user can save and then select from many different cards and many different issuers in order to make a payment. EX1005, FIG. 8 (reproduced below). Indeed, Petitioner relies on this multi-card configuration to assert that it “would have provided more choices and options with respect to how the user spent their money, would have allowed the user to select payment options that are the most appropriate for a given scenario, and reduced or eliminated the need for the user to

carry additional physical payment options.” Pet., 16 (citing EX1003, ¶135, which repeats, without citation or support, the Petition’s assertions). In Phillips, the card accounts are clearly provided from multiple different sources and then loaded on to a single mobile device. *See* EX1005, FIG. 8 (reproduced below), [0004]-[0005], [0036]-[0037]. The cards come from financial institutions while the mobile device comes from a company like Apple or Google. *See* EX1005, [0004]-[0005], [0036], [0040].



EX1005, FIG. 8.

Petitioner does not explain how the re-imagined multi-account and multi-issuer device works using Royyuru’s IKCV and dynamic PAN / DTC approach on a mobile device from the likes of Apple, Google, etc. *See* Pet., 16-18. For example,

which entity generates the unique card key that is used in generation of the dynamic transaction cryptogram? The mobile device company or the financial institution / payment processor? How would the contemplated device associate and store the relevant keys? How is the DTC validated? These questions are fundamental to the proposed combination, yet nowhere does Petitioner explain how the combination would actually work.

For example, in Royyuru, the payment processor 350 can maintain a key repository 355. EX1004, FIG. 3 (above). As Royyuru explains, “[g]enerally speaking the key of the key repository 355 corresponding to the card-level key 317 of the presentation instrument 305 allows authentication module 361 to authenticate the presentation instrument 305 and/or the consumer using the presentation instrument 305 based on the received DTC 327.” EX1004, [0048]. Moreover, as discussed above in Sections III.A and V.A.1, the dynamic PAN can be “based on the real PAN and an Institution Key Card Variant (IKCV).” EX1004, [0005], [0054]-[0055]. This all works well when the IKCV is—as per Royyuru—“generated when *each card (device) is being customized*” (EX1004, [0057]) and stored on the device. But Petitioner does not explain how its Royyuru-Phillips combination would work when re-imagining Royyuru as a multi-card and multi-issuer device (where the device is controlled *separately* from the IKCV and card-key).

Moreover, besides the combination being unworkable and unexplained, Petitioner’s assertion that a POSITA would have combined Royyuru and Phillips because it “would have provided more choice and options with respect to how the user spent their money, would have allowed the user to select payment options that are the most appropriate for a given scenario, and reduced or eliminated the need for the user to carry additional physical payment options” rests on the conclusory assertion of its expert (at paragraph 135 of Exhibit 1003), who simply repeats, without citation or support, Petitioner’s assertion. Such conclusory testimony should be afforded little to no weight—especially given the evidence against discussed below. *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).

Petitioner’s expert also asserts, again without citation or support, that “[a] POSITA would have recognized that such benefits would have outweighed any

minor increases in memory usage to store the additional cards and information.” EX1003, ¶135. Neither Petitioner⁷ nor its expert attempt to weigh these alleged “benefits” against the alleged “minor increases” created by the proposed combination; Petitioner’s expert just asserts that the scale would have tipped toward combining the references. That is not evidence, that is just unsupported argument, and without any evidence, Petitioner’s Grounds fail.⁸ See, e.g., *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (“To satisfy its burden of proving obviousness, ***a petitioner cannot employ mere conclusory statements***. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.”); *Solus Advanced Mat’ls Co. Ltd. v. SK Nexilis Co., Ltd.*, IPR2024-01462, Paper 14 at 17-18 (PTAB Apr. 25, 2025) (“Petitioner’s contention that implementing Dobashi’s RSm values into Hanafusa’s electrolytic copper foil is the application of known techniques to a known structure to yield predictably results is similarly conclusory and lacking in persuasive explanation. ***Such conclusory statements regarding the POSITA’s alleged reasonable expectation of success are not sufficient*** to support a finding of

⁷ Petitioner omits this portion of the expert’s declaration from the Petition.

⁸ Petitioner relies on the selection process of Phillips to assert the proposed combinations meet elements [1.f], [15.c], and [19.j].

obviousness. Such assertions, lacking factual substantiation, are insufficient for evaluating reasonable expectation of success as part of an obviousness determination.”) (internal citation omitted).

Moreover, these “minor” inconveniences that Petitioner’s expert glosses over are anything but minor. For example, in a co-pending IPR petition (IPR2025-01361, EX2025) challenging a related patent, Petitioner relies upon “*Law*” (U.S. Patent App. Pub. No. 2015/0134540, EX2024)⁹—which Petitioner and the same expert here likewise assert are in the same field, including using mobile devices with NFC for facilitating payment transactions. *See also, e.g.*, EX2024, [0002]-[0003]. *Law* recognized the importance—in designing a mobile payment transaction application—of reducing the storage utilized by the mobile device (on the secure element of an embedded chip such as a UICC or SIM card), as well as the required amount of data used, processing power, and computing time. EX2024, [0063] (“In many cases, the software payment card is stored on the secure element to protect the sensitive payment data.... It is recognized that secure elements are ***limited in their storage capabilities***. They are typically available in the form of an embedded chip. Such as in a universal integrated circuit card (UICC), or in a subscriber identity

⁹ In the co-pending IPR petition (EX2025), Petitioner seeks to combine “*Law*” with Gomez, Amacker, and Casey (all of which Petitioner uses in this IPR petition).

module (SIM) card.”); [0071] (“[T]he secure element [of the mobile device] typically has *very limited storage space*” and thus “having multiple card applications on the secure element [in] some cases is *not possible* due to insufficient storage space.”), [0072] (“Therefore, it is *desirable to reduce the amount of storage space* that card applications require on the secure element so as to not limit the number of software payment cards a user can load into a secure element. Along the same lines, it is desirable for mobile phone carriers to *reduce the amount of data used* by ‘card application’ on the secure element so that other types of applications can be loaded thereon.”), [0243] (same), [0140] (“This saves on processing power and reduces the computation time when making a transaction.”). Law further recognized that it can be “appreciated that associating multiple funding cards (and each of their card applications) with a mobile device for NFC payments *can be limiting*.” EX2024, [0071].

Notably, Phillips also uses a “secure element” on a SIM to store the payment application, card numbers, and other sensitive data. EX1005, [0024]. The “secure element” in Phillips is the same as the secure element in Law, and faces the same constraints as Law regarding increased use in storage space (as well as relatedly, data use, processing power, and computing time). Petitioner fails to account for any of these issues in its proposed combination (let alone explain where or how the

various information would be stored or address the other issues with the proposed combination, as discussed above).

In other words, evidence that Petitioner put forth to challenge another of Patent Owner's related patents using overlapping prior art demonstrates that Petitioner's unsupported assertions here are not so simple, and on this record, demonstrate that a POSITA would *not* have sought to "modif[y] Royyuru such that the device stores information for multiple payment options and provides a graphic interface, including payment method indicia, to allow user selection of a payment method as shown in FIG. 8 of Phillips." Pet., 16; *see also* Pet., 20-21 (relying on Phillips and FIG. 8 for element [1.f]), 35, 37.

For these additional reasons, Petitioner has failed to show there is a reasonable likelihood that it will prevail as to at least one claim based on Grounds 1A-1F.

B. Grounds 2A-2E: The "Gomez"-Based Grounds

For Grounds 2A-2E, Petitioner relies on a base combination of Gomez, Amacker, and others. However, as explained below, Gomez, and the combination as a whole, fails to teach or render obvious (i) using limited-use payment information "in place of" card issuer payment information, and (ii) receiving a transaction request via an NFC interface (including, among other reasons, because Gomez teaches away from the proposed combination), as required by all of the Challenged Claims.

1. Gomez Does Not Teach Limited-Use Payment Information for Use “in Place of” Card Issuer Payment Information

For Petitioner’s Gomez-based grounds (Grounds 2A-E), the mixed-and-matched embodiments in Gomez that Petitioner rely upon (and Petitioner’s proposed combinations as a whole) fail to teach or render obvious generating limited-use information for use “in place of” issuer payment information, as recited in elements [1.i], [15.d], and [19.k] of independent claims 1, 15, and 19:

- Element [1.i]: “generating, by the processor, a limited-use payment information, and using said limited-use payment information *in place of* said card issuer supplied payment information”
- Element [15.d]: “generating a limited-use number at said electronic device, and using said limited-use number *in place of* at least a portion of selected account issuer payment information”
- Element [19.k]: “responsive to receiving an NFC transaction payment request, generating a limited-use payment information for use *in place of* card issuer payment information”

For this requirement, Petitioner relies on Gomez alone. *See* Pet., 68-69, 80, 83.¹⁰ Petitioner asserts that the “authentication cryptogram” of Gomez “is used in

¹⁰ Similar to the Royyuru-based grounds, although Petitioner also relies on Amacker for element [19.k] in the Gomez-based grounds, Petitioner does not argue that

place of the card issuer supplied payment information (the ‘actual credit card account number’ disclosed by Gomez) in that the authentication cryptogram is combined with the static EPIC account number to form limited-use payment information and provided to the merchant rather than the issuer supplied payment information.” Pet., 68-69. Petitioner’s Gomez-based challenge mixes and matches the “manual” and “automatic” embodiments” in Gomez, which leads to multiple failures.

a. Petitioner’s Theory Relies on Gomez’s “Manual” Embodiment, But This Embodiment Requires Use of the Actual (Real) Payment Card Information, as Petitioner Effectively Admits in Another IPR Petition

Petitioner’s theory is premised on Gomez’s “manual” selection embodiment whereby the actual credit card number must be used throughout the transaction (including initially transmitting it from the EPIC payment card to the merchant POS at the beginning of the payment transaction). For example, for element [1.f] (“displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account

Amacker teaches limited-use payment information for use “in place of” card issuer payment information. Pet., 88-89. Moreover, as explained in the next section, a POSITA would not have applied Amacker’s teachings to Gomez with respect to receiving a transaction request.

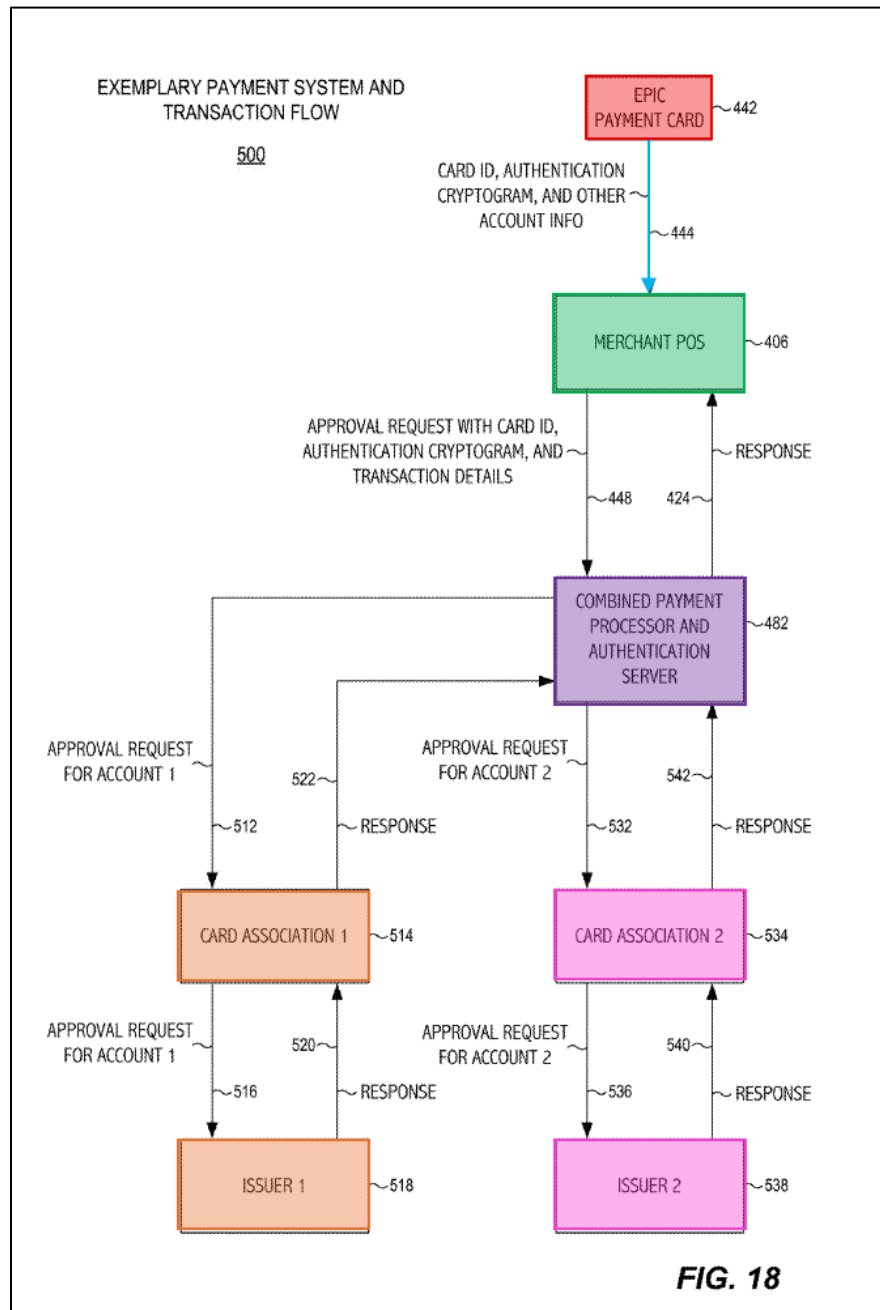
number of a payment card”), Petitioner relies on the “manual” embodiment of Gomez to assert that the “Gomez-Amacker-Spodak device” meets the claim element: “The Gomez-Amacker-Spodak device includes ‘a display and a selection capability’ to allow the user ‘to manually select the actual credit card that he/she wishes to use during a purchase transaction.’” Pet., 66 (citing Gomez (EX1007), 20:30-59, 21:5-20, FIG. 9). According to Petitioner, “[i]n the combination, Amacker confirms that ‘when the MWS 102 receives a payment request, the wallet presenter 214 may present relevant payment options that may be used to respond to the payment request (e.g., payment card selections, etc.).’” Pet., 65 (citing EX1008, 5:18-41, cl. 1; EX1003, ¶¶330-331); *see also* Pet., 80 (for [15.c] (“receiving, from a valid device user, a payment selection...”)) referring back to [1.f]); (similarly for [19.j] referring back to [1.f]); *see also* Pet., 61-62 (asserting motivation based on “manual” selection). In other words, Petitioner’s obviousness assertion for its Gomez-based grounds is premised on the initial use of the “manual” selection embodiment to select a particular issued payment account during a particular transaction. This “manual” embodiment of Gomez is fundamentally different from the “automatic” embodiment in terms of how the underlying account information is selected, communicated, and used for payment.

Automatic Mode. In the “Automatic” embodiment, a user pre-selects their account priority through the EPIC system (e.g., “online to link one or more actual

payment card accounts with the EPIC card account, including the preferred order that the authentication server should select such linked accounts to use for a given transaction”). EX1007, 20:1-6; *see also* EX1007, 20:7-29. That way, “during a purchase transaction, the EPIC system defaults to the major credit card selection flow established by the customer.” EX1007, 20:16-18. More specifically, and with reference to Figure 18 below, in such “automatic” process, **account information 444** (including the EPIC card account number) is communicated from **EPIC payment card 442** to **merchant POS 406**, which then transmits the approval request 448 to **acquirer 482**. EX1007, 18:43-49; *see also* EX1007, 5:65-6:6. **Acquirer 482** “analyzes the account number conveyed in the inbound approval request 448 to determine the appropriate card association or entity to next process the transaction approval request” by recognizing the EPIC card account number and “determin[ing] a first payment card account number (and corresponding actual account name) which is linked to the account.” EX1007, 18:50-59.

The request is then sent to **first card association 514** and then to **first issuer 518** for approval or denial. EX1007, 18:60-19:2. If approved, the transaction is processed using the first card; if denied, then an approval request automatically goes to the next priority card already linked to the account (**second card association 534** and **second issuer 538**), and so forth, until a card is approved or all cards are denied. EX1007, 19:4-34, 20:15-37. This process only works because the user pre-selected

the “Automatic” option mean[ing] that during a purchase transaction, the EPIC system defaults to the major credit card selection flow established by the customer” in advance (*e.g.*, “online” before the user is at a retailer). EX1007, 20:1-37.



EX1007, FIG. 18.

Manual Mode. Importantly, the Manual embodiment is different. In Manual mode, a user has the ability to select a payment account on-the-fly, right from the EPIC payment card itself “at the moment of the transaction.” EX1007, 20:30-42. Specifically, the user can select the payment account from a display and a selection capability, such as a membrane switch. EX1007, 20:30-42. “This option is useful, for example, for a customer having a corporate credit card who needs the ability to choose which card to use at the moment of the transaction.” EX1007, 20:33-35. However, with this “manual” embodiment, Gomez is silent on how the merchant POS, the Authorization Server, or the EPIC system knows which payment account to use in the transaction.

As Petitioner admits regarding Gomez’s disclosure in its co-pending Petition for *Inter Partes* Review challenging a patent related to the ’579 Patent:

Gomez also describes how a user may manually choose which of the actual credit/debit cards to use at the moment of a transaction. However, Gomez ***does not explicitly disclose how the selected actual credit/debit card payment information is communicated to the merchant*** and EPIC authentication server during a transaction.
EX2025, 53-54 (citations omitted).

However, if the EPIC card account number (not the actual “live” credit card number) was transmitted by the payment card in connection with this “manual” selection process, there is no way the EPIC system would know which card the user

selected “at the moment of the transaction.” Petitioner effectively admits this. *See* EX2025, 53-54. Thus the only possible explanation is that in Gomez the real account information is transmitted from the EPIC payment card to the merchant POS system during Manual mode operation. This is buttressed by Gomez’s disclosure elsewhere, for example, that “[t]he payment card number [used in the transaction] may represent a ‘live’ card number or other payment card account number....” EX1007, 5:19-20; *see also, e.g.*, EX1007, 2:19-21 (“The static payment card identifying number may represent a live (i.e., ‘actual’) credit card number or other payment card (e.g., debit card) account number”).

As such, because the display and selection for element [1.f] relied upon by Petitioner occur only in Gomez’s “Manual” mode, Gomez does not disclose element [1.i] under Petitioner’s theory because this element requires “generating, by the processor, a limited-use payment information, and using said limited-use payment information *in place of* said card issuer supplied payment information” (and similar elements [15.c]/[15.d] and [19.j]/[19.k]). Alternatively and at the very least, given Gomez’s lack of “explicit disclosure” according to Petitioner (EX2025, 53-54), Petitioner cannot meet its burden on elements [1.i], [15.d], and [19.k] as it concerns the Manual mode embodiment. *See also* Section V.B.1.b, below.

Petitioner seems to recognize this because it does not rely on the Manual mode disclosure in connection with elements [1.i], [15.d], and [19.k]. Instead, Petitioner

flips to the “Automatic” mode disclosure, pointing to the portions of Gomez that are only operable when a user pre-selects a priority for the linked underlying credit cards. Pet., 68-69, 80, 83. Petitioner’s mixing and matching of embodiments is fatal to its Gomez-based challenge. *See, e.g., Samsung Elecs. Co. Ltd. v. Mojo Mobility Inc.*, IPR2023-01100, Paper 11, 18-19 (PTAB Feb. 12, 2024) (denying institution where combination “appears unworkable and mixes incompatible features of the two different coil arrangements without sufficient explanation to justify their combination”); *PayPal, Inc. v. IOENGINE, LLC*, IPR2019-00930, Paper 16, 34 (PTAB Oct. 29, 2019) (denying institution where Petitioner “improperly mixes and matches two discrete embodiments”); *AT&T Servs.*, IPR2024-01143, Paper 15 at 33 (denying institution and finding Petitioner’s “conflicting arguments inconsistent and thus not persuasive”).

Petitioner does not give a reason why (or explain how) a POSITA would combine these different options (nor even address that these are separate embodiments with a separate transaction flow). Importantly, however, the specification treats them as alternatives. A user either implements Manual mode or Automatic mode at any given time. EX1007, 20:1-63. If a user is in Automatic mode, there is no reason to display or select anything on or from a touch-screen display, as required by element [1.f] (and similar requirements in elements [15.c] and [19.j]). Nor does Gomez disclose doing so in the Automatic Mode (such display and

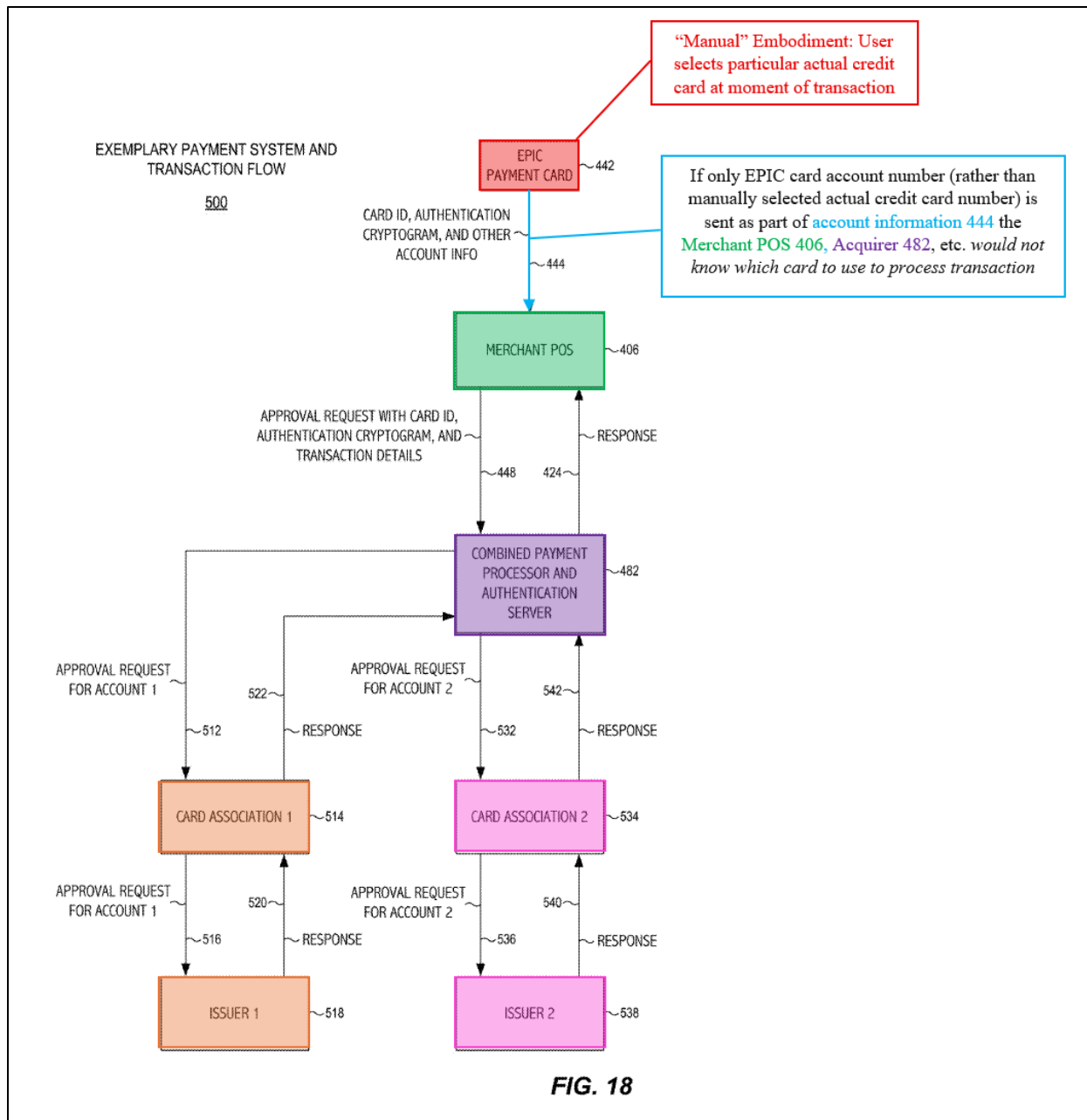
selection happens in Gomez only in the Manual mode, (EX1007, 20:30-35)). If a user is in Manual mode, there is no “explicit disclosure” in Gomez, as Petitioner acknowledges (EX2025, 53-54) about what gets communicated to the merchant during the transaction. All signs are that it is the *real* credit card number that must be transmitted from the EPIC payment card to the merchant POS in Gomez’s Manual mode, which fails to meet element [1.i], [15.d], and [19.k].

b. If Gomez Does Not Teach How the Selected Credit Card Number is Used Throughout the “Manual” Process, Petitioner’s Proposed Combination is Inoperative, Unworkable, and Unexplained

If Petitioner is correct that Gomez is not “explicit” in how the “manual” selection process “at the moment of the transaction” occurs (EX2025, 53-54), Petitioner’s theory would still necessarily fail. In this scenario, Petitioner provides no argument or evidence as to how its proposed combinations would involve both (i) selecting the particular credit card to use at the time of the transaction (as alleged for elements [1.f], [15.c], and [19.j]) and (ii) transmitting the EPIC card account number and authentication cryptogram “in place of” the actual credit card number (as alleged for elements [1.i], [15.d], and [19.k]).

In such a scenario, Petitioner’s proposed combination would not function because the EPIC system would have no way of knowing which credit card was selected for use. Indeed, Petitioner’s Gomez-based challenge includes *no argument or evidence* as to how the process would actually work. For example, if the user

selected—“at the moment of the transaction”—the “actual credit card that he/she wishes to use during a purchase transaction” (*see* Pet., 66; EX1007, 20:30-35), but then “the authentication cryptogram is combined with the static EPIC account number to form limited-use payment information and provided to the merchant rather than issuer supplied payment information” (“the ‘actual credit card account number’ disclosed by Gomez”) (Pet., 68-69), the actual credit card account number selected would never be transmitted and thus *not* known to any other part of the system. This can be seen in reference to Figure 18 of Gomez, below. If a user selects a particular “actual credit card” using **EPIC payment card 442** “during a transaction at the moment of the transaction” (as Petitioner’s [1.f]/[15.c]/[19.j] theory is premised on) but the **EPIC payment card 442** transmits only the EPIC card number (along with the authentication cryptogram) as part of **account information 444** to **merchant POS 406** then the actual credit card selected would never be known and the transaction could *not* proceed. The same is true in the other embodiments and figures in Gomez (all of which necessitate that the card number would be transmitted to the merchant POS, as in, *e.g.*, Figures 2, 3, 16, and 17).



EX1007, FIG. 18 (red “Manual...” and blue “If only...” text boxes added for reference).

Thus, to the extent that it is determined that Gomez does not teach how the selected actual credit card is transmitted in the “manual” embodiment (as Petitioner alleges in its co-pending IPR Petition (EX2025, 53-54)), Petitioner’s proposed

combinations for its Gomez-based challenge—starting with the “manual” selection embodiment for elements [1.f], [15.c], and [19.j] and then switching to the “automatic” embodiment for elements [1.i], [15.d], and [19.k]—would be inoperative, unworkable, and unexplained. Petitioner has thus failed to meet its burden to show how the proposed combination would meet all claim limitations under this scenario as well. *See, e.g., AT&T Servs.*, IPR2024-01143, Paper 15 at 33; *Samsung Elecs.*, IPR2023-01100, Paper 11 at 18-19; *PayPal*, IPR2019-00930, Paper 16 at 34.

2. A POSITA Would Not Have Sought to Modify Gomez with Amacker to Receive an NFC Transaction Payment Request; Gomez Teaches Away from and Expressly Discourages the Proposed Combination

Petitioner’s Gomez-based grounds do not teach or render obvious a device receiving a request for transaction payment via an NFC interface, as recited in elements [1.e], [15.a], and [19.k]:

- Element [1.e]: “*receiving a request for a transaction payment at said electronic device via the NFC interface*”
- Element [15.a]: “*receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient proximity communication request to an NFC interface of the electronic device*”

- Element [19.k]: “responsive to *receiving an NFC transaction payment request, ...*”

For this requirement, Petitioner relies on the teachings of Amacker (Pet., 65-66, 80, 83) and argues that “a POSITA would have modified Gomez based on Amacker to receive a payment request for a transaction and display payment options for conducting the transaction at the device” (Pet., 60-64).

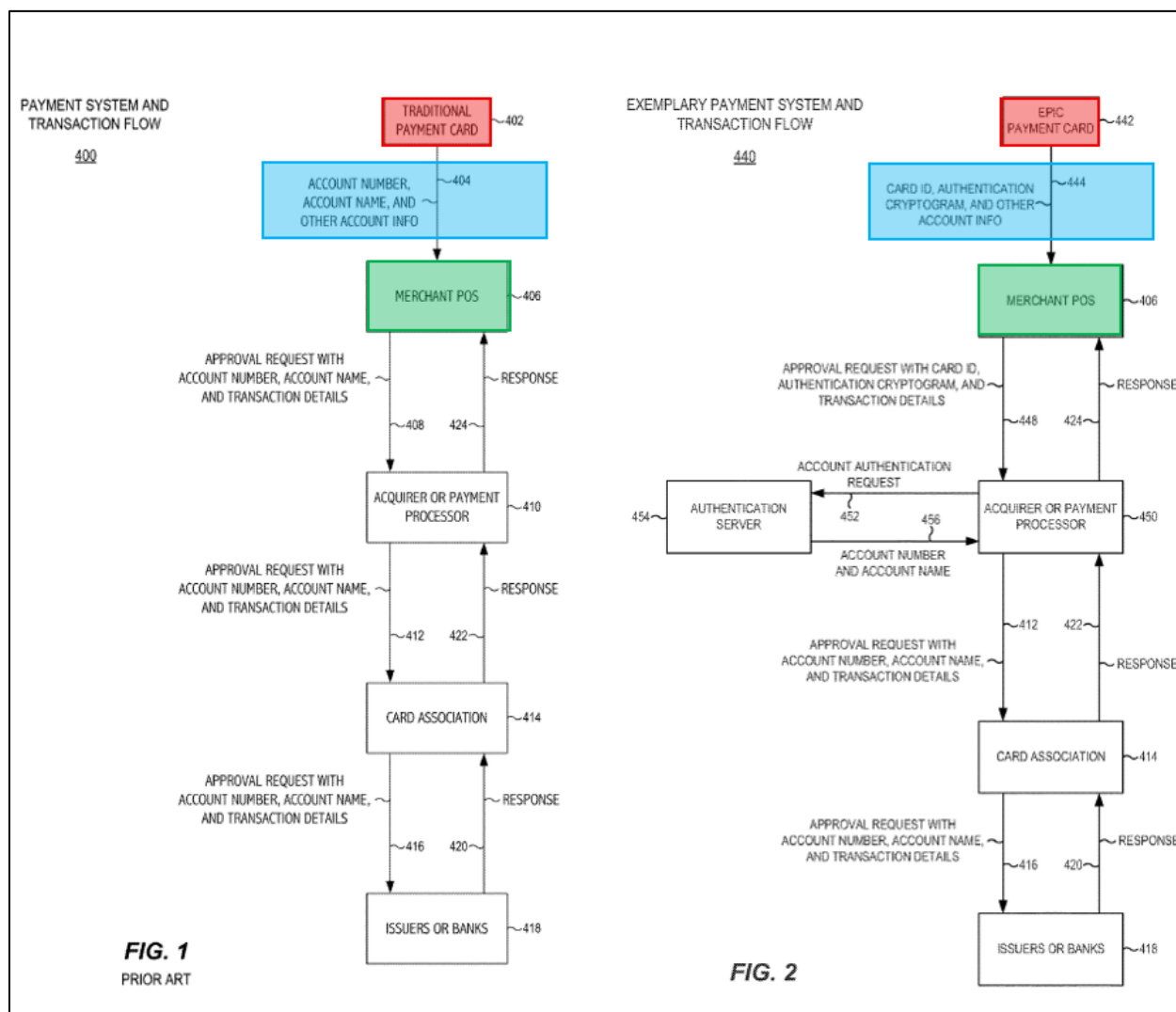
However, Petitioner’s argument ignores Gomez’s express teachings to ***not*** make the contemplated changes (and, in fact, not make ***any*** changes to the system at the “traditional” point-of-sale or card issuer). It also fails to appreciate the fundamental differences between Gomez and Amacker. These missteps lead to several fundamental problems with Petitioner’s proposed combinations.

First, as discussed above in Section III.C, the entire point of Gomez is that its “EPIC” payment card may be presented like a traditional credit card using a magnetic stripe and used in a “traditional” payment system without needing any changes in infrastructure by the point-of-sale merchant or the card issuer. Indeed, 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 to be made by either the point-of-sale merchant or the card issuer.” EX1007, 2:40-41; *see also, e.g.*, 3:65-4:7 (“FIG. 1 is a block diagram of a ***traditional*** payment system 400 and transaction flow related to purchase transaction

approval at a retail merchant. A *traditional* payment card 402, such as a credit card or debit card, includes *a magnetic stripe* on which is permanently encoded certain account information.... This account information (labeled 404) is communicated to merchant 406, such as by swiping the payment card 402 through a magnetic card reader on a point-of-sale (POS) terminal (not shown).”; 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.”), 5:67-6:2 (“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.”), 10:8-17 (“using *traditional* POS terminal equipment”), 14:3-11 (“*traditional* payment card system” including NFC transmission).

This is further evident in the comparison of Figures 1 and 2 of Gomez. Figure 1, below left, “is a block diagram depicting a traditional payment system 400 and transaction flow related to purchase transaction approval at a retail merchant,” whereby “[a] **traditional payment card 402**, such as a credit or debit card, includes a magnetic stripe on which is permanently encoded certain account information,” which “**account information (labeled 404)** is communicated to **merchant 406**, such as by swiping the **payment card 402** through a magnetic card reader on a point-of-sale (POS) terminal (not shown).” EX1007, 3:65-4:7. Figure 2, below right, then retains all of these traditional features, including that “**EPIC payment card 442**

includes a re-writable magnetic stripe” with “**account information 444**.” EX1007, 5:48-64. As in the traditional system (depicted in Figure 1), in Figure 2, “**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).” EX1007, 5:64-67. As Gomez explains in reference to Figure 2 implementing its EPIC payment card, “[s]ince 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.” EX1007, 5:67-6:2. “The **merchant 406** combines the **account information 444** with transaction information, *as before*, [*i.e.*, as in the “traditional” system in Figure 1] and forms an approval request 448 which is communicated to an acquirer 450.” EX1007, 6:3-6. Notably, **merchant POS 406** requiring the magnetic card swipe of a payment card is designed to be the *same* in both the “traditional” “prior art” system in Figure 1 and the EPIC payment card system in Figure 2.



EX1007, FIGs. 1-2

Yet, in Petitioner’s reimagined combination adding Amacker to Gomez would lose the traditional aspects of its EPIC payment card—including the magnetic stripe capability necessary to remain compatible with “traditional” merchant POS systems disclosed in Gomez—by modifying Gomez’s EPIC payment card “to include a larger touchscreen display and/or is integrated into a device having a touchscreen

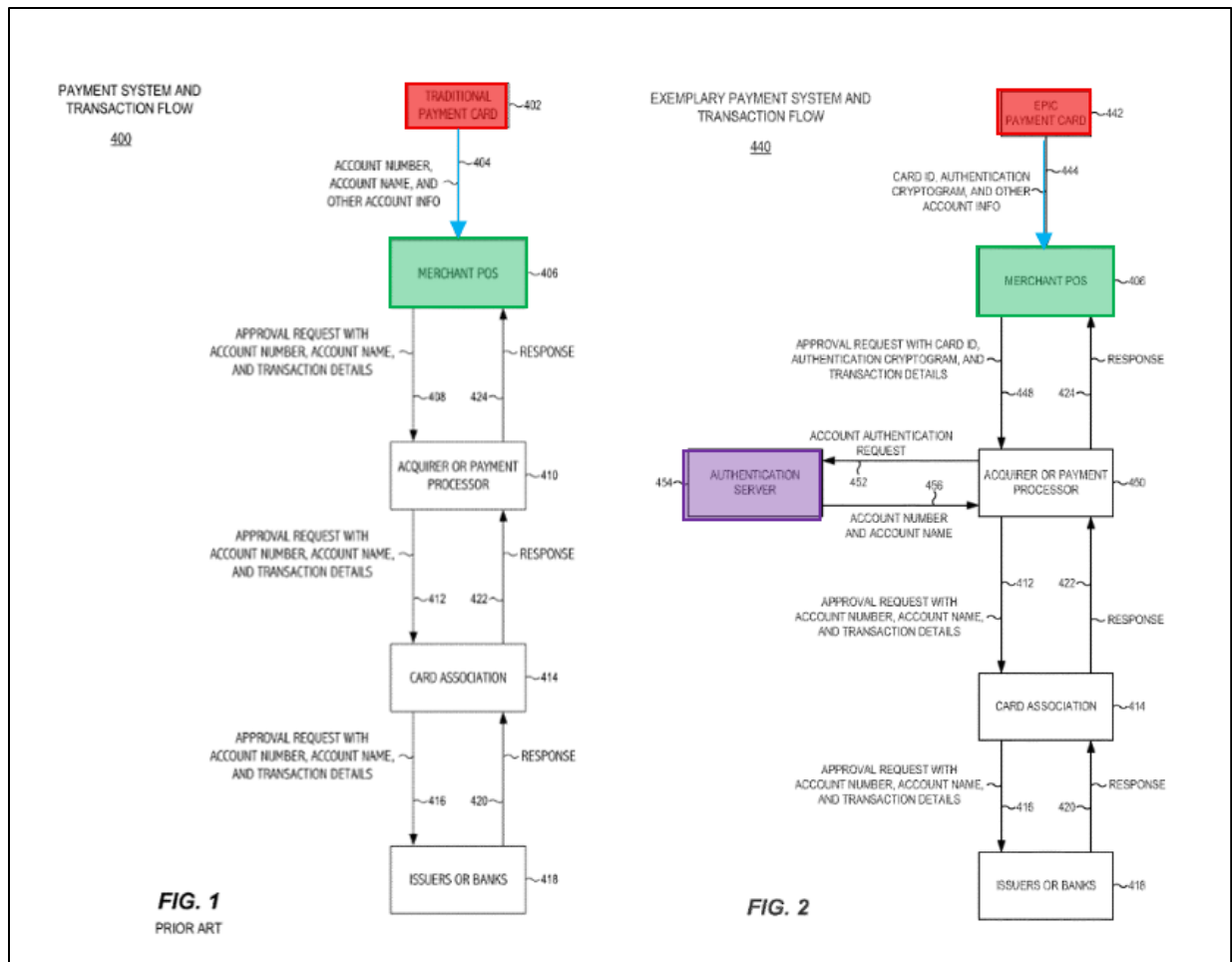
display, as taught by Amacker.” Pet., 59. There is no reasoned basis (and Petitioner provides none) for why a POSITA would seek to make such a combination, when it would require losing key compatibility with traditional systems.

Moreover, while Gomez mentions a mobile phone, it does so only in the context of a user setting up an EPIC account on the backend, not in connection with using the mobile phone as the EPIC payment card or otherwise that the mobile phone has any applicability to making a payment transaction at a traditional merchant POS. *See* EX1007, 20:44-59. If it was, in fact, obvious to turn the EPIC card into a mobile phone as in Amacker (it is not for the reasons explained in this section), then logically Gomez would have mentioned that in its disclosure. That Gomez does not only serves to further confirm a POSITA would not have done so, as it would require losing the core features necessary to traditional payment transactions at a merchant POS.

Second, as discussed above in this Section V.B.1 and in Section III.C, Gomez specifically explains that the “traditional” system to which “no changes” at the **merchant POS** or the card issuer is depicted in its Figure 1, below. *See also* EX1007, 3:65-4:7.

Also as discussed in Section III.C, above, to ensure that its system remains completely compatible with traditional systems without change, Gomez discloses only unilateral communication from the payment card *to* the traditional POS system

as part of the traditional “transaction flow.” *See also* EX1007, 3:65-4:7. It never discloses any communication from the POS system to the card. This is evident, for example, in the comparison of the “prior art” “traditional” system disclosed in Figure 1 with the EPIC card system in Figure 2, where Gomez discloses that **the information** is sent from **the payment card** to **the merchant POS**, but the merchant POS does not send anything to the payment card. EX1007, 3:65-4:7, 5:13-34; *see also* Section III.C, above. This one-way communication is further confirmed by the bi-directional communication elsewhere (*e.g.*, approval requests and responses between the merchant POS and acquirer, the acquirer and card associations, etc.). *See* EX1007, FIGs. 1-2 (below).

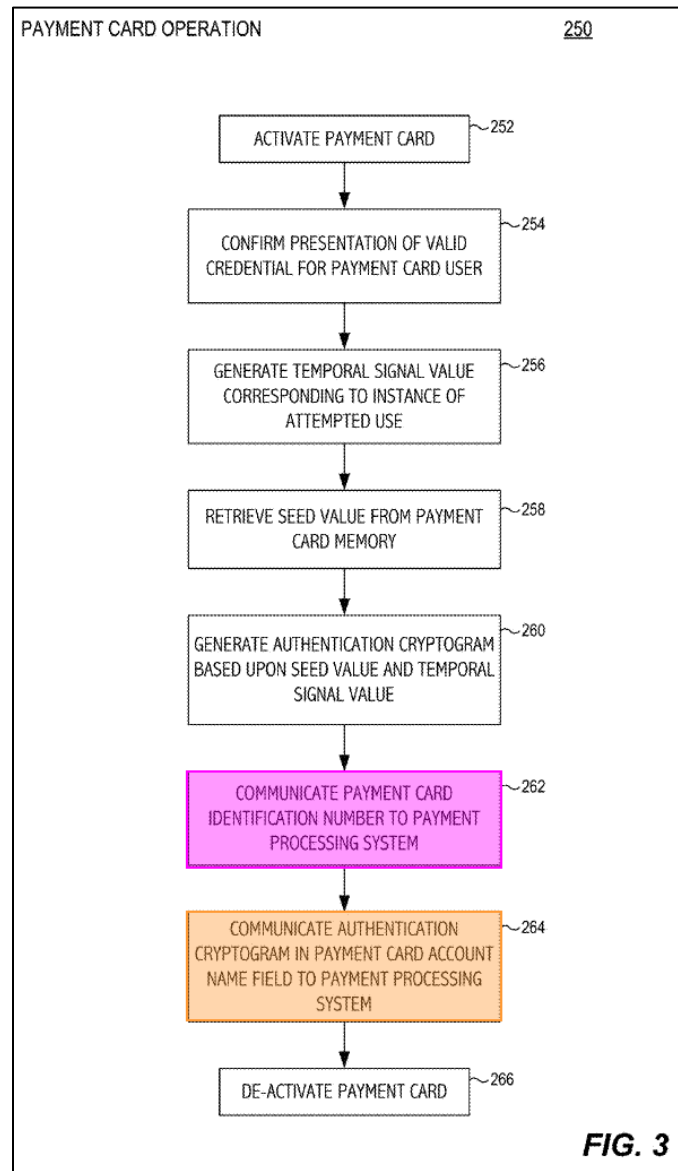


EX1007, FIGs. 1-2; *see also, e.g.*, FIGs. 16, 17, 18 (same one-way information flow from card to merchant POS).

Gomez confirms that in this traditional infrastructure for card swipe (and additionally contactless transactions) the same one-way communication flow occurs: transmitting the information from the card *to* the merchant POS as in traditional payment systems that Gomez is designed to work with, again “[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. For example, in addition to the

disclosures of Figures 1 and 2 and 16-18, Gomez also discloses that the same one-way communication is used for both for magnetic swipe and NFC in Figure 3. Gomez discloses that “[a]t **step 262** [in Figure 3, below] the card communicates the payment card identifying number *to* the payment system.” EX1007, 7:49-50; *see also, e.g.*, 2:42-45 (Gomez’s “payment card may use a programmable magnetic stripe or contactless technology to provide total compatibility with existing POS equipment”). Per Gomez, “[i]n some embodiments this [*i.e.*, sending the payment card number to the **merchant POS**] may be accomplished using a magnetic stripe on the payment card,” and “[i]n some embodiments this [again, sending the payment card number to the **merchant POS**] may also be accomplished using near field communication (NFC)” EX1007, 7:50-54. Similarly, “[a]t **step 264** the card communicates the authentication cryptogram in a payment card account name field *to* the payment processing system” (*i.e.*, to the **merchant POS**). EX1007, 7:57-59; *see also* 14:3-11 (“Transactions are secured by an authentication cryptogram that is generated for each attempted use, and is preferably communicated in the account name field (*i.e.*, of a magnetic stripe on the card, in a NFC transmission, using an online web page, etc.) instead of the cardholder’s actual name. The authentication cryptogram is also preferably encoded using an alpha-numeric code, which may be communicated in the account name field of a traditional payment card system since that field allows alphabetic characters.”). That is, Gomez *exclusively* discloses one-

way communication, as in traditional systems (both card-swipe and contactless) and corresponding “transaction flow” that Gomez was expressly designed to work with, with “no changes.”

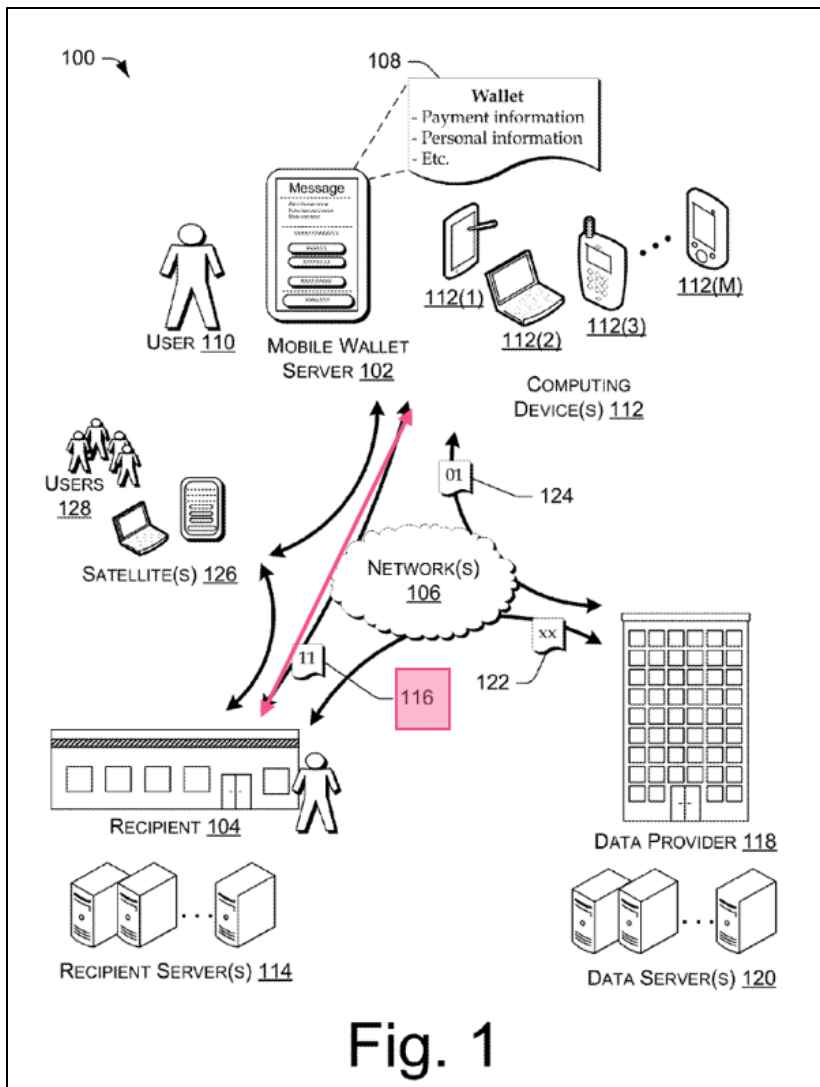


EX1007, FIG. 3; *see also* FIG. 4 (step 286).

Moreover, Gomez teaches that, as in a traditional transaction flow, payment information is communicated from the payment card to the merchant POS at the start

of the process, once “the card is activated by the card user” and the user confirms a valid credential (e.g., at steps 252 and 254 in Figure 3 above). EX1007, 6:65-7:16; *see also* 3:65-4:7, 5:48-6:2, 8:11-24, FIGs. 1-3.

In contrast, Amacker teaches a process in which the recipient initiates contact with the mobile wallet server to request information, which request the user can accept or reject. *See* Section III.D, above; *see also, e.g.*, EX1008, 2:40-49, 3:62-4:6, 6:52-61. This can be seen in Figure 1 of Amacker, below, where there is **bi-directional** communication (**data 116**) between the recipient server 114 and MWS 102 with an entirely different transaction flow. As Amacker explains, “the recipient server(s) 114 may exchange data 116 via the network 106,” where “[t]he **data 116** may include a request transmitted **from** the recipient server(s) 114 **to** the MWS 102 via the network 106.” EX1008, 3:62-4:1. Then “[a] response may be returned to the recipient server(s) from the MWS in the form of an approval that includes associated personal information from the wallet 108,” or [i]n the alternative, the user 110 may optionally reject the request from the recipient server(s) 114 and not disperse personal information from the wallet 108.” EX1008, 4:1-6.



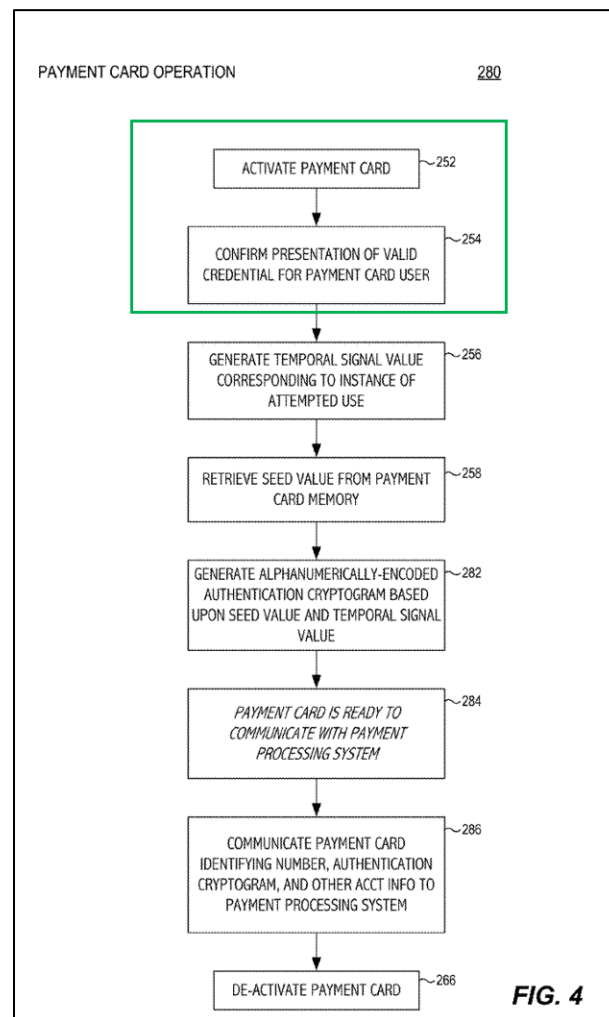
EX1008, FIG. 1.

Amacker does not attempt to be compatible with traditional point-of-sale infrastructure and transaction flow (as Gomez discloses is a necessity) and does not teach presenting the mobile wallet server at a point-of-sale terminal. Thus, applying Amacker's teachings to Gomez would require changes to payment system infrastructure, thereby defeating a primary benefit and necessary part of Gomez's 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. Indeed, Gomez’s statements that “*no changes*” are needed, and its EPIC payment card is designed “to provide total compatibility with existing POS equipment,” etc. (*see, e.g.*, EX1007, 2:40-45, 5:32-34, 5:67-6:2, 10:8-17, 14:3-11, FIGs. 1-2)—teachings Petitioner does not address—teach away from and expressly discourage a POSITA from looking to references that would require such changes to be made in modifying Gomez’s system (such as Amacker). *See, e.g., DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009) (“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.”) (quotation omitted); *Chemour Co. FC, LLC v. Daikin Indus., Ltd.*, 4 F.4th 1370, 1376-77 (Fed. Cir. 2021) (“This is particularly true in light of the fact that the Kaulbach reference appears to teach away from broadening molecular weight distribution and the known methods for increasing melt flow rate. Specifically, Kaulbach includes numerous examples of processing techniques that are typically used to increase melt flow rate, which Kaulbach cautions should *not* be used due to the risk of obtaining a broader molecular weight distribution.”) (emphasis in original).

Third, Amacker’s request for information would be, at best, redundant to Gomez’s system, wherein a user activates the EPIC card, the user is verified, and the

card provides information to the POS terminal *without* a need for a request from the terminal (as discussed above and evident by, for example, Gomez's Figure 3). Gomez, for example, requires the user to take two initial affirmative steps: (1) "At step 252 the card is activated by the user" and (2) "At step 254 the card confirms the presentation of a valid credential for the payment card user," such a PIN number or fingerprint sensor. EX1007, 6:65-7:16.



EX1007, FIG. 4.

Further, since the user already purposefully activated the EPIC payment card, verified a valid credential, and purposefully presented it to the POS terminal (*e.g.*, by swiping it through a magnetic card reader or presenting it in a contactless transaction), thereby signifying the user's desire to perform the transaction, it would be redundant (as well as add an unnecessary step that would only serve to complicate Gomez's system) to then require the user to accept or deny a request for information. But regardless, not only would it be redundant, here too it would require changes to the system, which again, Gomez teaches away from (and expressly discourages). *See, e.g.*, EX1007, 2:40-45, 5:32-34, 5:67-6:2, 10:8-17, 14:3-11, FIGs. 1-2; Section III.C, above.

Fourth, also underscoring the incompatibility of the two references, Amacker seeks to "reduc[e] dissemination of the personal information to additional storage locations (*e.g.*, an entity server used to store personal account information)" (EX1008, 2:49-57) by storing information on the user's mobile wallet server. Gomez, however, teaches that a customer "enter[s] all credit cards information" into the EPIC system, so the EPIC authentication server can retrieve and provide "the actual payment card account number and account name to use for processing the transaction." EX1007, 6:23-27, 20:1-13, FIG. 2. Thus, Gomez teaches exactly the approach that Amacker seeks to avoid: disseminating the personal credit card

information to storage on a third-party system (*i.e.*, the EPIC system). This too cuts against Petitioner’s proposed combination

Fifth, Petitioner argues that a POSITA would have modified Gomez based on Amacker because “[t]his modification would have improved the resulting system by allowing the user to better ensure that they are approving a payment transaction and transmitting payment information to a correct merchant terminal,” “would allow the user to visually review transaction data before approving (or denying) the transaction,” and “would have allowed the user ... extra opportunity to change their mind regarding a transaction, and provide extra assurance that the user intends to initiate a payment transaction rather than having inadvertently opened a payment application.” Pet., 61-62. In support of its conclusory arguments, Petitioner cites only to its expert, who does no more than repeat the same argument, essentially verbatim. EX1003 ¶¶314-315. Such argument (and the corresponding lack of evidence) should be afforded little weight. *See, e.g., Precision Cancer*, IPR2025-00242, Paper 7 at 15-16; *Xerox*, IPR2022-00624, Paper 9 at 15-17; *AT&T Servs.*, IPR2024-01143, Paper 15 at 28, 38.

Regardless, as just explained, the system of Gomez already includes features whereby the user confirms intent to enter a transaction. Petitioner’s argument that the modification would provide “better” or “extra” assurance just confirms the redundancy of Amacker’s teachings were they to be applied to Gomez. Any

incremental benefit from this “extra” assurance would be outweighed by the additional steps imposed on the user, increasing the time and effort required to complete each transaction, especially compared to the traditional card swipe. For example, in the combination of Amacker with Gomez, a user—having already decided to make a transaction and ready to pay the merchant—may have to further (1) activate the card, (2) provide an identifier so the recipient can connect to the device and transmit a request for transaction payment, and then (3) approve or deny the request on the device. A POSITA would not have made such a combination, which is cumbersome and repetitive for the user, particularly where Gomez states that its teachings, by themselves, can “greatly reduce[], if not virtually eliminate[]” theft and fraud. EX1007, 1:58-63.

Lastly, Petitioner asserts that “a POSITA would have modified Gomez such that the EPIC payment card of Gomez is modified to include a larger touchscreen display and/or is integrated into a device having a touchscreen display, as taught by Amacker” and that “[a] POSITA would have recognized that including a larger touchscreen display would have allowed the device to display additional information regarding payment cards, details of the transaction, and transaction status on the device while allowing for easier, intuitive user manipulation via the touchscreen, such as when selecting a payment card, thereby improving the user experience.” Pet., 59-60. Its expert says the same thing, verbatim, without additional evidence or

analysis. EX1003, ¶312. Neither Petitioner nor its expert explain how such a “larger touchscreen display” would or could be implemented into Gomez’s EPIC payment card. Indeed, for all the reasons discussed above, a POSITA would not have sought to modify the size of Gomez’s EPIC payment card, as it would necessarily lose compatibility with traditional systems. This is yet another reason that Petitioner’s proposed combination fails.

For these additional reasons, Petitioner has failed to show there is a reasonable likelihood that it will prevail as to at least one claim based on Grounds 2A-2E.

VI. CONCLUSION

As discussed above, Petitioner’s combinations fail to disclose key limitations of each Challenged Claim of the ’579 Patent and are otherwise unworkable; therefore, the asserted Grounds do not render obvious any claims. The Director should, therefore, deny institution of the Petition.

Dated: November 7, 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 13,683 words, excluding the parts of the paper exempted by 37 C.F.R. §42.24(a) but including any words added to figures.

Dated: November 7, 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 November 7, 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: November 7, 2025

/Matthew G. Berkowitz/

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