

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner

v.

CARDWARE INC.,
Patent Owner

Case No. IPR2023-00314
Patent No. 10,628,820

CARDWARE'S PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The '820 Patent.....	5
III.	Petitioner's Purported Prior Art.....	9
	A. Mullen-876	10
	B. Kobylkin.....	13
	C. Smith.....	15
	D. Gomez.....	19
IV.	Claim Construction.....	21
V.	Level of Ordinary Skill in the Art	21
VI.	Argument	21
	A. Petitioner Fails to Show That The Challenged Claims Are Directed to Printed Matter.....	21
	B. Petitioner Fails to Meet Its Burden as to Grounds 1A, 1B, and 1C....	23
	1. Petitioner Has Not Shown that Mullen-876, Alone Or In Combination With Kobylkin, Discloses “A Thin Shaped Body Having No Fixed Payment Numbers Disposed Thereon” As Required By Limitation 1(1).	24
	2. Petitioner Has Not Shown That Mullen-876 Discloses A “Limited-Use Payment Information...Used...For Payment Transactions ...At Payment Card Facilities” As Required By Limitation 1(6).	30
	C. Petitioner Fails to Meet Its Burden as to Grounds 2A, 2B, and 2C....	36
	1. Petitioner Has Not Shown That Smith Discloses A “Card Device Payment Account Information” or Using it to	

“Generate Limited-Use Payment Information” As Required By Limitations 11(7) and 11(8).	37
2. Petitioner Does Not Demonstrate That A POSITA Would Have Combined Smith with Kobylkin or Gomez.....	41
3. Petitioner Has Not Shown that Smith Or Kobylkin Discloses “Card Issuer Provided Payment Card Information” As Required By Limitation 15(6).	43
VII. The Board Should Exercise Its Discretion to Deny Institution Under 35 U.S.C. § 314(a)	45
A. The Board Should Deny Institution Based on the Efficient Use of the Board’s Time and Resources.....	46
B. The Board Should Deny Institution Under <i>Fintiv</i>	47
1. Factor 1 is Neutral Because There is No Stay of the Parallel District Court Litigation.....	48
2. Factor 2 Favors Denial Because the Board’s Written Decision Deadline Will Come Long After the Trial Date	48
3. Factor 3 Favors Denial Because of the Parties’ Significant Investment in the Parallel Proceeding by the Time of Institution, Including for Invalidity	50
4. Factor 4 Favors Denial Because the District Court Litigation Involves the Same Claims and the Same Arguments and Petitioner has Only Stipulated to Very Narrow Estoppel	50
5. Factor 5 Favors Denial Because the Parallel District Court Litigation and the Petition Involve the Same Parties.....	52
6. Factor 6 Favors Denial Because The Merits Are Weak	52
VIII. Conclusion	52

TABLE OF AUTHORITIES

	Page
Cases	
<i>Apple Inc. v. Fintiv Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	45, 47, 51
<i>Chevron Oronite Co. v. Infineum USA L.P.</i> , IPR2018-00923, Paper 9 (PTAB Nov. 7, 2018)	46
<i>Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.</i> , IPR2020-00122, Paper 15 (PTAB May 15, 2020)	48
<i>C.R. Bard Inc. v. AngioDynamics, Inc.</i> , 979 F.3d 1372 (Fed. Cir. 2020)	22
<i>Deeper, UAB v. Vexilar, Inc.</i> , IPR2018-01310, Paper 7 (PTAB Jan. 24, 2019)	46
<i>Ericsson Inc. v. Collision Commc 'ns, Inc.</i> , IPR2022-01233, Paper 12 (PTAB Jan. 19, 2023)	47, 51
<i>Google LLC v. Jawbone Innovations, LLC</i> , IPR2022-00888, Paper 12 (PTAB Nov. 28, 2022)	46
<i>In re DiStefano</i> , 808 F.3d 845 (Fed. Cir. 2015)	22
<i>Nanya Tech. Corp. v. Monterey Research, LLC</i> , IPR2021-00171, Paper 8 (PTAB May 26, 2021)	45, 46
<i>Next Caller Inc. v. TrustID, Inc.</i> , IPR2019-00961, Paper 10 (PTAB Oct. 16, 2019)	48
<i>NetScout Sys. Inc. v. Longhorn HD LLC</i> , IPR2021-01258, Paper 11 (PTAB Feb. 10, 2022)	46
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	37
<i>Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.</i> , 711 F.3d 1348 (Fed. Cir. 2013)	37

<i>Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC</i> , IPR2019-01218, Paper 7 (PTAB Jan. 7, 2020)	48
<i>Sand Revolution II, LLC v. Continental Intermodal Group – Trucking, LLC</i> , IPR2019-01393, Paper 24 (PTAB Jun. 16, 2020)	47, 49
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)	50
<i>Tate Access Floors, Inc. v. Interface Architectural Res., Inc.</i> , 279 F.3d 1357 (Fed. Cir. 2002)	37
<i>Xerox Corp. v. ByteMark, Inc.</i> , IPR2022-00624, Paper 12 (PTAB Feb. 10, 2023)	28

Statutes

35 U.S.C. § 314(a)	45, 46, 51
35 U.S.C. § 316(a)(11)	48

PATENT OWNER'S EXHIBIT LIST

No.	Exhibit Description
2001	Docket Control Order for <i>CardWare Inc. v. Samsung Electronics Co., Ltd.</i> , Case No. 22-cv-00141-JRG (E.D. Tex.)
2002	Median Time-to-Trial for Patent Cases before Judge Gilstrap for cases filed on or after January 1, 2019 (Source: DocketNavigator; as of March 10, 2023)
2003	Order Denying Motion to Stay in <i>CardWare Inc. v. Samsung Electronics Co., Ltd.</i> , Case No. 22-cv-00141-JRG (E.D. Tex.)

I. INTRODUCTION

On December 23, 2022, Samsung Electronics Co., Ltd. (“Samsung” or “Petitioner”) filed a Petition requesting *inter partes* review of claims 1-20 (“Challenged Claims”) of U.S. Patent No. 10,628,820 (“the ’820 Patent”) (Ex. 1001), entirely on obviousness Grounds. Paper 2 (“Petition” or “Pet.”). On January 20, 2023, 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 1C, which rely on the Mullen-876 primary reference, and Grounds 2A through 2C, which rely on the Smith primary reference, each suffer from several significant flaws.

First, none of the Petitioner’s references disclose a thin shaped body having no fixed payment numbers disposed thereon as required by claim 1. Instead of disclosing a card with no fixed payment numbers disposed thereon, Mullen-876 discloses device embodiments with a display that conveys *fixed* numbers in *all* modes of operation. Specifically, even when that display is conveying “dynamic credit card numbers,” Mullen-876 teaches that there is always at least one static prefix number, an “information type” portion, that is used to facilitate processing recognition of whether the remainder of the displayed payment information is static

or dynamic. Indeed, Mullen-876 specifically teaches the importance of fixed leading digits of the account number in order to retain compatibility, and to identify the payment network “digits one and two may be representative of credit card type 1211 (e.g., American Express).” *See* Ex. 1004, [0100].

Petitioner’s proposed combination of Mullen-876 (a credit card) and Kobylkin (effectively a rechargeable debit card) does not fill the gap and also makes little sense. The dynamic card of Mullen-876 is designed to “completely eliminate” fraud, including via “online” transactions. *See* Ex. 1004, [0003], [0012]; *id.*, [0021] (“[A] credit card may be provided that includes a dynamic security code for online purchases”). It makes no sense to modify Mullen-876 with the disposable debit card of Kobylkin, which cannot be used for online transactions. Petitioner’s expert simply parrots the petition on this point and does not even attempt to address this critical question. Moreover, Mullen-876 teaches away from a card with a purely dynamic credit card number that is continually updated without a display, because such an implementation would not be in synchronization with the processing facility for online transactions (*i.e.*, card-not-present use-cases). Further, with a blank (display-less) card, Mullen-876 would be incapable of presenting the number to a cardholder for checkout to the cashier for verification, rendering it useless for payment transactions or returns.

Second, none of Petitioner’s references disclose “limited use” payment information “used...for payment transactions...at payment card facilities,” *i.e.*, “limited” to use in card-present (and not online) transactions as required by claim 1. Instead, Mullen-876, the sole reference Petitioner relies on for this limitation, discloses payment information intended for use in card-present transactions *and* in online (card-not-present) transactions. The Mullen-876 solution—disclosing numbers on a display—does little to solve the specific security problem for card-present transactions (namely, that the number can be viewed by onlookers, including merchants).

Third, none of Petitioner’s references disclose “*card device* payment account information,” as required by claim 11. (Emphasis added). More specifically, none of Petitioner’s references disclose payment account information that is associated with the card or device, or use such information to generate limited-use payment information, as required by claim 11. Petitioner’s position simply read “card device” out of the claim language. Instead, every number disclosed in Smith, the sole reference Petitioner relies on for these limitations, discloses a mobile cloud account number (“MCA”) that is associated with and used in transactions in place of a real card account number (“RCA”), which is not associated with a device and, in fact, can be associated with multiple cards.

Fourth, Petitioner fails to show how the proposed combinations would meet the limitations of the Challenged Claims. With respect to Grounds 1A through 1C, Petitioner fails to show how a POSITA would have combined Mullen-876 with Kobylkin to create a “thin shaped body having no fixed payment numbers disposed thereon” as required by independent claim 1, when both devices clearly disclose card embodiments bearing the representations of fixed payment numbers.

With respect to Grounds 2A through 2C, Petitioner fails to show how using the mobile device of Smith to activate and/or fund the physical card of Kobylkin for card-present transactions would be useful for online transactions as required by independent claims 11 and 15. Also with respect to Grounds 2A through 2C, Petitioner fails to show any motivation for a POSITA to implement the credential checks of Gomez intended for an electronic card bearing payment information on its face in the far more sophisticated and secure mobile device of Smith.

Fifth, none of Petitioner’s references discloses “card issuer provided payment card information” as required by claim 15. Contrary to Petitioner’s assertions, Smith’s mobile device only downloads and saves service provider, and not card issuer, provided information. In fact, Smith discloses that card-issuer provided information—*i.e.*, the RCA—is never downloaded to the device, whether wired or wirelessly. Also, in addition to failing to show that its asserted combination of Smith and Kobylkin would be useful at all, as discussed above, Petitioner fails to show that

using the mobile device of Smith to activate the physical card of Kobylkin would require Smith's mobile device to download and save any information.

Both the Mullen-876- and Smith-based combinations fail to disclose all of the claim limitations and the proposed combinations are otherwise unworkable. Institution should be denied.

II. THE '820 PATENT

When David Wyatt conceived of the invention claimed in the '820 patent, over a decade ago, there were "several different types of credit cards available in the marketplace." Ex. 1001, 1:35-36.

As the patent explains:

A first type of credit card is a conventional, standard piece of plastic with a magnetic strip, which is readily available and in wide commercial use. The advantage of this first type of credit card is that a large portion of the infrastructure for credit card transactions is built around this type of card, and consequently such a card works in a wide array of vendors' credit card machines, automated teller machines (ATMs), and other devices that support the present credit card and banking infrastructure.

Ex. 1001, 1:36-44.

The '820 patent also 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.” *Id.*, 9:56-60. The claimed invention “address[es] security concerns of a credit card owner on several fronts” while remaining compatible with the existing credit card infrastructure. *See id.*, 9:60-62.

For example, instead of a conventional credit card device that bears all of the static payment information necessary for completing a card-present or online transaction printed on it, the '820 Patent claims a credit card device with no fixed numbers on it at all. Specifically, the '820 Patent teaches an “electronic credit-card-like multifunction electronic device that has no fixed payment information,” as shown in Figure 11 below. Ex. 1001, 3:60-63; *id.*, 11:36-39 (“Effectively, embodiments of the present disclosure provide a multi-function electronic device that has no fixed number, as illustrated in FIG. 11, and therefore the account cannot be compromised.”). This no fixed payment numbers device specifically protects against certain security risks for card-present (in-store) transactions, including the risk that an onlooker sees usable payment numbers on a physical card and uses them at a later time illegally. *See, e.g.*, Fig. 11, below.

Card Device with no Fixed Payment Information

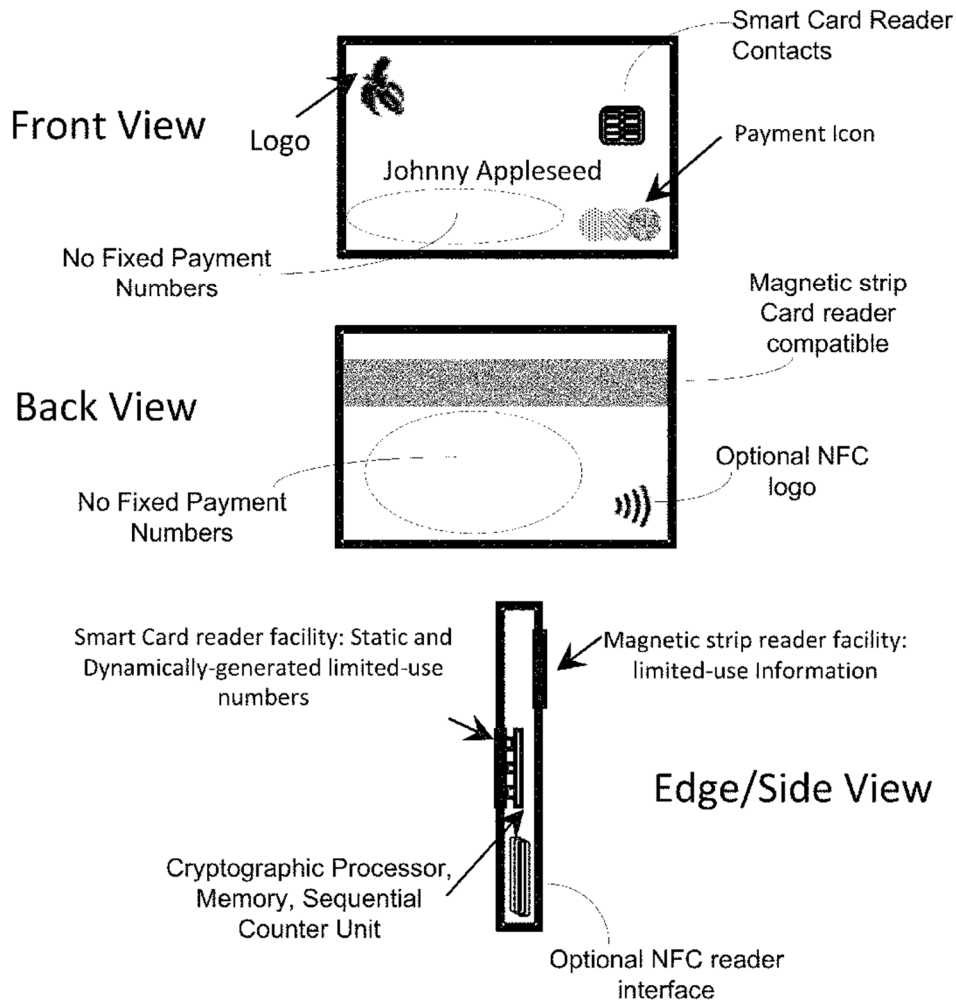


Fig 11

As stated in the '820 Patent, the claimed card device is able to perform online transactions by communicating with a "computer or other device" using wired and/or wireless forms of communication between the card and devices, via "any of the connection means available to the multi-function electronic device (USB 270, NFC 260, and RFID 265)." *See* Ex. 1001, 11:55-57.

Unlike Mullen-876, the claimed invention does not require a display in order to perform all modes of transactions on all facilities. The intentional absence of fixed-numbers limits the use of the card device to card-present reader facilities, while including interfaces to leverage a user's personal computing device to perform online transactions. *See id.*; *id.*, 12:49-13:11; *id.* Figs. 5, 10 (below).

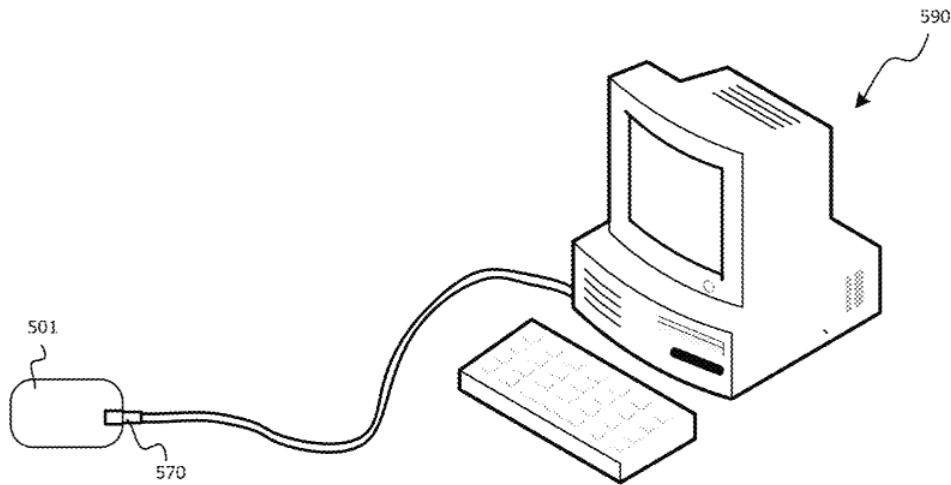


FIG. 5

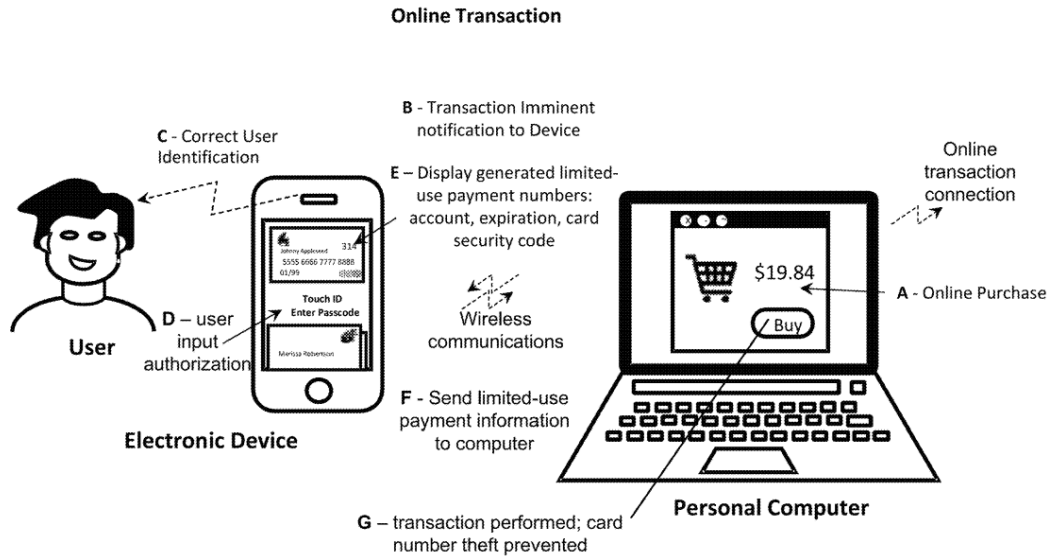


Fig 10

The claims of the '820 patent recite payment devices and online payment systems that include many of the foregoing features, among others. For example, Claim 1 claims a payment device having a thin shaped body (*i.e.*, a card) that conveys payment information, including limited-use payment information to be used at payment card reader facilities (*i.e.*, card-present transactions) in place of card issuer payment information. As another example, Claims 11 and 15 claim online payment systems including a thin shaped body and a personal device that generates and transmits limited-use payment information for use in online transactions.

III. PETITIONER'S PURPORTED PRIOR ART

Petitioner presents two sets of grounds: (i) Grounds 1A through 1C, based on the combination of U.S. Patent App. Pub. No. 2008/0302876 ("Mullen-876") and U.S. Patent App. Pub. No. 2013/0166441 ("Kobylkin"), alone or in combination

with one of two additional references; and (ii) Grounds 2A through 2C, based on the combination U.S. Patent App. Pub. No. 2013/0232083 (“Smith”), Kobylkin, and U.S. Patent No. 9,600,808 (“Gomez”), alone or in combination with one or more additional references.¹ As summarized below, Mullen-876 and Smith—alone and in combination with other references—fail to disclose key limitations, such as a “thin shaped body having no fixed payment numbers disposed thereon” or a “limited-use payment information...used...for payment transactions...at payment card facilities” required by claim 1, a “card device payment account information” as required by claim 11, and a “card issuer provided payment card information” as required by claim 15. Additional reasons why the Grounds fail are also provided below in Section VI.

A. Mullen-876

Mullen-876 describes credit cards and “systems and methods for protecting against credit card fraud.” Ex. 1004, [0002]. Mullen-876 describes “a dynamic credit card with a visible number that changes periodically (e.g., roughly every minute) or changes after each use,” “such that credit card numbers may not be copied by thieves and used at later times. *See id.*, Abstract, [0009]. This “dynamic number”

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

is “displayed to a user via a display (e.g., so that online purchases can be made) or written onto a magnetic stripe such that the number may be processed by traditional credit card merchants (e.g., swiped).” *Id.*, Abstract, [0065], [0112].

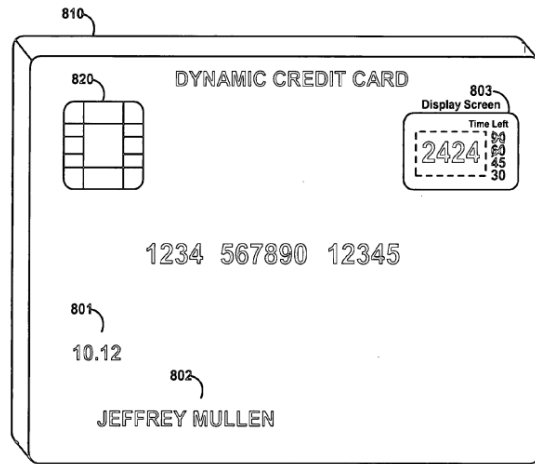


FIG. 8

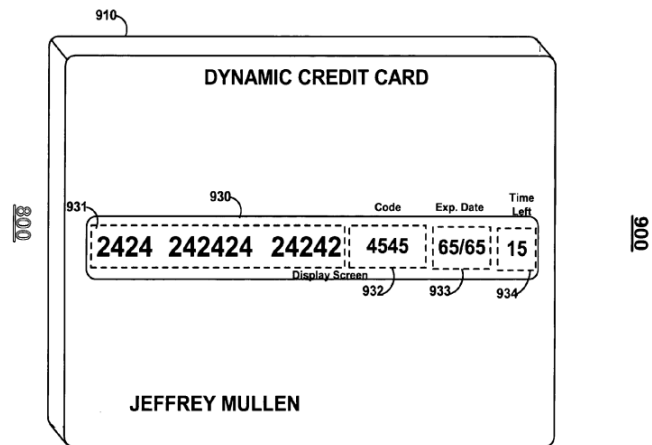
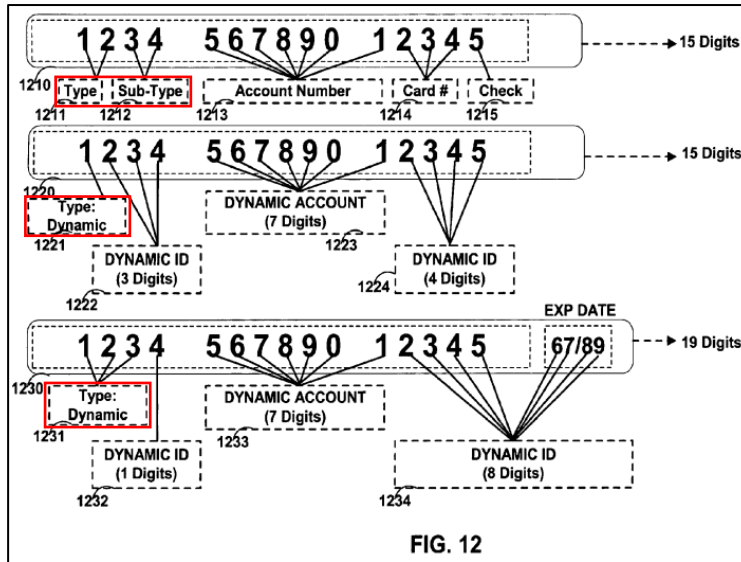
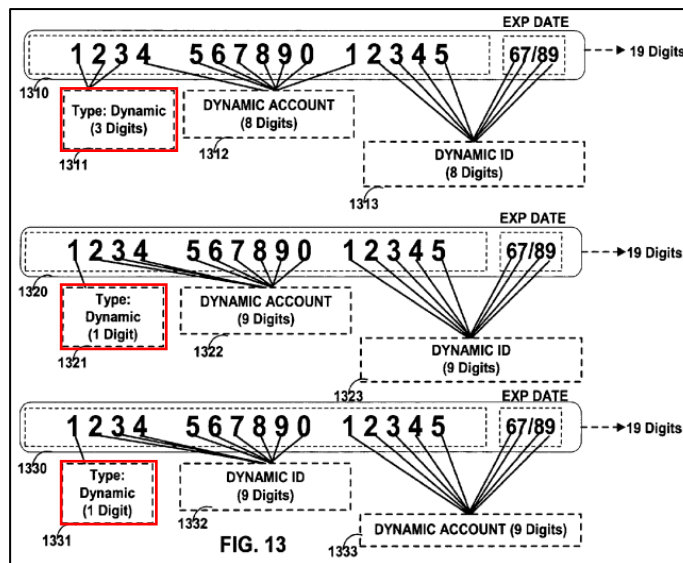
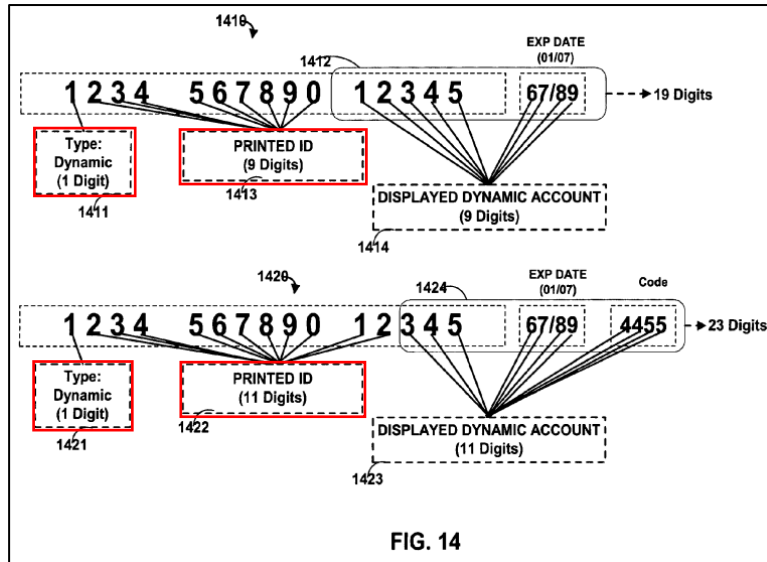


FIG. 9

Mullen-876 describes cards that display static (*i.e.*, fixed) and “dynamic” payment numbers. For example, Figure 8 (above) depicts a credit card with the credit card number and expiration number “printed and/or pressed” into the card and a display “for displaying a security code (e.g., a credit card verification number).” Ex 1004, [0091]. As another example, Figure 9 (above) depicts a credit card with a display that displays a “dynamic credit card number 931,” that includes one or more static portions, as shown in red boxes in Figures 12 through 14 below. *See id.*, [0092], [0100]-[0109], Figs. 12-14.





These static portions of the displayed dynamic credit card number displayed on the card convey type information about the card and the “dynamic credit card number”—including whether the following numbers are static or dynamic—so that the receiving processing facility can select the appropriate verification process or route the payment information to the correct processing facility. *See id.*, [0100]-[0109], Figs. 12-14.

B. Kobylkin

Kobylkin describes “[a]n instant disposable payment card [having] a quick response (QR) code,” as shown in Figure 5 (below). Ex. 1005, Abstract, [0011]; *id.*, [0032] (“The instant disposable payment card can be a disposable card printed on paper or any other material.”). The QR code is associated with a user’s payment provider account such that “product purchased with the instant disposable payment card can readily be paid for via the payment provider account (via the instant

disposable payment card account).” *Id.*, [0030]; *see also id.* [0038] (“The QR code can contain information about...a user account, a payment provider, [or] a code or card identifier...”). “The user can activate or fund the instant disposable payment by scanning the QR code, such as with a user’s smart phone,” and the user can request to “connect an existing payment provider customer account to the card account. *Id.*, [0031]. Because the card account number is encoded into the QR code, after activating and/or funding “[t]he user can [then] use the card to make payments, such as by a merchant scanning the QR code.” *Id.* [0031]-[0032]; *see also id.*, [0035] (disclosing that a merchant can “scan the QR code to accept payment from the user for goods or services”).

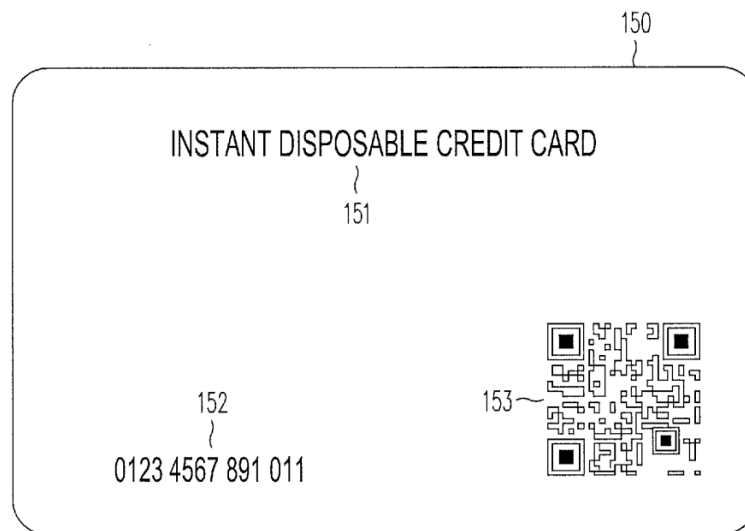


FIG. 5

C. Smith

Smith describes techniques for conducting contactless payment transactions with a mobile device. Ex. 1006, [0002]. Smith discloses a mobile device that maintains “mobile cloud accounts” in a virtual wallet, where any of the mobile cloud accounts can be used to conduct a contactless transaction. Ex. 1006, [0032]-[0037]; *see also id.*, [0029] (“Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.”). “A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA).” *Id.*, [0034]. “The RCA may correspond to a payment account issued to the user by an issuer 112,” and “[t]he MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA.” *Id.* “As a result, the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.” *Id.*

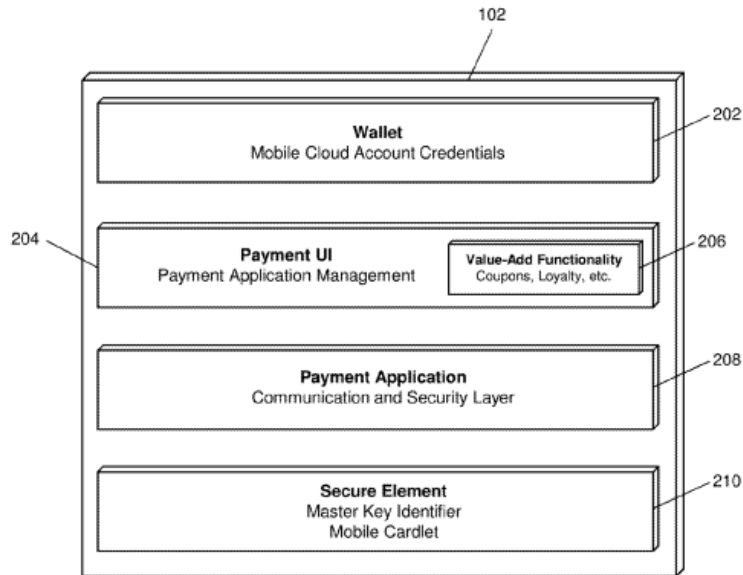


FIG. 2

As shown in Figure 2 above, Smith discloses a mobile device for conducting contactless payment transactions using the MCA. *See* Ex. 1006, [0041]. The mobile device includes a secure element that stores “a master key identifier and a mobile cardlet” in separate portions therein. *Id.*, [0043], [0050]-[0051]. The master key identifier “may be unique to the mobile device” and “may be provisioned to the secure element...by the manufacturer of the mobile device...at the time of the manufacture” or “maybe provisioned to the mobile device... and stored in the secure element...via over-the-air (OTA) processing.” *Id.*, [0044], [0049], [0051], [0054]. The mobile cardlet may also be provisioned physically or via OTA processing but “may contain no payment credentials upon provisioning to the mobile device” and only later “may be configured to store mobile cloud account data for the transmission

of payment credentials including the [MCA] to the contactless terminal[.]” *Id.*, [044], [0045], [0049].

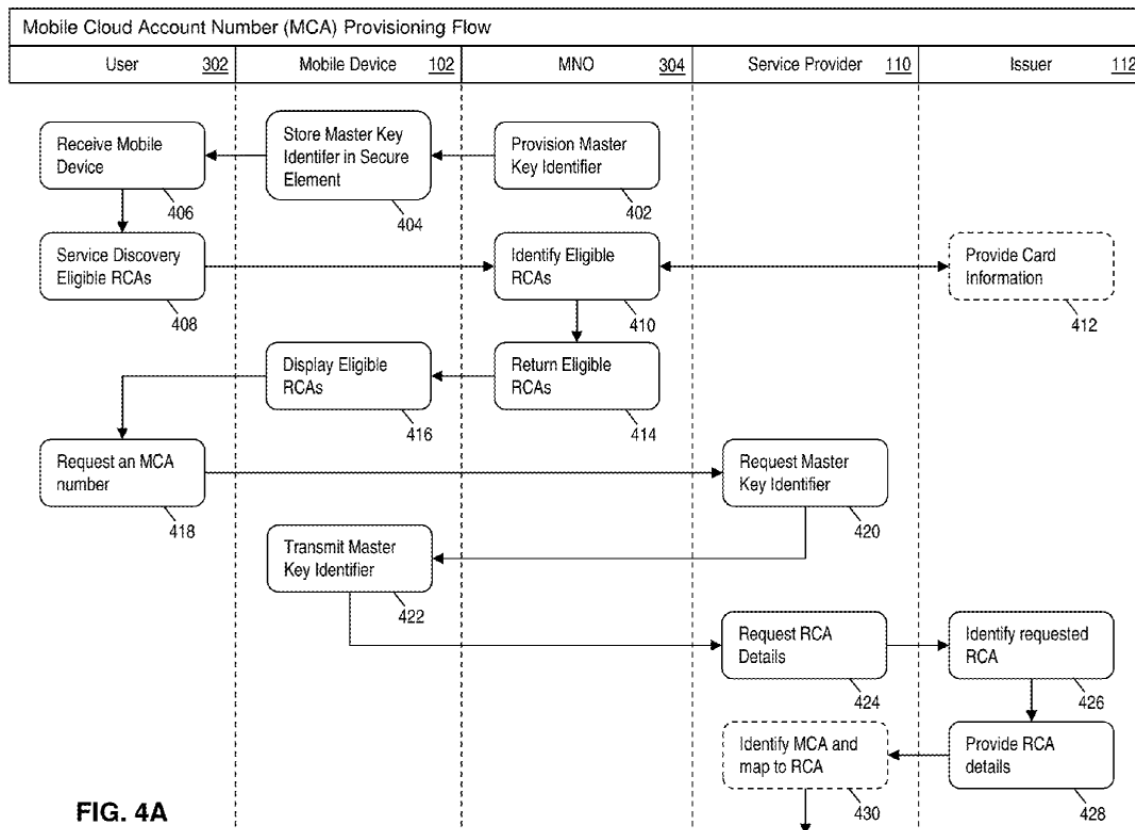
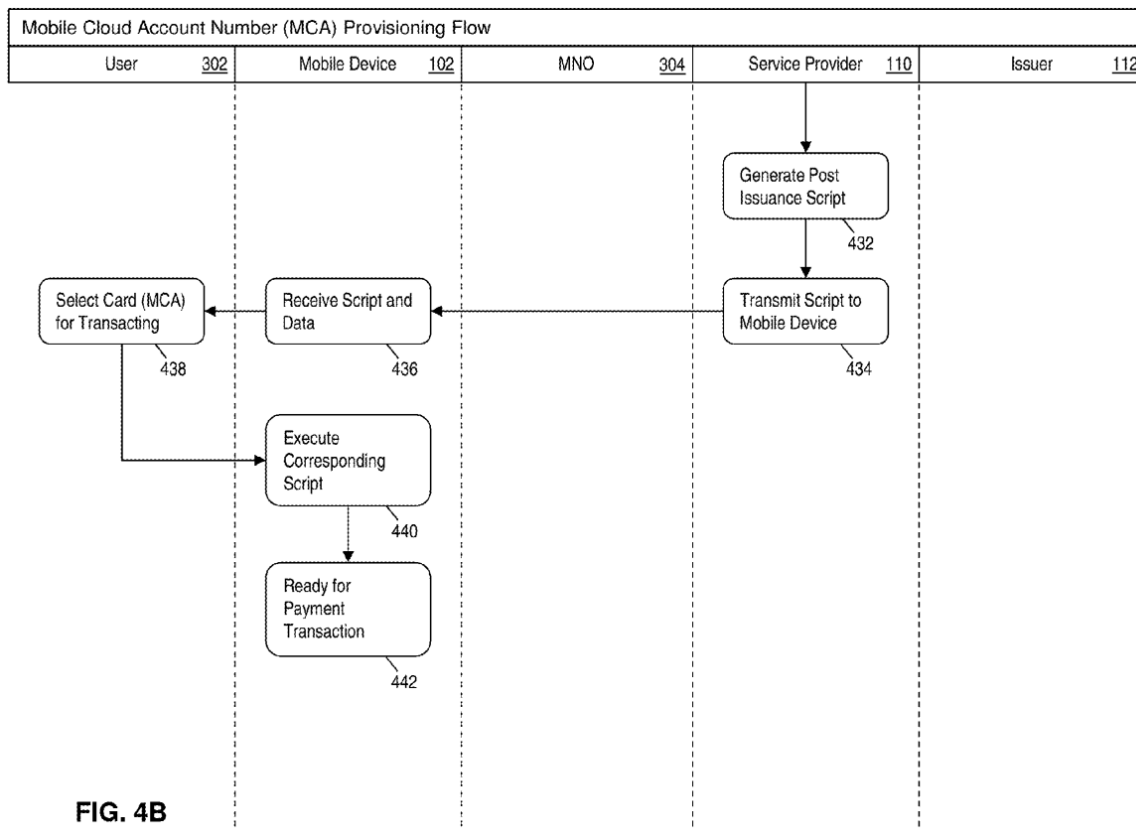


FIG. 4A



Id., FIG. 4A, 4B.

As shown in Figures 4A and 4B above, Smith discloses that a user may submit a request for MCA for an eligible RCA to a service provider via their mobile device. Ex. 1006, [0056]. The service provider will then request master key identifier from the secure element of the user's mobile device and RCA-related information from the issuer and them to identify an MCA and map the MCA to the RCA. *Id.*, [0056]-[0057]; *see also id.*, [0079]-[0087], Fig. 9 (describing the process of a service provider mapping an MCA to an RCA). The service provider will then issue a script to the mobile device that causes the mobile device to transmit the mobile cloud

account data (including the MCA) into the mobile cardlet saved inside the secure element. *Id.*, [0058]-[0059].

D. Gomez

Gomez describes a payment card that incorporates and displays thereon, a static “EPIC account number” linked to a user’s standard credit/debit card number. The “EPIC account number” is used in payment transactions in place of the user’s standard credit/debit card number, and is sent to a merchant with an “authentication cryptogram” that is generated at the time of a transaction. Ex. 1007, 5:48-6:22.

Gomez depicts various embodiments of its EPIC cards in Figures 9-14 (below; fronts depicted in Figures 9, 11, 12, 13, and 14 and backs in Figures 10 and 12). The EPIC account numbers are shown in red boxes, below, “as with many traditional payment cards.” Ex. 1007, 11:19-27, 11:63-66, 12:41-45, 13:5-10, 13:14-19, 13:34-39; *see also id.*, 5:7-10 (disclosing that, in an exemplary system, payment card “information [] can be gleaned from a payment card either by visually observing information printed or embossed on the card, or by reading the magnetic stripe”). “A fully static (16-digit account number) and (3-digit) security code,” as with traditional cards, “are preferably utilized.” *Id.*, 11:49-52. In other words, the EPIC account number is hard-encoded onto the payment card.

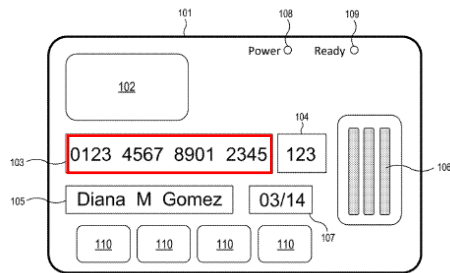


FIG. 9

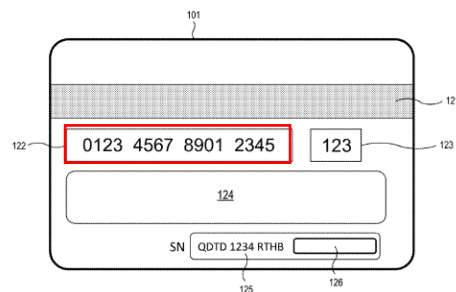


FIG. 10

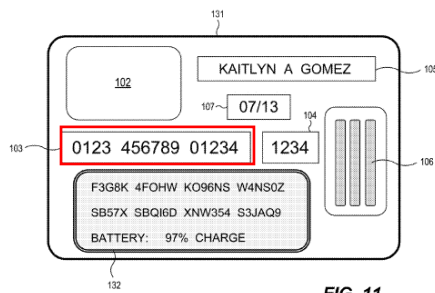


FIG. 11

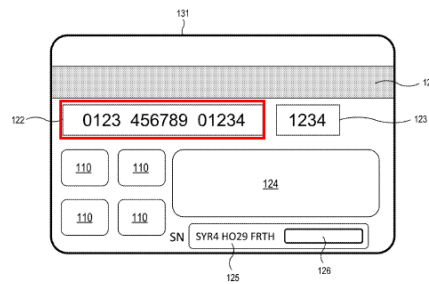


FIG. 12

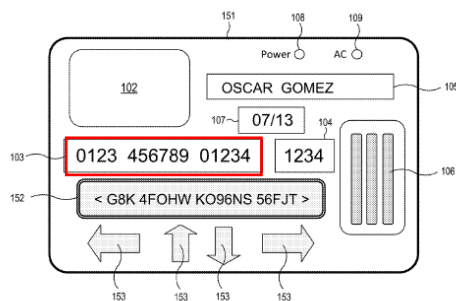


FIG. 13

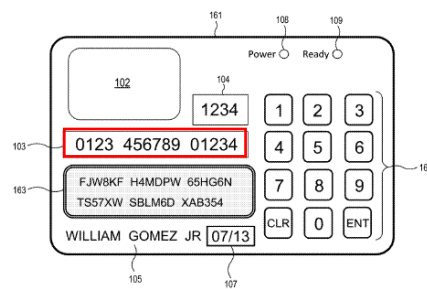


FIG. 14

According to Gomez, when a card holder wishes to complete a transaction, the card holder “swipes the payment card through a POS terminal at the merchant just like a traditional magnetic stripe payment card,” and the information such as the public identifying number, is ““left behind”” and “readily observable.” Ex. 1007, 5:32-40; *see also id.*, 13:63-65 (“the payment card identification [is] visible and left behind after a transaction”).

IV. CLAIM CONSTRUCTION

For the purposes of this Preliminary Response only, Patent Owner believes that the claims should carry their plain and ordinary meaning. In some instances, Patent Owner believes that Petitioner ignores or is simply incorrect about the plain and ordinary meaning of claim terms. Patent Owner's explanations about those issues are contained within the body of the arguments set out below.

V. LEVEL OF ORDINARY SKILL IN THE ART

For the purposes of this Preliminary Response only, Patent Owner does not dispute Petitioner's assertion that a person of ordinary skill in the art as of the Critical Date (a "POSITA") would have had (1) a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and (2) one to two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technology, where graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

VI. ARGUMENT

A. Petitioner Fails to Show That The Challenged Claims Are Directed to Printed Matter

Petitioner offers a conclusory argument that the limitations requiring no fixed payment numbers of Challenged Claims 1, 2, 11, 12, 15, and 16 are directed to printed matter and not entitled to patentable weight. *See* Pet. 3-4. Petitioner is wrong

because “a limitation is printed matter only if it claims the content of information,” and these limitations do not claim the content of any information. *See id.*; *In re DiStefano*, 808 F.3d 845, 848-51 (Fed. Cir. 2015) (“[P]rinted matter must be matter claimed for what it communicates.”); *C.R. Bard Inc. v. AngioDynamics, Inc.*, 979 F.3d 1372, 1381 (Fed. Cir. 2020) (“[P]rinted matter encompasses any information claimed for its communicative content.”). Rather, these limitations claim that the thin shaped body of claims 1 and 2, the thin payment device of claims 11 and 12, and the thin card-shaped payment card device of claims 15 and 16 do *not* communicate such information.

Even if the limitations were directed to printed matter—they are not—they are entitled to patentable weight because they are functionally related to the claimed devices within the claimed system. *See DiStefano*, 808 F.3d at 850-51. Specifically, the claimed “no fixed payment numbers” enhances the security of the claimed systems of claims 1, 2, 11, 12, 15, and 16 by removing the possibility that “a malicious third party [would] record [such information] in order to later make fraudulent transactions on the account.” *See Ex. 1001*, 9:55-62. Further, the absence of the fixed payment numbers ensure that “[o]nly the [limited-use payment information] generated at the instant the [claimed systems are] being used matters,” because it is the only payment information in the claimed systems that is communicable to a merchant. *See id.*, 18:1-5, claims 1, 11, 15.

B. Petitioner Fails to Meet Its Burden as to Grounds 1A, 1B, and 1C.

Petitioner's Ground 1A asserts that Challenged Claims 1, 2, 6, and 10 are obvious over a combination of Mullen-876 and Kobylkin; Ground 1B asserts that Challenged Claims 3-5 and 7-8 are obvious over the same Mullen-876-Kobylkin combination, plus Patel; and Ground 1C asserts that Challenged Claim 9 is obvious over the same Mullen-876-Kobylkin combination, plus Smith. These Grounds should be rejected at least because none of the references discloses or teaches a payment device (i) "having no fixed payment numbers disposed thereon or (ii) that conveys "limited-use payment information...for payment transactions...at payment card reader facilities" required by independent claim 1.

Moreover, the combination of Mullen-876 and Kobylkin, with or without Patel or Smith, makes no sense. A POSITA would never combine those two references to achieve the re-imagined product that Petitioner proffers. The card of Mullen-876 is intended as a "complete" solution. To allow online transactions, the card of Mullen-876 displays a number on its display, such that a user can enter that number online. Kobylkin is effectively a rechargeable (and disposable) debit card that displays a QR code. There is no reason why a POSITA would have effectively reduced the functionality of the card of Mullen-876, given its stated intention to be a complete solution, and effectively eliminated the online payment capability by eliminating the displayed numbers.

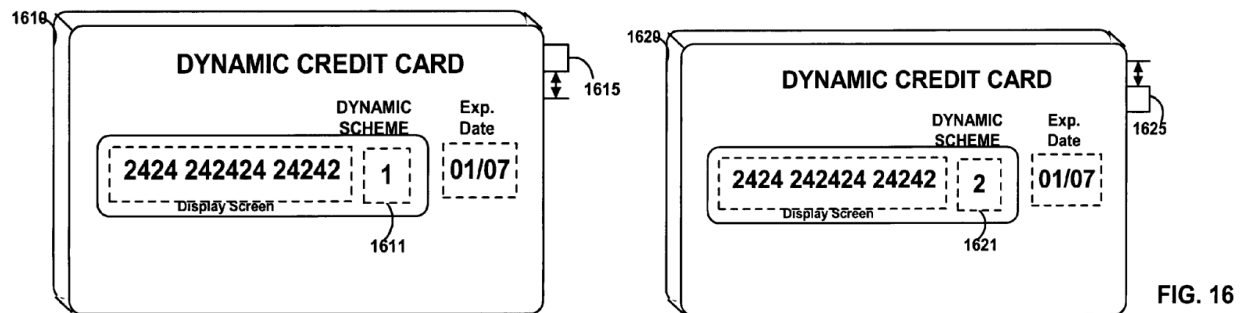
1. Petitioner Has Not Shown that Mullen-876, Alone Or In Combination With Kobylkin, Discloses “A Thin Shaped Body Having No Fixed Payment Numbers Disposed Thereon” As Required By Limitation 1(1).

Limitation 1(1) recites, “a thin shaped body having no fixed payment numbers disposed thereon[.]” Pet., vi; Ex. 1001, 19:59-60. Claims 2 through 10 each depend directly from claim 1 and therefore include the same limitation. See Pet. vi-x; Ex. 1001, 20:8-22:9.

Petitioner asserts that this limitation is met by (i) Mullen-876’s disclosure of a dynamic credit card which displays “dynamic credit card number” on a display; (ii) Mullen-876’s disclosure of a dynamic credit card number that is “updated continually in real time” such that the dynamic credit card would “not include a display”; and (iii) Mullen-876’s dynamic credit card in combination with Kobylkin’s disclosure of a “substantially blank card.” Petitioner is wrong on all points.

First, none of the dynamic credit card numbers disclosed in Mullen-876 is truly dynamic, and thus none are absent of fixed payment numbers. Every dynamic credit card number taught by Mullen-876 has at least one fixed payment number disposed on a card, contrary to the requirements of limitation 1(1). For example, Petitioner asserts that Figure 16 of Mullen-876 shows an example dynamic credit card having no fixed payment numbers disposed thereon, relying on one half of Figure 16. Pet. 12. But, as shown below, the full Figure 16 (reproduced below)

plainly shows that the card number (“2424 242424, 24242”) and the expiration date (“01/07”) do not change. That is, when the switch 1615 is switched to location 1625, only the “dynamic scheme” number changes. *See id.*, [0111], Fig. 16. The “dynamic scheme” number is not a payment number; it represents the dynamic coding scheme used by the card to generate the dynamic portion of the dynamic credit card number. *See id.*



Ex. 1004, Fig. 16.

Mullen-876’s other embodiments also do not disclose a card with no fixed numbers disposed thereon as required by limitation 1(1). Figure 8 discloses a card with the credit card number and expiration date “printed and/or pressed into” it. Ex. 1004, [0091], Fig. 8. Although Figure 9 of Mullen-876 purports to disclose a card with a display screen 931 displaying “dynamic credit card number 931,” Mullen-876 repeatedly teaches that its dynamic credit card numbers—such as the “dynamic credit card number 931” in Figure 9—include a static portion representing the card type. *See id.*, [0093] (disclosing that “the dynamic credit card may transmit

information indicative of the credit card being a dynamic credit card” so that the recipient would “then know to utilize” other received information).

Any observer would understand that such displayed, static numbers are, in fact, fixed payment numbers, disposed thereon the card.

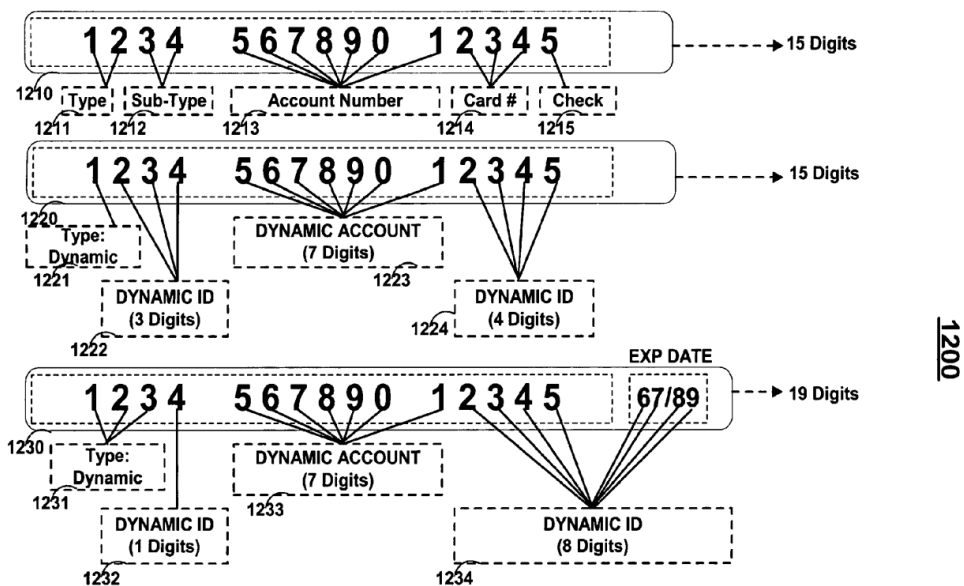


FIG. 12

For example, Mullen-876 discloses in reference to Figure 12 (reproduced above) that “digits one and two [of the number displayed on display 1210] may be representative of credit card type 1211 (e.g., American Express) while digits three and four may be representative of subtype 1212 (e.g., personal credit card, business credit card, American Express Blue, Airline Miles Card, Cash-back Card).” Ex. 1004, [0100], Fig. 12. Accordingly, the first one to four digits in Figure 12 are static, in contrast to the rest of the digits, which are dynamic. Mullen-876 also discloses that a recipient of a dynamic credit card number, for example a processing facility,

may look at the first digit 1221 of the dynamic credit card number 1220 “to determine if the card is a dynamic credit card, a Visa card, a Mastercard, or an American Express card” and then “utilize the appropriate verification process for a particular type or...communicate the number...to the appropriate processing facility.” *See id.*, [0101]-[0102]. That data does not and would not change dynamically. Mullen-876 similarly discloses that the numbers of Figures 13 and 14 include a static portion. *See id.*, [0106], Fig. 13 (discussing that Figure 13 shows three dynamic topologies, each of which include including “type information,” and other “dynamic information”); *id.* [0107]-[0108], Fig. 14 (“Topology 1410 may include static information (e.g., static type 1411 and static information such as identification information 1413) and a display 1412 that may include dynamic information such as dynamic information 1414)...Topology 1420 may be provided that includes static information such as type 1421, information 1422, and dynamic information 1423 displayed on display 1423.”).

Second, Mullen-876 itself teaches that a dynamic credit card with a dynamic credit card number (“DCCN”) that “continually” updates “beyond the refresh rate of the display” would be “useless.” *See* Ex. 1004, [0016], [0056]. Continually updating the DCCN would “quickly exhaust a pool of available numbers,” would “cause the dynamic number to become out of synchronization with the processing facility” such that DCCNs produced by the card “*may not be able to be validated by*

the processing facility” and would “make it impossible for a user to enter a number online.” *Id.* (emphasis added).

Third, contrary to Petitioner’s assertion, a POSITA would not have combined Mullen-876 with Kobylkin. For one, Mullen-876 discloses a credit card; Kobylkin effectively discloses a rechargeable debit card. But, even more importantly, the card of Mullen-876 is intended to “completely eliminate” credit card-related fraud issues (although Mullen-876 did not achieve the goal and did not solve the problem of avoid theft of numbers copied from the display). Ex. 1004, [0004]. As part of this, Mullen-876 discloses a partially dynamic credit card that can be used for an “online credit card purchase.” *Id.*, [0020]; *see also id.*, Abstract, [0012], [0021]. Mullen-876 accomplishes this by displaying a number to the user, who can enter it at the paying stage of an online store. *Id.* Petitioner bizarrely proposes replacing this capability with Kobylkin’s QR code-based approach, which, of course, cannot be used in an online store from a thin-shaped card. Indeed, Kobylkin does not contemplate a thin shaped card that is usable online. Petitioner never explains why a POSITA would *reduce* the functionality of Mullen-876, particularly when Mullen-876 indicates that it is designed as a “complete[]” fraud solution. And, Petitioner’s expert just regurgitates verbatim Petitioner’s positions and should be given no weight in this regard. Pet., Ex. 1003, ¶¶ 115-116; *Xerox Corp et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 (Aug. 24, 2022) (precedential) (expert declarations

that simply repeat a petition argument are “conclusory and unsupported” and are “entitled to little weight.”).

Further, a POSITA would not have expected that the combination of Mullen-876’s card with Kobylkin’s instant disposable payment card to results in a card with no fixed numbers that would “present less risk of fraud.” *See* Pet. 8-9. This is because Kobylkin’s card is not blank at all; it bears a quick read (QR) code representing a payment number printed on it. *See* Ex. 1004, [0017] (“[T]he instant disposable payment card can be a substantially blank card. For example, the instant disposable payment card can have only a QR code or the like thereon.”); *id.*, [0023] (“[T]he payment provider can issue a plurality of blank cards having a QR codes [*sic*] printed thereon.”). In fact, “[t]he account number is encoded into the QR code and transferred to the payment provider” such that a transaction can be completed simply by a merchant scanning the QR code. *See id.*, [0031]-[0032]. A fixed number encoded into a QR graphical encoding does not enhance security, defend privacy, nor protect against duplication or theft. QR codes are amenable to photographic recording (as is already a common method of recording standard credit card

information²), and modern smartphones directly translate QR codes as part of standard functionality, *i.e.*, no additional application required.

As a result, a POSITA would understand that, just like with a traditional credit card information, “a malicious third-p arty [*sic*] [can] record the [QR code] in order to later make fraudulent transactions on the account” represented by the QR code. *See* Ex. 1001, 9:58-60; *see also* Ex. 1004, [0003] (“Particularly, credit card numbers are copied and used without permission. Copying may take many forms.”). Accordingly, a POSITA would not have understood the combination of Mullen-876 and Kobylkin would result in the creation of a card having no fixed payment numbers disputed thereon, and would not have had a reasonable expectation that such combination would make it less “susceptible to theft and/or compromise”, enhance privacy, nor reduce the risk of fraud. *See* Ex. 1001, 2:1.

2. Petitioner Has Not Shown That Mullen-876 Discloses A “Limited-Use Payment Information...Used...For Payment Transactions ...At Payment Card Facilities” As Required By Limitation 1(6).

Limitation 1(6) recites, “wherein further the limited-use payment information is to be used in place of card issuer information for payment transactions by said device at payment card reader facilities[.]” Pet., vi; Ex. 1001, 20:3-7. Claims 2

² *See, e.g.*, “<https://www.wzzm13.com/article/news/investigations/mcdonalds-employee-accused-of-taking-photos-of-customers-credit-cards/69-71372991-6b6a-4bd1-ba7e-e7c23c13bd6c>”

through 10 each depend directly from claim 1 and therefore include the same limitation. *See* Pet. vi-x; Ex. 1001, 20:8-22:9.

Petitioner asserts that this limitation is met by the DCCN in Mullen-876. Pet. 17-18 (citing Ex. 1004, [0090], [0024], [0068]). But Mullen-876 never once states that this DCCN is *limited to use at payment card reader facilities*, as required by claim 1(6). *See supra* Section II.A. In fact, the nature and purpose of Mullen-876 is directed to a DCCN that is usable both at payment card reader facilities *and* online.

Claim 1 of the '820 patent is clearly different; it is directed to a card device with a limited-use number, where the nature of the use-limitation is that it is usable only for card-present transactions “at payment card reader facilities.” And through the absence of any fixed numbers visible thereon, is thus improved against “theft and/or compromise,” as per the '820 Patent. *See* Ex. 1001, 2:1. The plain and ordinary meaning of this is clear and obvious from both the claim language itself as well as the specification.

The '820 patent contains three independent claims. Claim 1 is directed to card-present transactions (*i.e.*, in person) while claims 11 and 15 are both directed to “online” transactions. This is spelled out in the claims themselves. For example, claims 11 and 15 each recite an “online payment system” and various limitations directed to online-based transactions.

On the other hand, claim 1 is directed to in-person transactions, which present unique fraud and security risks (different from those involved with online transactions). Claim 1 recites a payment device with a “reader interface” selected from a set that is all clearly for in-person transactions (*e.g.*, a magnetic-stripe and an NFC interface). A “reader interface” would be meaningless and non-sensical for an online payment system. Further, the payment information for a transaction must be “operable to be conveyed via the reader interface.” Again, this indicates an in-person payment system; by definition card-not-present transactions (requiring only the information visible on the card device) do not leverage the presence of a card to perform the transaction, and thus online payment systems do not convey payment information from the card via any reader interface, such as a magnetic-stripe, chip, or NFC contactless.

Per the claim language, the “payment information” that must be conveyed “via the reader interface” comprises “limited-use information.” Limitation 1(6) removes any remaining doubt about the nature of the “limited-use.” Specifically, the limitation states that “the limited-use payment information *is to be used in place of* card issuer payment information for payment transactions by said device *at* payment card reader facilities.” This is not a mere statement of intended use (nor does Petitioner so argue); it is defining the nature of the limited-use itself in the sense that the payment information is limited in its use to payment card reader facilities

(i.e., in-person, card-present transactions). *See also* Pet., vi; Ex. 1001, 20:3-7 (reciting that the limited-use payment information “is to be used...for payment transactions by [the claimed payment] device at payment card reader facilities” (emphasis added)).

This plain meaning is bolstered by dependent claims 4, 5, and 7, which claim specific embodiments of in-person, card-present transaction.

Limitation 4(1) requires that a “card processing authority reject[] as invalid, any use of [the] limited-use payment information obtained via any means other than: a payment card reader reading said limited-use payment information from the reader interface.” Pet., vii. This further limitation specifies, among other things, the particular entity (a card processing authority) that rejects transactions where the payment information is not obtained from a (physical) reader interface. Claims 5 and 7 are similar and require, respectively, a “card processing authority [that] is operable to reject, as not valid, a use of the limited-use card payment information in a card-not-present payment transaction” (requiring only a recorded information visible on the card device, not the transaction of information by the card device) and “a card issuer...limits valid approval of said limited-use payment information to performing a card-present payment transaction by the card device.” Pet., vii-viii. Again, the limited-use information is limited in the sense that it is only usable for card-present transactions.

Indeed, this is the entire purpose of claim 1. A card with no fixed numbers that generates “limited use” payment information and is used only for card-present transactions at physical card-reader facilities avoids the security risk inherent in displaying payment numbers on a physical card such that it can be viewed by merchants or other passers-by and then used for fraudulent transactions at facilities other than the intended limitation. In particular, claim 1 mitigates the risk that someone can steal the number and use it for online transactions, separate and apart from the physical card. The limited-use payment information of claim 1 is not usable for online transactions.

The '820 patent specification supports this. For example, the '820 patent specifies that, as a security measure, the claimed card device is able to generate, at the time of the transaction, a limited-use payment information “according to...information regarding the facility performing the transaction”—*i.e.*, the card reader that is reading a card device for a particular transaction. *See id.*, 10:66-11:4; *id.*, 11:29-33 (“[T]he dynamic part of the limited-duration credit card number generated may be based on...the facility that is reading the card.”); *id.*, 18:63-66; *see also id.*, 1:51-53 (“The reader provides the manner in which a facility interacts with the built-in processor on the card....”); *id.*, Fig. 11 (pointing out a “Smart Card reader facility” and “Magnetic strip reader facility” on the same card device).

In contrast, Mullen does not disclose that use of a DCCN is to be limited to use at payment card facilities, as required by limitation 1(6). To the contrary, Mullen-876 repeatedly recites that the same DCCN is used for transactions at payment card reader facilities *and* for online transactions. And, all the embodiments include a display for the express purpose of facilitating unlimited use, including for online transactions. *See* Ex. 1004, Abstract (“This dynamic [credit card] number may be displayed to a user via a display (e.g., so that online purchases can be made) or written onto a magnetic stripe such that the number may be processed by traditional credit card merchants (e.g., swiped).”); *id.*, [0065] (“[A] dynamic credit card may be utilized using traditional infrastructure and may be utilized for online (or telephonic) purchases and purchases that require the card to be swiped (or entered into a credit card reader).”); *id.*, [0112] (“Transmission [of “dynamic information (e.g., a dynamic credit card number...)”] may take the form of writing information to a magnetic stripe or displaying information on a display such that a user can enter the information in the checkout/payment stage of an online shopping process...”). Although Mullen-876 discloses that a DCCN may be rejected if used in a different location than where it was generated, this feature relies on associating the DCCN with a *geographic* location, not by limiting use of the DCCN to card-present transactions nor to a card-read facility use-limitation, as required by Limitation 1(6). *See* Ex. 1004, [0082].

Because Petitioner advances no other arguments about how other references identified in Grounds 1A, 1B, and 1C disclose this limitation or why a POSITA would have modified the device of Mullen-876 to convey “limited-use payment information...used...for payment transactions by said device at payment card reader facilities,” Petitioner has not shown a reasonable likelihood of success as to Grounds 1A, 1B, and 1C.

C. Petitioner Fails to Meet Its Burden as to Grounds 2A, 2B, and 2C

Petitioner’s Ground 2A asserts that Challenged Claims 11, 12, 15, 16-18, and 20 are obvious over a combination of Smith, Kobylkin, and Gomez; Ground 2B asserts that Challenged Claims 13 and 19 are obvious over the same Smith-Kobylkin-Gomez combination, plus Varadarajan; and Ground 2C asserts that Challenged Claim 14 is obvious over the Smith-Kobylkin-Gomez-Varadarajan combination, plus Mullen-876. These Grounds should be rejected at least because (i) none of the references discloses or teaches a “card device payment account information” or using such information to “generate limited-use payment information” as required by independent claim 11; (ii) Petitioner has not shown that a POSITA would have implemented the electronic card security measures of Gomez in the mobile device of Smith; and (iii) Petitioner has not shown that Smith or Kobylkin Discloses “card issuer provided payment card information” as required by limitation 15(6).

1. Petitioner Has Not Shown That Smith Discloses A “Card Device Payment Account Information” or Using it to “Generate Limited-Use Payment Information” As Required By Limitations 11(7) and 11(8).

Limitation 11(7) recites “wherein the wireless interface is operable to wirelessly obtain card device payment account information” and limitation 11(8) recites, “wherein the processor is operable to generate limited-use payment information based on the card device payment account information.” Pet. x; Ex. 1001, 22:22-26. Claims 12 through 14 depend from claim 11 and therefore include the same limitation. See Pet. xi-xii; Ex. 1001, 22:36-23:38.

Petitioner asserts that these limitations are met by the “mobile cloud account data” of Smith. Pet. at 53-55 (citing Ex. 1006, [0007], [0021]-[0022], [0029]-[0031], [0044]-[0050], [0058]-[0059], [0067], [0075], [0099], [0103]). But Smith never once states that the “mobile cloud account data” is associated with the device that receives it as required by claim 11.

The plain and ordinary meaning of a card device payment account information is information that is associated with a particular device. In other words, every claim term is presumed to have meaning. See *Power Integrations, Inc. v. Fairchild Semiconductor Int’l, Inc.*, 711 F.3d 1348, 1360 (Fed. Cir. 2013) (“Claim construction begins with the language of the claim....We presume that the terms in the claim mean what they say.”) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc); *Tate Access Floors, Inc. v. Interface Architectural Res.*,

Inc., 279 F.3d 1357, 1370 (Fed. Cir. 2002)). Accordingly, “card device payment account information” must mean something more than just “payment account information.” The phrase “card device” is presumed to have at least *some* meaning. At a minimum, “card device” should at least indicate an association of the payment account information with the particular “card device.” Anything less would fail to differentiate the claim term from the broader phrase “payment account information.” Petitioner ignores this and simply treats the phrase as “payment account information.”

An issuer-issued card account number, termed a real card account number (RCA) in Smith is not associated with a device or card. Indeed, Smith discloses that an RCA have multiple cards issued with the same number, such as when family members or employees of the same corporation share the same credit card account. Ex. 1006, [0084].

Similarly, a patent or other prior art reference disclosing a payment device might indicate that the mobile cloud account data is generated and saved in the secure element of the mobile device. But, again, that does not say anything about whether the account number is associated with the device that receives it, as required by limitations 11(7) and 11(8). *See* Ex. 1001, 22:36-23:38. The same mobile cloud account data could be generated for a RCA and used on multiple electronic devices such as, again, where there are multiple users sharing the same credit card account. In other words, just because the prior art reference only discusses a payment solution

in the context of a single device, does not mean that the mobile cloud account data is associated with that device.

Petitioner advances just this flawed logic in arguing that Smith’s mobile cloud account data is the “card device payment account information” associated with a device. Petitioner assumes that, because Smith discusses only a single device/ single account configuration, the mobile cloud account data is associated with the device that receives it. *See* Pet. 53-54. This is not true. Smith discloses that the “mobile cloud account data” includes a “issuer public key certificate,” a mobile cloud account number (MCA), and an “ICC public key certificate.” *See* Ex. 1006, [0007], [0009]. None of this information is associated with a device.

Smith discloses that a service provider creates the issuer public key certificate; there is no disclosure that this certificate is associated with a device. *Id.*, [0085]. And it is counter-intuitive to assert that a service provider would know every device made by a third party, including the ones they are not responsible for servicing, and which may or may not have a user’s payment information. The MCA, which corresponds to the RCA, is generated by a service provider and may be generated to include attributes of the RCA or even a portion of the RCA. *Id.*, [0083]-[0084]. But the RCA is also not associated with a device—it just “correspond[s] to a payment account”—and so an MCA corresponding to an RCA is also not associated with a device. *Id.*, [0007], [0083]-[0084]. Finally, the ICC public key certificate is also

created by a service provider by certifying an ICC public key—part of an RSA key pair also generated by the service provider—using an issuer private key from an issuer. *Id.*, [0037], [0085], [0089]. Again, Smith does not disclose that the ICC public key certificate, or the ICC public key and the issuer private key issued to generate it, are associated with a device. *Id.*

If Smith intended the mobile cloud account data to be associated with a device, it certainly would have disclosed as much. In fact, Smith refers to a “master key identifier” as “unique” to the mobile device. *See* Ex. 1006, [0043], [0049]. This master key identifier is also stored in the secure element of the mobile device, but separate from the “master cardlet” that stores mobile cloud account data, and may even be provisioned to the secure element by the mobile device maker at the time of the manufacture of the mobile device. *Id.*, [0033], [0043]-[0044], [0077]-[0078], Fig. 8. In contrast, Smith never once says that the separately saved, mobile cloud account data is associated with the device that receives it, or indicates that Smith ever contemplated that the mobile cloud account data was associated with a device.

Because Petitioner advances no other arguments about how other references identified in Grounds 2A, 2B, and 2C disclose these limitations or why a POSITA would have modified the device of Smith to “wirelessly obtain card device payment account information” or to “generate limited-use payment information based on the

card device payment account information,” as required in claim 11, Petitioner has not shown a reasonable likelihood of success as to Grounds 2A, 2B, and 2C.

2. Petitioner Does Not Demonstrate That A POSITA Would Have Combined Smith with Kobylkin or Gomez

Petitioner relies on the combination of Smith and Kobylkin, and asserts that a POSITA would have used Smith’s mobile device “to activat[e] and/or fund[the] disposable payment card” of Kobylkin, in “*the same manner described in Kobylkin.*” Pet., 38 (citing Ex. 1003, ¶¶230-231) (emphasis added). However, Petitioner does nothing to explain how or why a POSITA would activate or fund Kobylkin’s instant disposable payment card (*i.e.*, a physical card) in the context of the online (*i.e.*, card-not-present) transactions claimed in claims 11 and 15. *See* Ex. 1005, Abstract, [0003]. Specifically, claims 11 and 15 claim systems for performing online transactions in which the payment information—specifically the limited-use payment information—is conveyed directly from the claimed “personal computing device” to complete an online, card-not-present, transaction. *See* Ex. 1001, 12:49-13:19, Figs. 5, 10; *see also id.*, 22:10-35 (claim 11 reciting “a display operable to provide a visual user-interface operable for performing online transactions”); *id.*, 23:39-59 (claim 15 reciting “wherein the payment information provided by the computing device is used in online transactions in place of a card issuers payment card information”).

In contrast, Petitioner argues only that a POSITA would have used the personal computing device to activate and/or fund the physical card of Kobylkin. *See* Pet. 38. As described above, however, such activation and/or funding requires only that a user use their mobile device to scan the QR code on the card and request that such card be connected to their existing account. *See supra*, Section III.B; Ex. 1005, [0030]-[0031]. Once activated and/or funded the physical card can then be scanned to transmit separate, card account information encoded on the card to a merchant via the QR code—*i.e.*, in **card-present** transactions. *See* Ex. 1005, [0031]-[0032], [0035]. Thus, Samsung’s asserted combination of Smith and Kobylkin would not be useful at all for online transactions, as required by claims 11 and 15.

Petitioner further relies on the combination of Smith and Gomez, and asserts that a POSITA would have implemented in Smith the user credential check prior to generating a payment cryptogram disclosed in Gomez, as required by claim 15. Pet., 38-39. However, Smith discloses a complete solution built upon a more sophisticated device “such as a cellular phone, smart phone, table [*sic*] computer, etc.” that a POSITA would understand already includes security measures to prevent fraudulent access to the functions of the mobile device, including a “payment application [to] provide security for the functions performed by the mobile device...as disclosed herein.” *See* Ex. 1006, [0033], [0042]. In contrast, the disclosure of Gomez relied upon by Petitioner discloses a far less secure payment

card bearing a “fully static payment card number” printed or embossed onto the card which also leaves behind the “readily observable” payment number—making the disclosed “credential checks” necessary to maintain security. *See* Ex. 1007, 5:13-18; *id.* 5:32-40 (disclosing that the numbers used in a payment transaction are “left behind” and “readily observable”); *id.*, 13:63-65 (“[T]he payment card identification is visible and left behind after a transaction.”).

3. Petitioner Has Not Shown that Smith Or Kobylkin Discloses “Card Issuer Provided Payment Card Information” As Required By Limitation 15(6).

Limitation 15(6) recites “wherein card issuer provided payment card information is wirelessly downloaded into the computing device.” Pet. xii; Ex. 1001, 22:22-26. Claims 16 through 20 depend from claim 15 and therefore include the same limitation. *See* Pet. xiii; Ex. 1001, 23:49-50.

Petitioner asserts that this limitation is met by the “mobile cloud account data” of Smith. Pet. at 59-60 (citing Ex. 1006, [0023], [0031], [0037], [0044], [0050], [0070]-[0071]). But Smith never once states that the “mobile cloud account data” is provided by a card issuer as required by claim 15. To the contrary, Smith is consistent that the mobile cloud account data is generated and provided to a mobile device by a mobile cloud service provider, not the card issuer. *See* Ex. 1006, [0019], [0037], Figs. 4A-4B, 5. Consistent with this disclosure, Smith further discloses that the mobile cloud account data includes only information created or generated by the

service provider and not an issuer—the MCA, the issuer public key certificate, and the ICC public key certificate. *See id.*, [0037], [0083]-[0085], [0089]. Although Petitioner references one passing reference in Smith that “the service provider 110 may be operated by or on behalf of the issuer 112” such reference appears relevant only to the corporate relationship between a service provider entity and an issuer entity, not combining the functions of a service provider and issuer into one entity. *See id.* [0037]. Indeed, it would make little sense to combine the functions of a service provider and issuer into one entity, as a breach would compromise the security of both MCAs and RCAs.

Indeed, Smith consistently discloses that issuer-provided information—the RCA, or “real card account number”—is not stored on the mobile device specifically to “reduc[e] the potential for fraud.” *See* Ex. 1006, [0034]; *see also id.*, Fig. 4A; *id.* [0054] (describing that, in step 412 of Figure 4A, “the issuer 112 may provide real card account information to the MNO [(mobile network operator)] 304 for use in the determination of eligible RCAs”); *id.* [0056] (describing that, in Figure 4A, “[t]he service provider 110 may then, in step 424, request details for the real card account identified by the user from the issuer 112”). Instead, the mobile device uses the MCA in payment transactions. *See id.*, [0034], Fig. 5.

Petitioner also asserts that this limitation is met by the combination of Smith with Kobylkin. *See* Pet., 59-60 (citing Ex. 1005, [0031], [0050], [0070]-[0071]).

However, Petitioner’s cited disclosure does not show that the card account information carried by the QR code of Kobylkin is “downloaded into”—and thus saved on—the mobile device at all, as required by claim 15. *See* Ex. 1001, 23:49-50; *see also id.*, 11:57-12:7, 13:12-22. Instead, Kobylkin merely discloses that the mobile device is used as a transient conduit through which “the card account number [which] is encoded in the QR code [is] transferred to the payment provider over [a] communication link (URL encoded or tone dialing code).” *See* Ex. 1005, [0031]. Moreover, as discussed above, Petitioner fails to show how a POSITA would have combined the two references to meet the limitations of claims 11 and 15. *See supra* Section VI.B.2.

Because Petitioner advances no other arguments about how other references identified in Grounds 2A, 2B, and 2C disclose this limitation or why a POSITA would have modified the device of Smith to wirelessly download “card issuer provided payment card information,” as required in claim 15, Petitioner has not shown a reasonable likelihood of success as to Grounds 2A, 2B, and 2C.

VII. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)

Patent Owner respectfully submits that discretionary denial of institution under Section 314(a) is warranted based on (i) the efficient use of the Board’s time and resources and (ii) consideration of the factors set out in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

A. The Board Should Deny Institution Based on the Efficient Use of the Board’s Time and Resources

The Board should deny institution because the vast majority—if not all—of Petitioner’s multiple challenges fail to meet the “reasonable likelihood” institution standard and, as such, institution would not be an efficient use of the Board’s time and resources.³ *See, e.g., Nanya Tech. Corp. v. Monterey Research, LLC*, IPR2021-00171, Paper 8, 22 (PTAB May 26, 2021) (exercising discretion under Section 314(a) to deny institution where “Petitioner could at best succeed in 8 of 41 challenges, 8 of 20 claims, and 2 of 9 Grounds” and thus “it would not be an efficient use of the Board’s time and resources to institute review”); *Google LLC v. Jawbone Innovations, LLC*, IPR2022-00888, Paper 12, 38-39 (PTAB Nov. 28, 2022) (exercising discretion under Section 314(a) to deny institution where “Petitioner fail[ed] to satisfy the ‘reasonable likelihood’ institution standard for four of the five

³ As discussed above, Patent Owner respectfully submits that Petitioner has failed to show a “reasonable likelihood” of prevailing with respect to any challenged claim under any proposed ground. Therefore, denial is warranted for that reason alone. To the extent that the Board, however, finds some challenges meet the “reasonably likelihood” standard, those are minimal, at best, and denial is still warranted as explained in this section.

challenges and thirteen of the fourteen challenged claims”); *NetScout Sys. Inc. v. Longhorn HD LLC*, IPR2021-01258, Paper 11, 24 (PTAB Feb. 10, 2022) (denying institution where “Petitioner fail[ed] to demonstrate a likelihood of prevailing with respect to its challenges to at least 11 of [the 12] claims.”); *Deeper, UAB v. Vexilar, Inc.*, IPR2018-01310, Paper 7, 43 (PTAB Jan. 24, 2019) (informative) (denying institution because “instituting a trial with respect to all twenty-three [challenged] claims and on all four grounds based on evidence and arguments directed to only two claims and one ground would not be an efficient use of the Board’s time and resources”); *Chevron Oronite Co. v. Infineum USA L.P.*, IPR2018-00923, Paper 9, 11 (PTAB Nov. 7, 2018) (informative) (denying institution where “Petitioner demonstrate[d], at most, a reasonable likelihood of prevailing with respect to two dependent claims out of a total of twenty challenged claims”).

B. The Board Should Deny Institution Under *Fintiv*

The circumstances of the concurrent Related Litigation, *CardWare Inc. v. Samsung Electronics Co., Ltd.*, Case No. 2:22-cv-00141-JRG-RSP (E.D. Tex.), demonstrate that denial is warranted. Specifically, as set forth below, the *Fintiv* factors show that considerations of efficiency, fairness, the merits, and the integrity of the AIA strongly favor denial. *See Fintiv*, IPR2020-00019, Paper 11, 6.

1. Factor 1 is Neutral Because There is No Stay of the Parallel District Court Litigation

Petitioner has moved the district court to stay the Related Litigation pending the resolution of this IPR, which motion was *denied*. Ex. 2003, 1. Even if Petitioner again moves for a stay, this factor is neutral, as any subsequent decision will come after institution, and is “based on a variety of circumstances and facts beyond [the Board’s] control and to which the Board is not privy.” *See Sand Revolution II, LLC v. Continental Intermodal Group – Trucking, LLC*, IPR2019-01393, Paper 24, 7 (PTAB Jun. 16, 2020); *Ericsson Inc. v. Collision Commc’ns, Inc.*, IPR2022-01233, Paper 12, 12 (PTAB Jan. 19, 2023).

2. Factor 2 Favors Denial Because the Board’s Written Decision Deadline Will Come Long After the Trial Date

The district court in the Related Litigation entered its Docket Control Order in October 2022, setting jury selection for trial for February 5, 2024. Ex. 2001, 1. Pursuant to 35 U.S.C. § 316(a)(11), the projected statutory deadline for a Final Written Decision in this proceeding is five months later in July 2024. Accordingly, this factor weighs strongly in favor of denying institution. *See Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC*, IPR2019-01218, Paper 7, 7-10 (PTAB Jan. 7, 2020) (denying institution where jury selection was scheduled for approximately six months before trial in the Board proceeding would conclude); *Next Caller Inc. v. TrustID, Inc.*, IPR2019-00961, Paper 10, 8-16 (PTAB Oct. 16, 2019) (denying

institution where trial was scheduled to conclude “several months before a final decision would be due”); *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15, 8 (PTAB May 15, 2020) (“Because the trial date is substantially earlier than the projected statutory deadline for the Board’s final decision, this factor weighs in favor of discretionary denial.”).

Petitioner largely ignores the actual trial date and relies instead on median time-to-trial statistics generally for the period from July 1, 2021 to June 30, 2022 for EDTX civil trials. Pet. 71-72. Such arguments fail for at least three reasons. First, while the Board considers the median time if before it, it is not required only to consider the median time or disregard the *actual* trial date of February 5, 2024. Ex. 1101 (Director’s Interim Procedure), 8-9. Second, Petitioner cites *no* evidence that Judge Gilstrap will not be able to meet the currently scheduled trial date, further demonstrating that the actual trial date should be the key consideration here. Third, and perhaps most importantly, if median time-to-trial is used, the more appropriate and accurate metric is to use the presiding judge’s median time-to-trial for patent cases: Judge Gilstrap’s median time-to-trial for jury trials for patents cases filed since January 1, 2019 is 19.4 months, which is even faster than the current trial date. Ex. 2002, 1.

Factor 2 thus weighs in favor of denial.

3. Factor 3 Favors Denial Because of the Parties' Significant Investment in the Parallel Proceeding by the Time of Institution, Including for Invalidity

The parties have already served Infringement and Invalidity Contentions, and by the time of the institution decision, document production will be substantially complete and the claim-construction process well be underway and completed shortly thereafter. Ex. 2001, 3-4. These substantial investments—including for invalidity—weigh in favor of discretionary denial. *See Sand Revolution*, IPR2019-01393, Paper 24, 10 (noting that investment in invalidity contentions is relevant to this factor).

Factor 3 weighs in favor of denial.

4. Factor 4 Favors Denial Because the District Court Litigation Involves the Same Claims and the Same Arguments and Petitioner has Only Stipulated to Very Narrow Estoppel

Petitioner offers only an extremely narrow stipulation to assert this factor favors institution. Pet. 72-73 (“Should IPR be instituted based on this Petition, Petitioner stipulates that it will not pursue in the Related Litigation any invalidity grounds against the Challenged Claims of the [challenged] patent that are the same as those raised in this Petition.”). Petitioner is wrong.

With this stipulation, the likelihood of inefficiency and conflicting decisions is particularly significant because of the potential overlap of issues and because, with trial beginning February 5, 2024, the Related Litigation will have reached a final

jury verdict on validity months before the statutory deadline for a Final Written Decision. Ex. 2001, 1. Indeed, Petitioner stipulated only not to pursue the *very same grounds*. This leaves open the possibility of Petitioner using the *same* art and arguments in the Related Litigation, buttressed only by an additional prior art reference, for example—which effectively nullifies the import of the stipulation.⁴

Thus, as here, “if the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favor[s] denial.” *Fintiv*, IPR2020-00019, Paper 11, 12. As the Board noted in *Fintiv*, when both the district court and the Board will consider the same (or substantially the same) prior art and arguments, “concerns of inefficiency and the possibility of conflicting decisions [are] particularly strong.” *Id.*

⁴ Petitioner could have—but chose not to—offer a full-scope estoppel stipulation as the petitioner did in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12, 18-19 (PTAB Dec. 1, 2020) (precedential). Moreover, in proceedings on related patents, Petitioner requested leave to file a broader stipulation in view of recent faster time to trial metrics in the Eastern District of Texas. *Samsung Electronics Co., Ltd. v. CardWare Inc.*, IPR2023-00196 (Paper 7), -00210 (Paper 9), -00211 (Paper 9), and -00219 (Paper 7) (Apr. 18, 2023). Petitioner has not filed anything in this proceeding.

Factor 4 favors discretionary denial.

5. Factor 5 Favors Denial Because the Parallel District Court Litigation and the Petition Involve the Same Parties

As noted, the pending parallel Related Litigation involves the same parties and the same challenged patent. Pet. 74. Petitioner fails to address Factor 5 at all. *See* Pet. 72-73 (skipping from Factor 4 to Factor 6). In actual fact, this factor weighs in favor of discretionary denial. *Ericsson*, IPR2022-01233, Paper 12, 16.

6. Factor 6 Favors Denial Because The Merits Are Weak

As shown above, the Petition lacks strength on the merits. *See supra* Section VI. Factor 6 thus favors denial.

Considering all factors together—five favoring denial and one being neutral—the Petition should be denied in the Director’s discretion under 35 U.S.C. § 314(a). *See, e.g., Ericsson*, IPR2022-01233, Paper 12, 18 (denying institution where “only factor 4 weighs against discretionary denial, factor 1 is neutral, and factors 2, 3, 5, and 6 weigh in favor discretionary denial”).

VIII. CONCLUSION

As discussed above, Petitioner’s combinations fail to disclose key limitations of each Challenged Claim of the ’820 Patent and are otherwise unworkable; therefore, the asserted Grounds do not render obvious any claims. Moreover, the same issues will be addressed in the District Court before the Board can issue a Final Written Decision. The Board should, therefore, deny the Petition.

Dated: April 20, 2023

Respectfully submitted,

SHEARMAN & STERLING LLP

/s/ Yue (Joy) Wang

Yue (Joy) Wang (72,578)

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 10,205 words, excluding the parts of the paper exempted by 37 C.F.R. §42.24(a).

Dated: April 20, 2023

Respectfully submitted,

SHEARMAN & STERLING LLP

/s/ Yue (Joy) Wang

Yue (Joy) Wang (72,578)

CERTIFICATE OF SERVICE

I hereby certify that the foregoing Patent Owner's Preliminary Response and Exhibits listed on the List of Exhibits were served on April 20, 2023, via electronic mail upon counsel of record for Petitioner at the following email addresses:

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Nicholas Stephens, Reg. No. 74,320
Daniel D. Smith, Reg. No. 71,278
IPR39843-0144IP1@fr.com
PTABInbound@fr.com
axf-ptab@fr.com
jjm@fr.com
nstephens@fr.com and
dsmith@fr.com

SHEARMAN & STERLING LLP

/s/ Matt Berkowitz

Matt Berkowitz