

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

CARDWARE INC.,
Patent Owner

Case No. IPR2025-01151
U.S. Patent No. 11,328,286

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	Page
I. INTRODUCTION.....	1
II. THE '286 PATENT CLAIMS	4
III. PETITIONER’S ALLEGED PRIOR ART	6
A. Collinge	7
B. Bona.....	9
C. Smith	10
D. Petitioner’s Proposed Combinations for the Challenged Independent Claims.....	13
IV. CLAIM CONSTRUCTION	14
A. The District Court in the Parallel Proceeding has Rejected Petitioner’s Printed Matter Doctrine Argument.....	14
B. Device Account Number	14
C. Petitioner Omits its Contradictory District-Court Indefiniteness Arguments that the Claim-Scope Allegedly Cannot be Ascertained.....	15
V. LEVEL OF ORDINARY SKILL IN THE ART	17
VI. ARGUMENT	17
A. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination Has A “Device Account Number” of Limitations 1(d)(1), 20(c), and 20(f)	17
B. Petitioner and its Expert Fail to Show a Motivation to Combine and Explain Why A POSITA Would Combine the PPAN of Smith With the Remote-SE System of Collinge.....	27
C. Petitioner Fails to Demonstrate that a Person of Ordinary Skill in the Art would Use the Secure Card Device of Bona with the Secure Element-Free Mobile Device of Collinge	30
VII. CONCLUSION	38

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Microchip Tech. Inc. v. Aptiv Tech. AG</i> , IPR2024-00558, Paper 12, 10-12 (PTAB Oct. 7, 2024)	16
---	----

Regulations

37 C.F.R. §11.18	16
37 C.F.R. §42.11	16
37 C.F.R. §42.12(b)	16

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 available at https://www.uspto.gov/patents/ptab/interim-director-discretionary-process
2003	Agreed Scheduling Order in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv00446-ADA (W.D. Tex. May 20, 2025)
2004	Standing Order Governing Proceedings (OGP)—Patent Cases for cases before Judge Albright (dated Mar. 5, 2025)
2005	DocketNavigator Time to Trial Statistics for Patent Cases before Judge Albright
2006	Judges’ Directory and Biographies for the U.S. District Court for the Western District of Texas, available at https://www.txwd.uscourts.gov/judges-information/judges-directorybiographies/
2007	Complaint in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Nov. 4, 2024)
2008	First Agreed Scheduling Order in <i>CardWare Inc. v. Google LLC</i> , No. 7:24cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2009	Complaint in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2010	Invalidity Contentions Cover Pleading in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Apr. 7, 2025)
2011	Defendants’ Notice of Subpoena to Apple, Inc. in <i>CardWare Inc. v. Samsung Elecs. Co., Ltd.</i> , No. 2:22-cv-00141-JRG-RSP (E.D. Tex. Dec. 9, 2022)
2012	Apple Inc.’s Response and Objections to Defendants’ Subpoena in <i>CardWare Inc. v. Samsung Elecs. Co., Ltd.</i> , No. 2:22-cv-00141-JRG-RSP (E.D. Tex. Dec. 23, 2022)
2013	Letter from CardWare, Inc. to Apple Inc. dated October 10, 2023 “RE: Patent Portfolio of CardWare Inc.”

No.	Exhibit Description
2014	Proof of Delivery to Apple Inc. dated October 11, 2023, for Letter from CardWare, Inc. to Apple Inc. dated October 10, 2023 “RE: Patent Portfolio of CardWare Inc.”
2015	DocketNavigator Time to Trial Statistics for Patent Cases in the Western District of Texas
2016	Apple’s Opening Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. May 27, 2025)
2017	CardWare’s Responsive Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. June 17, 2025)
2018	Apple’s Reply Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. July 1, 2025)
2019	CardWare’s Sur-Reply Claim Construction Brief in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. July 17, 2025)
2020	Joint Claim Construction Statement in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. July 18, 2025)
2021	Comparison Chart for References Relied Upon in Apple’s Invalidity Contentions in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex.)
2022	Excerpts from Defendant Google LLC’s Invalidity Contentions in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Apr. 3, 2025)
2023	Claim Construction Order in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv00446-ADA (W.D. Tex. Aug. 29, 2025)
[New] 2024	DECISION Denying Institution of <i>Inter Partes</i> Review in <i>Samsung Elecs. Co., Ltd. v. CardWare, Inc.</i> , IPR2023-00210, Paper 13 (PTAB June 13, 2023)

I. INTRODUCTION

On June 20, 2025, Apple Inc. (“Apple” or “Petitioner”) filed a Petition requesting *inter partes review* of claims 1-27 (“Challenged Claims”) of U.S. Patent No. 11,176,286 (“the ’286 Patent”) (EX1001), entirely on obviousness grounds. Paper 1 (“Petition” or “Pet.”). On July 10, 2025, the Board issued a Notice of Filing Date Accorded for the Petition and set the time for filing Patent Owner’s preliminary response. Paper 3.

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.

First, each of claims 1-14 and 20-26 require some form of a “device account number.” Petitioner addresses these in Grounds 2-5 and 8-10 and in each case, relies on a “PayPass” Primary Account Number of (“PPAN”) in a reference to Smith to meet this limitation. But the PPAN of Smith is not a device account number—it has no connection or association to a particular device. Rather, like the actual account number, and the “temporary” account number that Smith focuses on, the PPAN is mapped to a customer ID, as shown in Figure 6 of the reference (where the PPAN and “mobile PAN” are defined to be the same).

Second, Petitioner fails to explain why a POSITA would have combined Collinge with Smith (again, as is relevant to each of Grounds 2-5 and 8-10). Petitioner asserts that a POSITA would have used the PPAN of Smith as a more secure version of a PAN and used that with Collinge's cryptogram approach. But there is no evidence that the PPAN is more secure. Smith does not say that, and Petitioner and its expert simply assume that fact. It does, however, have limitations because it is a MasterCard specific standard, per Smith, and therefore would limit issuer-flexibility. Collinge and Smith are also incompatible references addressing very different problems. Collinge is specifically focused on cryptogram-based payments using mobile devices that lack secure elements. Smith, on the other hand, is designed for use in devices that *have* a secure element, and is focused on a temporary PAN during the brief period when an issuer is setting up an actual account. It barely even discusses a PPAN or its functionality.

Third, Petitioner fails to explain why a POSITA would have combined Collinge and Bona, which is the base combination underlying *all* Grounds. Claim 15 (Ground 1) is representative on this issue and requires "a payment system comprising: a *payment card device*" that is "free of any fixed payment numbers" and "is operable for use in a merchant card-reader equipment" as well as a "personal computing device" which completes the transaction. EX1001, 21:52-53, 21:48-51. Petitioner relies primarily on Bona's smart card and Collinge's mobile device to

meet these limitations, Pet., 20-25, and asserts that a POSITA would have used Bona's "payment card device free of any fixed payment numbers ... with Collinge's NFC-enabled computing device." Pet., 23. Petitioner further argues that given the prevalence of mag-stripe-only terminals, a POSITA would have been motivated to "transmit the necessary transaction information to Bona's companion card for use in a magnetic stripe transaction using NFC communications." Pet., 25. Even if this is correct, it would not meet the rest of the limitations of claim 15, which require that a "merchant is operable to receive a payment information provided by a personal computing device," (limitation 15(e)) not a smart card like that in Bona. In order to show that limitation 15(e) is met, Petitioner flips the combination (relative to limitation 15(a)) and suggests that Collinge's mobile payment application transmits the payment cryptogram to the merchant (whereas in connection with limitation 15(a), Petitioner argued that a POSITA would have used Bona and the mag-stripe functionalities to make the payment). These two arguments are inconsistent with each other. Pet., 37.

Petitioner also fails to explain why a system using the cryptogram and device of Collinge would transmit the cryptogram to the card of Bona or why the combination would be flipped vis-à-vis 15(a) and 15(e). Aside from this, Petitioner does not ever explain how a POSITA would have fit the cryptogram of Collinge into

the mag-stripe data of Bona, given that mag-stripe data conforms to a pre-determined standardized approach.

The Board should therefore decline to institute the proceeding.

II. THE '286 PATENT CLAIMS

When David Wyatt conceived of the invention claimed in the '286 Patent over a decade ago, there were “several different types of credit cards available in the marketplace.” EX1001, 1:39-40.

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.

EX1001, 1:39-41.

The claims of the '286 Patent generally relate to systems and methods for reducing fraud during payment transactions through the use of a novel payment system. Independent claim 1, which has similar limitations to independent claims 15 and 20—collectively, the three challenged independent claims—is illustrative and is

directed to a payment system comprising a physical card device and a computing device that may perform a payment transaction via an interface of the electronic device. EX1001, 19:50-20:16 (claim 1). The processor of the computing device is operable to store a transaction sequence count, a device account number, and secrets that are limited to the computing device. EX1001, 19:61-64. The electronic device can also receive, store, and transmit payment information that is not visible on the payment card and generate a limited use card payment information for an authenticated card user. EX1001, 19:61-20:3. The electronic device is designed to convey the limited-use card payment information which may be rejected as invalid by a card issuer authority when the limited use card payment information is used outside of its “limitations of use” in a transaction. EX1001, 20:4-10. The card issuer authority may reject a transaction as invalid if the transaction attempt is outside of the limited use number’s limitations of use. EX1001, 20:9. The card issuer authority may also validate card payment information as “authentic” when it is received from an authenticated users’ payment card or an authenticated users computing device. EX1001, 20:11-15. If the transaction is “authentic,” then the card issuer authority may complete the transaction. EX1001, 20:15-16.

The various cryptographic techniques of the '286 Patent drastically improve security vis-à-vis prior art while maintaining convenience and flexibility by allowing selection and use of different payment accounts.

III. PETITIONER’S ALLEGED PRIOR ART

Petitioner relies upon ten references in its Grounds (Collinge, Bona, Smith, Patterson, Lin, Kranzley, Eng, Chin, Fisher, and Hammad). In Ground 1, Petitioner presents the combination of Collinge and Bona to challenge independent claim 15 and dependent claims 17-18. In Ground 2, Petitioner adds a third reference to the combination (Smith) to challenge independent claims 1 and 20 and dependent claims 5, 8, 11, 14, and 21-27. In Ground 3, Petitioner adds a fourth reference (Patterson) to challenge dependent claims 2-4. In Ground 4, Petitioner adds a reference (Lin) to the combination of Ground 1 to challenge dependent claim 9. In Ground 5, Petitioner adds a fourth reference (Kranzley) to challenge dependent claim 10. In Ground 6, Petitioner puts forth the combination of Collinge, Bona, and Kranzley to challenge dependent claim 16. In Ground 7, Petitioner puts forth the combination of Collinge, Bona, and Eng to challenge dependent claim 19. In Ground 8, Petitioner puts forth the combination of Collinge, Bona, Smith, and Chin to challenge dependent claims 12 and 13. In Ground 9, Petitioner puts forth the combination of Collinge, Bona, Smith, and Fisher to challenge dependent claim 7. In Ground 10, Petitioner puts forth the combination of Collinge, Bona, Smith, and Hammad to challenge dependent claim 6.

Patent Owner provides an overview of the references relevant to this POPR. Patent Owner then explains in the following sections how Petitioner’s Grounds using

these references fail to demonstrate a reasonable likelihood of success than any Challenged Claim is obvious.

A. Collinge

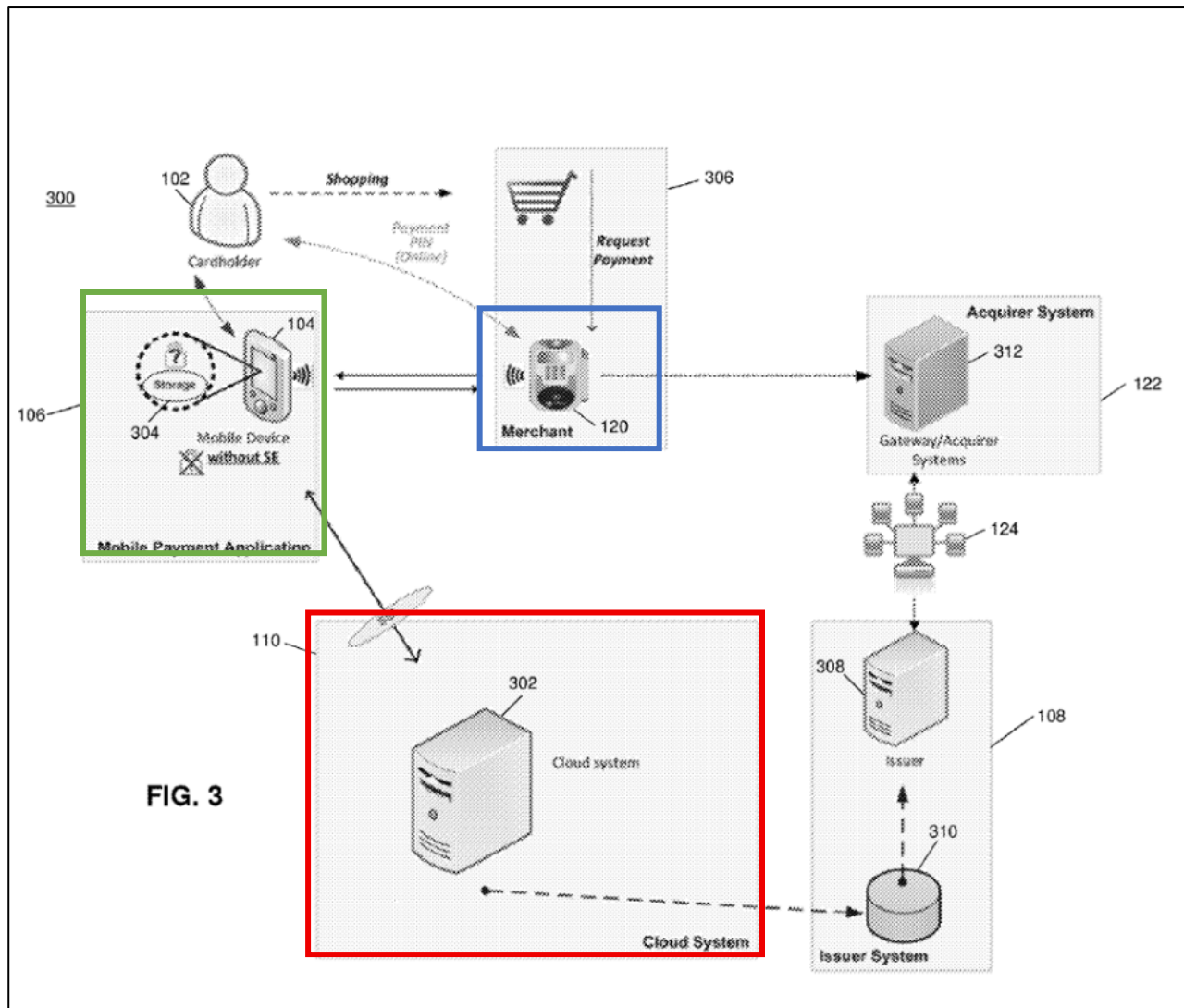
U.S. Patent App. Pub. No. 2013/0262317 (“Collinge”) is directed to techniques for “generating and provisioning payment credentials to a mobile device lacking a secure element.” EX1004, Abstract. Collinge explains that the system relies on two computing devices to perform its methods. EX1004, [0007], FIGs. 1-4, 6, 7. Collinge explains that such a two-computer system is necessary because “not all mobile devices have secure elements.” EX1004, [0004]. “As a result, a consumer who has a NFC-capable mobile device may not be able to use their device to conduct payment transactions if their mobile device lacks a secure element.” EX1004, [0004]. Therefore, per Collinge, “there is a need for a technical solution to enable a mobile device lacking a secure element to conduct contactless payment transactions.” EX1004, [0005].

Collinge seeks to solve this problem by creating a provisioning system comprising a **first computing device (e.g., a mobile phone)** that does not contain a secure element, and therefore is not suitable for long-term storage of the payment credentials. During the transaction, the payment credentials are transmitted to the mobile device from a **second device, a remote device**, that comprises a secure element (SE). EX1004, [0068]. The mobile device then uses the key and card profile

data provided by the remote-SE system to generate a cryptogram. EX1004, [0069].

Then, the mobile device “transmit[s] the generated cryptogram and payment credentials to a point-of sale terminal” to complete the transaction. EX1004, [0070].

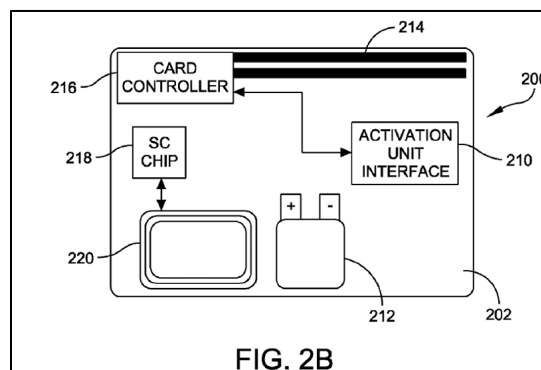
Based on the validation of both the cryptogram and the payment credentials, the transaction is authorized. EX1004, [0070], FIG. 3.



EX1004, FIG. 3.

B. Bona

U.S. Patent App. Pub. No. 2011/0140841 (“Bona”) is directed to a smart card usable in magnetic stripe swipe transactions. EX1009, Abstract. The smart card comprises a display, a magnetic strip emulator made with electromagnetically inducible material, a card controller that “controls all aspects of the functionality of the card” which is “a separate processor from the smart card chip.” EX1009, [0050]-[0052]. The card controller controls the magnetic strip emulator, such that the emulator can be used in a magnetic strip reader and still provide both static transaction data as well as “dynamic information” (e.g. CVC3) which “prevents fraudulent transactions.” EX1009, [0053]. During a transaction, the emulator, through a set of transducers, varies the magnetic fields at positions that align with a read sensor of existing reader terminals. EX1009, [0049]-[0051]. The card controller supplies the CVC3 and account information to the emulator, which, through the transducers, sends that information to the merchant in a credit card swipe transaction. EX1009, [0053], FIG. 2B.

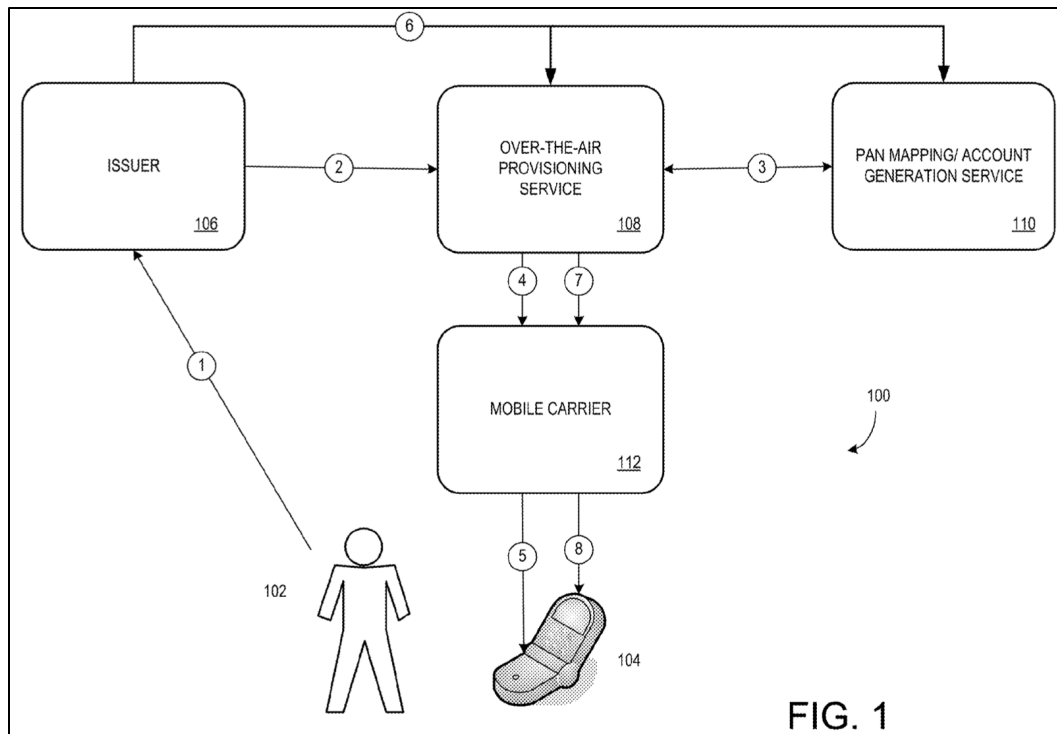


EX1009, FIG. 2B.

C. Smith

U.S. Patent App. Pub. No. 2010/0125508 (“Smith”) is directed to methods for automatically assigning a “temporary payment account number (‘PAN’)” to a consumer’s request for a new payment account, which “allow[s] the account holder to access the account during a time period in which the issuer systems are updated to include the actual payment account number (or ‘actual PAN’).” EX1010, [0012]; EX1010, Abstract.

As Smith explains, when a consumer uses a payment application on their mobile device to activate a payment account, “there may be a delay between [the] request...and the time at which an issuer can establish an actual account in response to that request,” which delay “may be frustrating to a consumer who want to use his or her mobile device to complete a purchase transaction.” EX1010, [0002]. It is therefore “desirable to allow consumers to activate such a payment application on a consumer’s mobile phone and then instantly, that is to say within a relatively brief period of time, use the mobile phone in a payment transaction.” EX1010, [0003].



EX1010, FIG. 1.

Smith explains, in reference to Figure 1 above, the following transactions involved in its method for issuing a payment account over a mobile network:

1. Transaction 1: A customer 102 enters account registration data and requests an issuer 106 issue a payment account using their mobile device 104.
2. Transaction 2: The issuer 106 assigns a temporary PAN to the customer's account registration data and transmits the temporary PAN to an over-the-air ("OTA") provisioning service 108 with a request to install a payment application and account information on the customer's mobile device 104.
3. Transaction 3: The OTA provisioning service 108 forwards the temporary PAN to a PAN mapping service 110, which assigns a PayPass PAN ("PPAN") to the payment application destined for the

mobile device 104 and maps the PPAN to the temporary PAN. The PAN mapping service sends the PPAN back to the OTA provisioning service 108.

4. Transaction 4: The OTA provisioning service 108 delivers a software package with a payment application and the PPAN to the mobile carrier 112 network associated with the mobile device 104.
5. Transaction 5: The mobile carrier 112 pushes the software package to the mobile device 104, during which process the customer 102 enters a verification code to confirm their identity and authorize installation of the software package.
6. Transactions 6 to 8: Once the issuer 106 issues an actual PAN for the account of the customer 102, it sends a request message to the PAN mapping service 110 to replace the temporary PAN with the actual PAN in its mapping database.

EX1010, [0013]-[0019]; *see also* EX1010, FIGs. 3 & 4, [0025]-[0032].

Smith further explains that the primary account number database 600 of Figure 6 below has “entries associated with consumers how [*sic*] have requested to use a mobile device to complete purchase transactions.” EX1010, [0039].

600				
CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE
FIG. 6				

EX1010, FIG. 6.

D. Petitioner's Proposed Combinations for the Challenged Independent Claims

Petitioner's proposed obviousness combinations for Grounds 1 and 2 are based on a combination of Collinge and Bona (Ground 1) and Collinge, Bona, and Smith (Ground 2). The rest of Petitioner's Grounds rely on additional references added to these combinations (*e.g.*, Collinge, Bona, Smith, and Patterson (Ground 3)). As best that Patent Owner can discern, Petitioner proposes that Collinge is the base reference, including its remote provisioning system and a mobile device lacking a secure element. Petitioner then proposes that a POSITA "would have been motivated to use Bona's payment card device free of any fixed payment numbers visible thereon and operable for use in payment card reader equipment with Collinge's NFC-enabled computing device (*i.e.*, cell phone) and payment system." Pet., 23. From there, Petitioner then proposes to that it would have been obvious to

use “Smith’s PPAN in place of Collinge’s PAN so that Collinge’s mobile device would not be required to store the PAN, which is a sensitive financial number,” in the Collinge-Bona combination. Pet., 53.

IV. CLAIM CONSTRUCTION

A. The District Court in the Parallel Proceeding has Rejected Petitioner’s Printed Matter Doctrine Argument

Petitioner asserts that certain claim terms are subject to the printed matter doctrine. Patent Owner disagrees, but for the purposes of this POPR, it is of no moment. Patent Owner notes that the district court, in the parallel proceeding involving Patent Owner and Petitioner, rejected Petitioner’s argument and specifically found that the disputed terms in that case were “[n]ot subject to the printed matter doctrine.” EX2023, 3.

B. Device Account Number

Independent claim 1 requires a “device account number” while independent claim 20 requires a “static device account number.” The “device account” number is each of a “device number” and an “account number”; the applicant simply put both of those descriptors together in one and referred to it as a “device account number.” A “static device account number” is also a “static number” since it is modified by all three descriptors.

The Board has already effectively determined as much in connection with IPR2023-00210, which involved a related patent with a common inventive

disclosure, U.S. Patent No. 10,339,520, claiming priority to the same original provisional application (61/794,891). In that proceeding, the Board denied institution on the merits because it determined that Petitioner (Samsung) failed to demonstrate that any of its references disclosed a “static device account number.” EX2024 (IPR2023-00210, Paper 13), 9. The Board held that “the ’520 Patent does not support construing ‘a static device account number’ as encompassing a number that is dynamically generated and valid for only a finite number of transactions or a specified period of time, such as two minutes, ten minutes, or three hours.” EX2024, 14.

The Board did not specifically address the words “device” or “account,” but it did determine that “static” modifies “number” and that Petitioner needed to show that the prior art disclosed such a “static” number. EX2024, 8. The same logic should apply to the words “device” and “account.” Just like a “static device account number” must be a “static number,” it also must be a “device” number and an “account” number.

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

In its IPR petition, Petitioner purports to apply “the plain and ordinary meaning of *all* claim terms as understood by a POSITA.” Pet., 5-6 (emphasis added). Its expert also purports to apply the plain and ordinary meaning. EX1003 ¶25.

Importantly, however, Petitioner omits that—in district court using a different expert—Petitioner asserted that claims 1-18 are indefinite because a POSITA allegedly could not determine the scope of the limitation in independent claims 1 and 15 based on the phrase “its valid limitations of use”. EX2016, 29-31; EX2018, 16-17; EX2020, 3. The district court has now rejected Petitioner’s arguments (*see* EX2023, 3), but regardless, Petitioner’s positions are inconsistent and it will surely insist on preserving its indefiniteness positions for appeal (and it has not waived its right to do so).

Patent Owner respectfully submits that Petitioner should not be able to assert, on the one hand, that the claimed scope cannot be ascertained and the claims are indefinite in district court, and on the other hand, tell the Board that they are amenable to an obviousness challenge.

Petitioner’s failure to inform the Board about these material facts should be reason to deny the Petition as it believes that the claims cannot actually be construed. Indeed, Petitioner is taking different positions concerning the claims as the need suits, and did not inform the Board. *See* 37 C.F.R. §11.18; (b)(1) (prohibiting “conceal[ment]” of material facts); 37 C.F.R. §42.11; 37 C.F.R. §42.12(b) (identifying available sanctions); *see also Microchip Tech. Inc. v. Aptiv Techs. AG*, IPR2024-00558, Paper 12, 10-12 (PTAB Oct. 7, 2024) (denying institution where Petitioner argued for indefiniteness in district court and refusing to “adopt the claim

construction upon which the Petition relies because it is not persuasively argued or adequately supported by either party.”).

V. LEVEL OF ORDINARY SKILL IN THE ART

For purposes of this Preliminary Response, Patent Owner does not challenge Petitioner’s level of ordinary skill in the art.

VI. ARGUMENT

A. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination Has A “Device Account Number” of Limitations 1(d)(1), 20(c), and 20(f)

Grounds 2-5 and 8-10 in the Petition fail because Petitioner fails to show that its proposed obviousness combinations include a “device account number” as required by the following limitations in independent claims 1 and 20 of the ’286 Patent:

1. 1(d)(1), requiring “wherein the processor is operable to store a transaction sequence count, a *device account number* and secrets limited to the computing device, and,”
2. 20(c), requiring “wherein the memory is operable to store a transaction sequence count, a *static device account number* and secrets limited to the computing device;”
3. 20(f), requiring “wherein the processor is operable to dynamically generate at least a portion of a limited-use payment information for use by an authenticated card user, and to combine said at least a portion of the limited-use payment information with at least said *static device account number* to create combined payment information;”

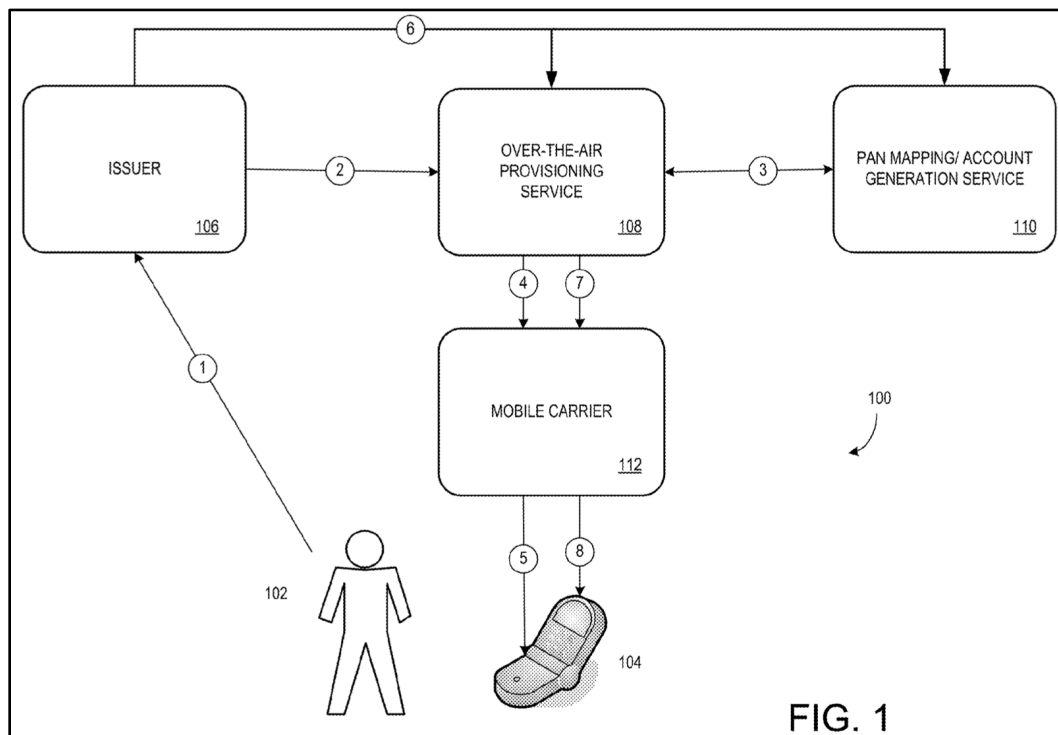
EX1001, 19:61-64, 22:61-63, 23:1-6 (emphases added) (collectively, “Device Account Number Limitations”).

Petitioner relies solely on Smith as allegedly disclosing the claimed “device account number.” Pet., 50-53, 71-73. In particular, Petitioner asserts that because the PPAN is “assigned to the mobile device” and “stored in the mobile device,” that it is a “device account number” (or “static device account number” in the context of claim 20). *See* Pet., 51 (“The PPAN (device account number) is . . . ‘stored in the mobile device 204.’” (emphasis in original)). Petitioner’s assertion is incorrect. Smith never once says that the PPAN is a “device account number” or is limited to (or even based on) a particular device in any way. Rather, the PPAN is account-based and, per Smith’s explicit language, can be mapped to multiple devices and used independently of whether a device is enabled or disabled for payment transactions. EX1010, [0029], [0041]. In sum, as explained further below, there is no indication anywhere in Smith that the PPAN is tied to a device identifier, or is limited in use to a particular device.

* * * *

As set out above in Section III(C), Smith is directed a temporary account number (temporary “PAN”) that a customer can use during the delay between “a request from a consumer to activate a payment account in connection with a mobile device and the time at which an issuer can establish an actual account in response to

that request.” EX1010, [0002]. The Smith invention allows an account holder to “access the account during a time period in which the issuer systems are updated to include the actual payment account number (or ‘actual PAN’).” EX1010, [0012]. Once the issuer systems have updated, the actual PAN is used instead of the temporary one. EX1010, [0012].



EX1010, FIG. 1.

Figure 1 (above) outlines a PAN and temporary PAN provisioning system. The process starts (transaction “1”) when a customer contacts an issuer 106 “via one or more web sites or by contacting a customer service representative.” EX1010, [0014]. The customer is then taken through a registration process in which the customer selects a verification code that will be used in a mobile device 104

personalization process. EX1010, [0014]. Importantly, there is no disclosure that the user ever provides a device ID during this registration process. Indeed, the user does not even need to register the device they are using to carry out the registration; the user can simply visit a website or call a customer representative (presumably from any device). *See* EX1010, [0014], [0028]. The user receives a verification code that allows for personalization on the device, but the disclosure suggests this is device agnostic—it could be any device, or multiple devices. *See* EX1010, [0014], [0028]. But either way, the issuer is blind to the device information during this registration step.

In the next step (transaction “2”), the issuer transmits data elements to an OTA provisioning service. These can include a request to “provision a new account with the temporary PAN” and “risk data elements,” such as a spending limit. EX1010, [0015]. Smith does not indicate that any “device” based information is transmitted; it is all account based. Petitioner focuses on transaction “3,” where the OTA provisioning service forwards a message “to a PAN mapping/account generation service 110 so that a PayPass PAN (or ‘PPAN’) may be assigned to the mobile device 104.” EX1010, [0016]; Pet., 51. “The PAN mapping/account generation service 110 assigns a PPAN to the device 104, and also maps the newly-assigned PPAN to the temporary PAN provided by the issuer 106.” EX1010, [0016]. These two sentences in Smith effectively constitute the entirety of Petitioner’s argument

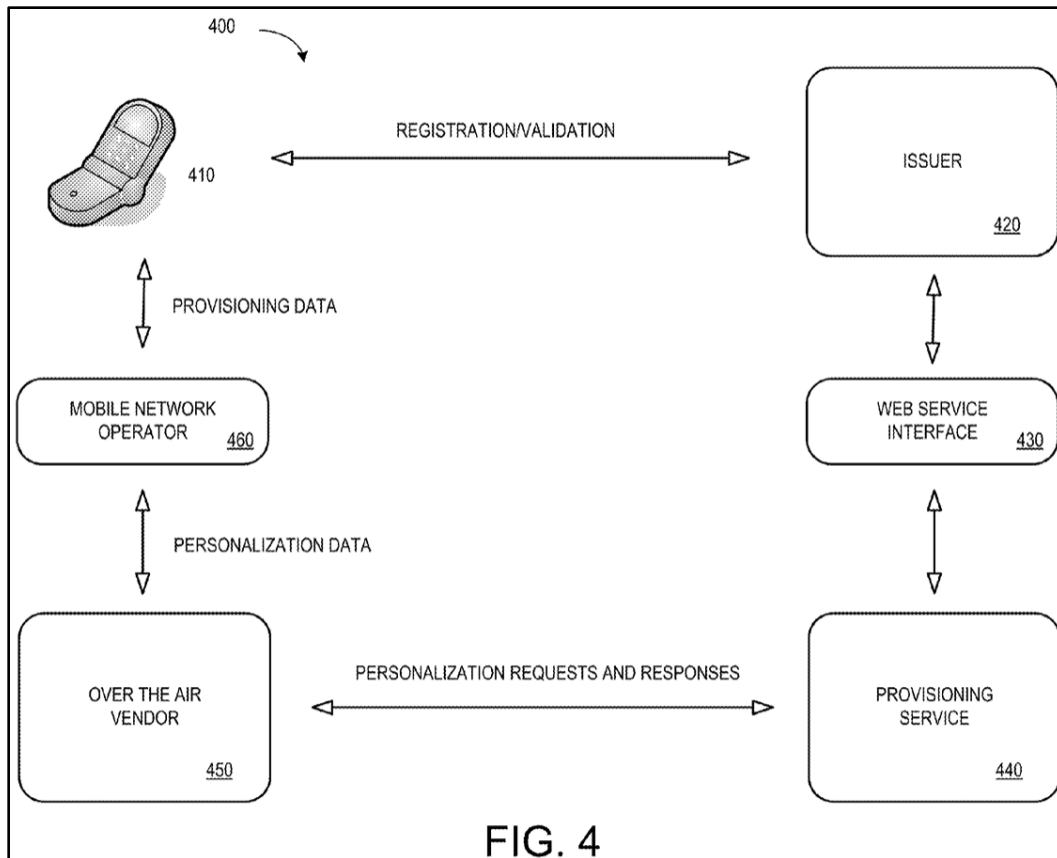
that the PPAN is a “device account number.” Pet., 50-53. Petitioner misinterprets Smith’s disclosure and, notably, omits any contextual explanation of this paragraph or Smith’s actual invention in its discussion of the Device Account Number Limitations.

Smith explains that upon receipt of the request (transaction “2”) to provision (or install) the payment application and account information in the customer’s mobile device, “the OTA provisioning service 108 begins creating a software package or applet for delivery to the customer’s mobile device. 104.” EX1010, [0016]. Once the mapping has been established (i.e., the PPAN to temporary PAN), the “newly assigned PPAN is returned to the OTA provisioning service 108 for inclusion in the software package to be installed on the mobile device 104.” EX1010, [0016]. Smith explains that the “software package may contain the software code required to install the PPAN, the risk parameters (if any), and other application information in the mobile device.” EX1010, [0017]. In other words, the provisioning of the PPAN to a mobile device is based upon the need to include that PPAN in the software package instance that is going to be provisioned; it is tied to the software and account, and not any device-identifying information.

In connection with transactions “4” and “5,” the customer enters a verification code “to confirm the customer’s identity and to authorize the installation of the software.” EX1010, [0018]. Again, the verification code may be entered in a device,

but it is to confirm the “customer’s identity,” and not a device identity. Smith’s approach is device agnostic.

Once the identity of the customer is established, the personalization process is initiated. EX1010, [0018]. This is described in further detail with respect to Figure 4 of Smith (below) and related disclosure. EX1010, FIG. 4, [0028]-[0029]. In order to initiate that process, the consumer can access a website and input personal information, a “model number” of the mobile telephone, or a phone number—notably, there is no discussion of inputting a Device ID. EX1010, [0028]. As part of the personalization process, the provisioning service may “obtain or create a PPAN and add it to a PAN mapping database.” EX1010, [0029]. Importantly, Smith indicates that “multiple NFC-enabled handsets may be managed for a single account.” EX1010, [0029]. In other words, Smith indicates that none of a PPAN, the temporary PAN or the actual PAN is device specific. They are each available for use on multiple devices.



EX1010, FIG. 4.

After personalization and after the issuer has updated their systems, the issuer provides a message to the mapping/account generation service 110 to update the database with the actual PAN, replacing the temporary PAN. EX1010, [0019]. This is transaction “6.” In all of Smith’s examples, this actual PAN, as well as the temporary PAN and the PPAN are mapped to the customer account (and the actual PAN is mapped to the PPAN). They are not mapped to a device identifier or a specific device. Figure 6, copied below, illustrates this. It is an example of a “database 600 that may be used in connection with the payment account apparatus 500.” EX1010, [0038].

600				
CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE
FIG. 6				

EX1010, FIG. 6.

As can be seen from Figure 6, there is no “Device ID” or any specific device identified. EX1010, FIG. 6. Rather, a “Consumer ID” is mapped to various account numbers, including a temporary PAN, a Mobile PAN, and an Actual PAN. EX1010, FIG. 6. *see also* EX1010, [0039]. The PPAN is a type of Mobile PAN. EX1010, [0026]. Smith explains that “[t]he consumer identifier 602 might be [a] code that uniquely identifies a consumer who has requested that his or her mobile device be enabled to complete purchase transactions.” EX1010, [0040]. Again, this is a mapping to a Consumer ID, irrespective of which device(s) that consumer wants to enable.

The other disclosures in Smith all indicate that the PPAN is linked to an actual PAN or a temporary PAN at any given time, and that these PANs are account

numbers, not device numbers. EX1010, [0013] (“a primary *account* number (or ‘PAN’)), EX1010, [0023] (“the payment network 218 ***identifies the PPAN and requests a look up of the related PAN;***” and “where the issuer 206 has not yet issued an actual PAN, the look up will return the ***temporary PAN associated with the PPAN.***”) (emphasis added).

Smith further describes that a “PayPass *account*” is a type of “payment *account*”; indeed, “PPAN” literally stands for PayPass Primary *Account* Number. EX1010, [0012] (“In some embodiments, features of the present invention allow a payment account issuing financial institution (an ‘issuer’) to effect instant issuance of a payment *account* (such as a *PayPass account*) over a mobile network to a mobile device without the need to set up the payment account within the issuer systems at the time of issuance.”) (emphasis added); *see also, e.g.*, EX1010, [0016] (“a PayPass PAN (or ‘PPAN’)”). Logically, a PPAN—*i.e.*, a PayPass payment *account* number—is simply a PAN for a PayPass account generally (and not device-based). Smith effectively states as much, indicating that a PPAN is mapped to a “funding account,” and not to a particular device. EX1010, [0041] (“[A] provisioning service might arrange for a mobile phone to be associated with a funding account (*e.g.*, by creating a PPAN and ***mapping the PPAN to a provided funding account*** in an account management system)”) (emphasis added). Smith states that the mobile device may also be associated with that funding account, but that does not mean that

the mobile device and the PPAN are associated with each other. Rather, each of the PPAN or the mobile device may be independently disassociated from that funding account. EX1010, [0041] (disclosing that the provisioning service may “disable the payment application on the mobile phone (without [*sic*: with] or without removing the personalization details)”). EX1010 [0028]-[0029], FIG. 4 (disclosing that personalization details include the PPAN). A PPAN could be re-assigned to a new device, or the same device could be provisioned with a new PPAN. EX1010, [0041]. Smith is consistent with each of these possibilities.

* * * *

In sum, Petitioner latches on to two sentences in Paragraph 16 of Smith to argue that the PPAN is a device account number. Pet., 50-53. But, when read in context, it is clear that the PPAN is linked to an account—initially a temporary PAN, and then later, an actual PAN—and not a particular device. Smith’s statement that a PPAN is “assigned to the mobile device,” is nothing more than shorthand to explain that a PPAN is provisioned to a mobile device (or “multiple NFC-enabled handsets,”) (EX1010, [0029])) as part of a personalized software package, which itself is tied to a Consumer ID and customer account. Figure 6 is strong evidence of this—it maps all of the different account numbers to a Customer ID without any mention of a device identifier. EX1010, FIG. 6. And, even during the registration process, the user only provides a phone number (device agnostic, and device-

changeable), personal information, and/or a model number (which could apply to countless actual devices). EX1010, [0028]. There is no indication anywhere in Smith that there is any mapping of a PPAN to a particular device, or even that the provisioning service is aware of the identity of the device to which it is provisioning the software. It appears to just be using the “phone number.” EX1010, [0028].

Accordingly, Petitioner has failed to meet its burden to show that Smith discloses a “*device account number*,” which is dispositive of Ground 2. Because claims 2-4 (Ground 3), 9 (Ground 4), 10 (Ground 5), 12-13 (Ground 8), 7 (Ground 9) and 6 (Ground 10) all depend on claim 1 and Petitioner does not put forth additional reasons as to why Bona, Smith, of Collinge disclose a “device account number” in those Grounds, they fail for the same reason as Ground 2.

B. Petitioner and its Expert Fail to Show a Motivation to Combine and Explain Why A POSITA Would Combine the PPAN of Smith With the Remote-SE System of Collinge

Petitioner claims that “Collinge in view of Smith teaches combining a CVC3 (limited-use payment information) and PPAN (static device account number) to create combined payment information which is collectively transmitted via NFC to a point-of-sale terminal for use in a financial transaction.” Pet., 73 (emphasis omitted). As discussed in Section VI.A., Smith does not teach a static device account number. But, even assuming the PPAN of Smith was a static device account number (it is not), Petitioner has failed to show that there was a motivation to combine or

reasonable expectation of success in combining Collinge with Smith, which are each directed to completely different mobile payment problems.

Petitioner asserts that “[a] POSITA would have been motivated to use Smith’s PPAN in place of Collinge’s PAN so that Collinge’s mobile device would not be required to store the PAN, which is a sensitive financial number.” Pet., 53. But Collinge is entirely directed to mobile devices that *lack* a secure element and thus cannot securely store sensitive financial information. EX1004, [0003]-[0005]. Collinge relies on a remote secure element (“SE”) to provision payment credentials to the device. EX1004, [0004]. There is no need for Collinge in an environment where the mobile device *has* a secure element; certainly nothing in either reference suggests that there is. Smith, on the other hand, is directed to the provision of a temporary PAN during the short period when an issuer is establishing a permanent account. EX1010, [0002]-[0003]. Smith specifically contemplates use of a secure element. EX1010, [0032].

Accordingly, Petitioner’s proposed combination makes no sense. The PPAN of Smith is intended to be used *with* a secure element, as per above. There is no reason that a POSITA would then use that PPAN in the system of Collinge, which lacks a secure element, and where the payment credentials are provisioned from a remote SE to a device. Moreover, the PPAN is a Mastercard-specific approach

(EX1010, [0022], [0026]) that lacks issuer-flexibility and thus would limit the usefulness of Collinge's invention.

Petitioner asserts that “[i]t was well known in the art that a device without a secure element (SE), such as Collinge's mobile device, could be vulnerable to malicious attacks and therefore storing Smith's PPAN instead of the PAN on Collinge's mobile device would have increased security for the user's account” and that “a POSITA would have understood that it is valuable to remove all traditional payment device account numbers from a user device so that if the device were stolen, the thief would have access only to PayPass PAN(s).” Pet., 53-54. There is no support in Smith or Collinge for this assertion. Smith is about issuing temporary PAN's during the very limited window of time when an issuer is establishing an actual account. The PPAN is discussed only in this context, without any mention of what it actually is, or whether it presents its own security vulnerabilities separate and apart from a PAN. Petitioner (and its expert, for that matter), simply assume, without evidence, that a PPAN would somehow be more secure. *See* Pet., 53-54 and EX1003, ¶¶241-243.

Further, Collinge provides its own security solution that does not depend on a replacement PAN; it involves provisioning a payment token payload including a single-use key, and then generating a cryptogram for use in a transaction. EX1004 [0044], [0070]. Smith was published years before Collinge was filed; if Collinge had

thought it useful to include a PPAN instead of a real PAN, Collinge easily could have said as much. But Collinge went a different direction and offered a cryptogram-based solution that is specifically used for mobile devices lacking a secure element.

C. Petitioner Fails to Demonstrate that a Person of Ordinary Skill in the Art would Use the Secure Card Device of Bona with the Secure Element-Free Mobile Device of Collinge

Each of Petitioner's proposed Grounds depend on the combination of Bona and Collinge. But, there are multiple reasons why Petitioner's proposed obvious combination does not make sense. Because claim 15 is representative of these issues, claim 15 is discussed in the below section; however, these arguments are equally applicable to all of Petitioner's Grounds, as each and every ground is based, at least in part, on the same basic arguments as to why a POSITA would combine Collinge and Bona. As it concerns limitations 15(a), 15(b), and 15(e) (and all similar limitations), Petitioner ignores all of the reasons why the smart card of Bona would not fit with Collinge's remote provisioning system for mobile phones without secure elements that it proposes.

Limitation 15(a) requires "a payment system comprising: a payment card device" that is "free of any fixed payment numbers" and "is operable for use in payment card reader equipment" and limitation 15(b) requires "a card-users personal computing device operable for completing a payment transaction." EX1001, 21:47-51, 24:52-53. Limitation 15(e) further explains that the personal computing device

of limitation 15(b) completes the transaction. EX1001, 21:65-66 (“a merchant is operable to receive a payment information provided by a personal computing device.”) With respect to these limitations, Petitioner argues that:

- (i) It would have been obvious to a POSITA to us[e] Collinge’s payment application on Collinge’s cell phone and also make payments at point-of-sale terminals” Pet., 24.
- (ii) “A POSITA would have understood that providing the user with both payment options would expand the number of POS terminals where Collinge’s payment credentials could be used and provide the user with additional payment options if an NFC-enabled point-of-sale terminal was broken, not enabled, or not present.” Pet., 24.
- (iii) A POSITA “would have had a reasonable expectation of success” that both Bona and Collinge were designed with “reference to the same well-known technical industry standards” and that “modifying Collinge to send payment credentials and dynamic data (such as a payment cryptogram) to Bona’s payment card would not change the functionality of Bona and Collinge.” Pet., 24-25.

Petitioner’s expert parrots the Petition (or vice versa—they are effectively the same, EX1003 ¶¶149-154) and adds little more than the conclusion that “Bona and

Collinge are directed towards improved payment systems that reduce the risk of fraudulent transactions.” EX1003¶154.

All of these obviousness arguments, from both Petitioner and its expert, ignore:

(1) that even if a POSITA would have been motivated to “transmit the necessary transaction information to Bona’s companion card for use in a magnetic stripe transaction using NFC communications,” as Petitioner claims, then the other limitations of claim 15 would not be met. Pet., 25. For instance, claim 15 also requires that a “merchant is operable to receive a payment information provided by a *personal computing device*,” (limitation 15(e)) not a smart card like that in Bona. EX1001, 21:65-67 (emphasis added). Petitioner does not argue otherwise, and instead, with respect to limitation 15(e), completely flips its proposed combination, arguing that the device of Collinge would transmit the payment information.

(2) the fact that Bona already describes a smart card that generates dynamic data (e.g. CVC3 numbers). Petitioner does not explain how the software of Bona would be modified by the system of Collinge so that they would be compatible with each others’ approach; and

(3) the purpose of Collinge, namely the provisioning of credentials from a first remote device to a device without a secure element. This stands

in contrast with the teachings of Bona, which describes smart card and mobile phone which both securely store payment credentials.

First, claim element 15(a) recites “a payment card device that is free of any fixed payment numbers disposed thereon and wherein said payment card device is operable for use in a merchant card-reader equipment.” EX1001, 21:48-51. To meet this limitation, Petitioner relies on a combination of Collinge with Bona. Petitioner asserts that “[i]t was well-known that many point-of-sale terminals only accepted a physical magstripe payment method,” Pet., 24, and that Bona recognized that “existing contactless transaction enabled cell phones cannot be used for magnetic stripe transactions, which is the dominant technology presently in use.” Pet., 24 (internal citations omitted). Petitioner relies exclusively on this evidence, and copy-paste assertions from its expert (EX1003, ¶¶143-144) to suggest that a POSITA would combine Collinge with Bona. However, this motivation conflicts with Petitioner’s argument related to claim element 15(e).

Limitation 15(e) recites “wherein a merchant is operable to receive a payment information provided by a personal computing device.” EX1001, 21:65-67. Here, instead of relying on Bona (which performs traditional mag-stripe transactions), Petitioner relies on the mobile device of Collinge (which replaces traditional mag-stripe transactions) to meet this limitation. Pet., 37. Petitioner simply ignores its previous position that “[i]n the combined system, Collinge would transmit the

necessary transaction information to Bona's companion card for use in a magnetic stripe transaction using NFC communications." Pet., 25. Indeed, Petitioner never explains why a POSITA would transmit the cryptogram of Collinge to the card of Bona, only to turn around and complete the transaction using the device of Collinge. Under Petitioner's theory, transferring the cryptogram from the mobile device to the card is entirely superfluous.

Collinge explains that it is targeted at "enabl[ing] a mobile device lacking a secure element to conduct contactless payment transactions." EX1004 [0005]. Collinge enables "contactless/NFC payment transactions using the mobile payment application" and a "single use key." EX1004, [0070]. Each embodiment of Collinge is directed exclusively at performing contactless payment transactions. *See* EX1004, [0070], [0072], [0079], [0092], [0112], [0118], [0122], [0125]. Collinge indicates that the credentials used by the remote secure element system include a "card profile" that may contain "common payment credentials" including those payment credentials that would otherwise be stored on a card's "magnetic stripe." EX1004, [0048]. Petitioner asserts that because Bona, not Collinge, seeks to "enable[] cell phones" to be "used for magnetic stripe transactions" a POSITA would be motivated to combine the teachings of Bona and Collinge. Pet., 24. However, Petitioner fails to reconcile the fact that Collinge seeks to enable *contactless* NFC transactions, not

card present transactions, that use the same information found in a magnetic stripe with the disclosure of Bona.

Second, even if a POSITA would want to use a remote mobile provisioning and application system, like the one described in Collinge (for some unspecified security reason), there is no reason they would look to the mobile application of Collinge to generate a CVC3 given that the smart card of Bona already generates a CVC3 code. Nor does Petitioner ever explain how a POSITA would fit the cryptogram of Collinge into the mag-stripe data of Bona (which already has a distinct CVC3 value). Specifically, Bona already discloses that “[t]he smart card would have some secured data, such as an identification of the user and an account number, as well as a smart card chip that can generate dynamic data (e.g., a code and/or transaction number).” EX1009, [0105], [0038] (disclosing “information can include the dCVV or CVC3 codes discussed above that are generated by the smart card for use in card present transactions.”). At the same time, Collinge describes that it is configured to generate a cryptogram via a mobile application exclusively stored on the mobile device in conjunction with a remote-SE system. EX1004, [0043], [0063]. Petitioner fails to explain why a POSITA would seek to generate a cryptogram of Collinge and combine it with the CVC3 (and other information) of Bona or how such a combination would work, or how the software of Bona would have to be adjusted to make that combination effective.

Instead, Petitioner asserts that “[a] POSITA would have appreciated that modifying Collinge to send payment credentials and dynamic data (such as a payment cryptogram) to Bona’s payment card would not change the functionality of Bona and Collinge.” Pet., 25. But, in so asserting, Petitioner simply ignores that the device of Bona already creates a CVC3 value. Petitioner also fails to explain how the cryptogram of Collinge would be encoded into the mag-stripe data of Bona or how the cryptogram of Collinge would be used, in addition to, the CVC3 of Bona, or how the software of Bona would be modified to use the cryptogram of Collinge.

Third, Petitioner fails to explain why a POSTIA would combine two complete (and alternative) systems. Collinge is directed *exclusively* to “generating and provisioning payment credentials to a mobile device lacking a secure element.” EX1004, Abstract. Collinge explains that the system it describes applies to mobile phones without secure element chips, because mobile phones that lack a secure element cannot “securely store payment card credentials.” EX1004, [0003]-[0004]. Petitioner’s expert acknowledges this when discussing the background of Collinge, but never considers it in connection with the proposed combination. EX1003 ¶76.

The reason this is important is that there is no need for the remote secure element system of Collinge in the smartcard of Bona. Bona already provides a secure system that stores the payment credentials that Collinge does not. Bona specifically explains that “a smart card would have some secured data, such as an identification

of the user and an account number, as well as a smart card chip that can generate dynamic data.” EX1009, [0105]. Bona further describes that the smart card device performs transactions “using secure data stored in the device.” EX1009, [0113].

Bona is therefore an *alternative* solution to the problem that Collinge seeks to solve.

And although Bona discloses one embodiment in which a smart card may be paired with a mobile device, the mobile device of Bona is similarly able to securely store credentials (which the mobile of Collinge cannot). EX1009, [0109], [0098], [0042].

But Bona is targeted mainly at systems in which the smart card comprises a display and a processor, such that the smart card can function and run applications without communicating with a mobile device. EX1009, [0045]-[0047]; FIGs. 2A, 3A, 8, 13A-B. Petitioner and its expert never consider the purpose of each disclosure or the problem that each reference is solving for. Instead, they just regurgitate boilerplate obviousness positions about motivations to combine and expectations of success that have little connection to the references and disclosures themselves. Petitioner and its expert briefly mention that a POSITA would be motivated to combine Bona with Collinge so as to allow the device of Collinge to be able to be used on magnetic stripe readers. Pet., 23-24; EX1003 ¶¶142-155. But Collinge does not seek to use magnetic stripe readers. In fact, Collinge discloses that the payment credentials that it sends via NFC include “magnetic stripe (mag stripe) payment credentials,” replacing the use of a physical magnetic stripe. EX1004, [0048]. Petitioner simply

fails to explain why a POSITA would combine the secure smart card of Bona with the remote secure element provisioning system of Collinge.

VII. CONCLUSION

For the reasons explained above, Petitioner has failed to show a reasonable likelihood of success that any challenged claim is unpatentable. Patent Owner thus respectfully submits that institution should be denied.

Dated: October 10, 2025

Respectfully submitted,

/Matt Berkowitz

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

mberkowitz@reichmanjorgensen.com

REICHMAN JORGENSEN

LEHMAN & FELDBERG LLP

100 Marine Parkway, Suite 300

Redwood Shores, CA 94065

Telephone: (650) 623-1401

Facsimile: (650) 560-3501

Lead Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE

I hereby certify that this paper complies with the type-volume limitation of 37C.F.R. §42.24 (as determined by the Microsoft Word word-processing system used to prepare this paper) because it contains 7,718 words, excluding the parts of the paper exempted by 37 C.F.R. §42.24(a).

Dated: October 10, 2025

/Matt Berkowitz/

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

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6, the undersigned certifies that on October 10, 2025 a copy of the foregoing document was served by email to counsel for Petitioner:

Adam P. Seitz (Reg. No. 52,206)
adam.seitz@eriseip.com
Mark Lang (Reg. No. 55,356)
Mark.Lang@eriseip.com
Lydia Raw (Reg. No. 76,436)
Lydia.raw@eriseip.com
PTAB@eriseip.com
ERISE IP, P.A.
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
Telephone: (913) 777-5600
Facsimile: (913) 777-5601

By: /Matt Berkowitz/

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