

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. IPR2025-01152
U.S. Patent No. 11,620,634

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE '634 PATENT CLAIMS.....	3
III. PETITIONER’S ALLEGED PRIOR ART	4
A. Collinge.....	4
B. Sahota.....	5
C. Smith	6
IV. LEVEL OF ORDINARY SKILL IN THE ART	9
V. ARGUMENT.....	10
A. Petitioner Fails to Show a Reasonable Likelihood of Success on All Grounds Because Collinge Teaches Away from a Sequential Parameter Originating From the Electronic Device.	10
B. Petitioner Fails to Meet Its Burden as to Ground 2.	16
1. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination has “static device-specific user account information” as recited in limitations 29(g) and 29(h).	16
VI. CONCLUSION.....	27

PATENT OWNER’S EXHIBIT LIST

No.	Exhibit Description
2001	Memorandum for Interim Processes for PTAB Workload Management, dated March 26, 2025
2002	Interim Director Discretionary Process <i>available at</i> https://www.uspto.gov/patents/ptab/interim-director-discretionary-process
2003	Agreed Scheduling Order in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. May 20, 2025)
2004	Standing Order Governing Proceedings (OGP)—Patent Cases for cases before Judge Albright (dated Mar. 5, 2025)
2005	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, <i>available at</i> https://www.txwd.uscourts.gov/judges-information/judges-directory-biographies/
2007	Complaint in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Nov. 4, 2024)
2008	First Agreed Scheduling Order in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2009	Complaint in <i>CardWare Inc. v. Google LLC</i> , No. 7:24-cv-00278-DC-DTG (W.D. Tex. Mar. 6, 2025)
2010	Invalidity Contentions Cover Pleading in <i>CardWare Inc. v. Apple Inc.</i> , No. 1:25-cv-00446-ADA (W.D. Tex. Apr. 7, 2025)
2011	Defendants’ Notice of Subpoena to Apple, Inc. in <i>CardWare Inc. v. Samsung Elecs. Co., Ltd.</i> , No. 2:22-cv-00141-JRG-RSP (E.D. Tex. Dec. 9, 2022)
2012	Apple Inc.’s Response and Objections to Defendants’ Subpoena in <i>CardWare Inc. v. Samsung Elecs. Co., Ltd.</i> , No. 2:22-cv-00141-JRG-RSP (E.D. Tex. Dec. 23, 2022)
2013	Letter from CardWare, Inc. to Apple Inc. dated October 10, 2023 “RE: Patent Portfolio of CardWare Inc.”
2014	Proof of Delivery to Apple Inc. dated October 11, 2023, for Letter from CardWare, Inc. to Apple Inc. dated October 10, 2023 “RE: Patent Portfolio of CardWare Inc.”
2015	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-cv-00446-ADA (W.D. Tex. Aug. 29, 2025)

I. INTRODUCTION

On June 20, 2025, Apple Inc. (“Apple” or “Petitioner”) filed a Petition requesting *inter partes review* of claims 1-72 (“Challenged Claims”) of U.S. Patent No. 11,620,634 (“the ’634 Patent”) (EX1001), entirely on multi-reference combination 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, for Grounds 1-5, Petitioner failed to demonstrate why a POSITA would be motivated to combine *Collinge* with *Sahota* to meet the limitation “said limited-use payment information is dynamically generated based on a per-transaction sequential parameter *originating from the electronic device*” of claim 1 (and similar limitations in other independent claims). *Collinge* is specifically directed to the security problem associated with mobile devices lacking a secure element. The invention of *Collinge* is directed to moving all payment credentials and the transaction counter to a *remote* secure element, which can then be provisioned, as-needed, to the mobile device. Accordingly, it specifically teaches away from a sequence counter originating from the electronic device; the whole idea is about

offboarding the credentials for payments. *Sahota* is older technology (by a decade) and effectively describes the very problem that *Collinge* is trying to address (*i.e.*, *Collinge* is directed to fixing security problems arising from the on-device storage of payment credentials and transaction account, such as that disclosed in the older *Sahota* invention). Specifically, the key issue of storing sensitive credentials on a device without a secure element is that they are susceptible to extraction, copying, hacking, phishing or cloning (*e.g.*, making an infinite number of cloned phones, all with the same usable payment information). Petitioner ignores this and suggests that a POSITA would have modified *Collinge* to create the exact problem that *Collinge* is fixing.

Second, for Ground 2, Petitioner fails to show that its proposed obviousness combination includes a “static device-specific user account information,” as required by claim 29. Petitioner relies on *Smith*’s “PPAN” as disclosing this limitation, but *Smith* teaches that the PPAN is mapped to a user’s account. This says nothing about whether it is “device-specific.” For example, *Smith* does not say that its PPAN is limited to a particular device (*e.g.*, it could be used with multiple devices at the same time) and does not say what happens if a user gets a new device (*e.g.*, the PPAN could be re-used on the new device). To the contrary, *Smith* says that “multiple NFC-enabled handsets may be managed for a single account.” EX1010, [0029]. Petitioner

offers no further obviousness argument based on *Smith* and this limitation. Pet., 68-78.

II. THE '634 PATENT CLAIMS

The '634 Patent generally relates to “electronic or smart payment devices and, more specifically, to more secure, smart multi-function *smart tokenizing*¹ electronic payment devices and transaction processing thereof.” EX1001, 1:26-31. The disclosed method involves receiving a priming operation from an identified user and a request for a payment transaction at an electronic device. EX1001, 19:59-62. The electronic device then displays on a touch-screen display “information reflecting the payment request, and an image representing a selected issued payment account.” EX1001, 19:63-65. The electronic device then “dynamically generat[es] ... limited-use payment information ... based on a per-transaction sequential parameter originating from the electronic device.” EX1001, 19:66-20:31. The method further includes “using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account.” EX1001, 20:32-35.

The “limited-use payment information,” which is used in place of issued payment information, is then transmitted from the electronic device via NFC

¹ Unless noted, all coloring and emphasis has been added.

interface and a status of the payment transaction is displayed on the device's touch screen display. EX1001, 20:36-43.

The various cryptographic techniques of the '634 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 seven references in its Grounds, but only *Collinge*, *Sahota*, and *Smith* are relevant to Patent Owner's preliminary responsive positions herein. Patent Owner provides an overview of these references in this Section III. Patent Owner then explains in the following sections how Petitioner's Grounds using these references fail to demonstrate a reasonable likelihood of success that any Challenged Claim is obvious.

A. 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, one of which is a remote secure element (SE) system that provisions payment credentials to a mobile device. EX1004, [0007], Figs. 1-4, 6, and 7. *Collinge* explains that such a two-computer remote-SE 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 solves this problem by creating a provisioning system comprising a remote-SE computing device that contains a secure element suitable to store payment credentials. During the transaction the payment credentials are transmitted to a mobile device that does not contain a secure element, and therefore is not suitable for long term secure storage of the payment credentials. EX1004, [0068]. The mobile device then uses the key 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].

B. Sahota

U.S. Patent App. Pub. No. 2005/0043997 (“*Sahota*”) is a 2003 reference focused on the “skimming” problem, which “refers to the electronic copying of the card’s magnetic stripe data to create counterfeit cards.” EX1011, [0003]. In other words, the premise of *Sahota*’s invention is that the real payment credentials are

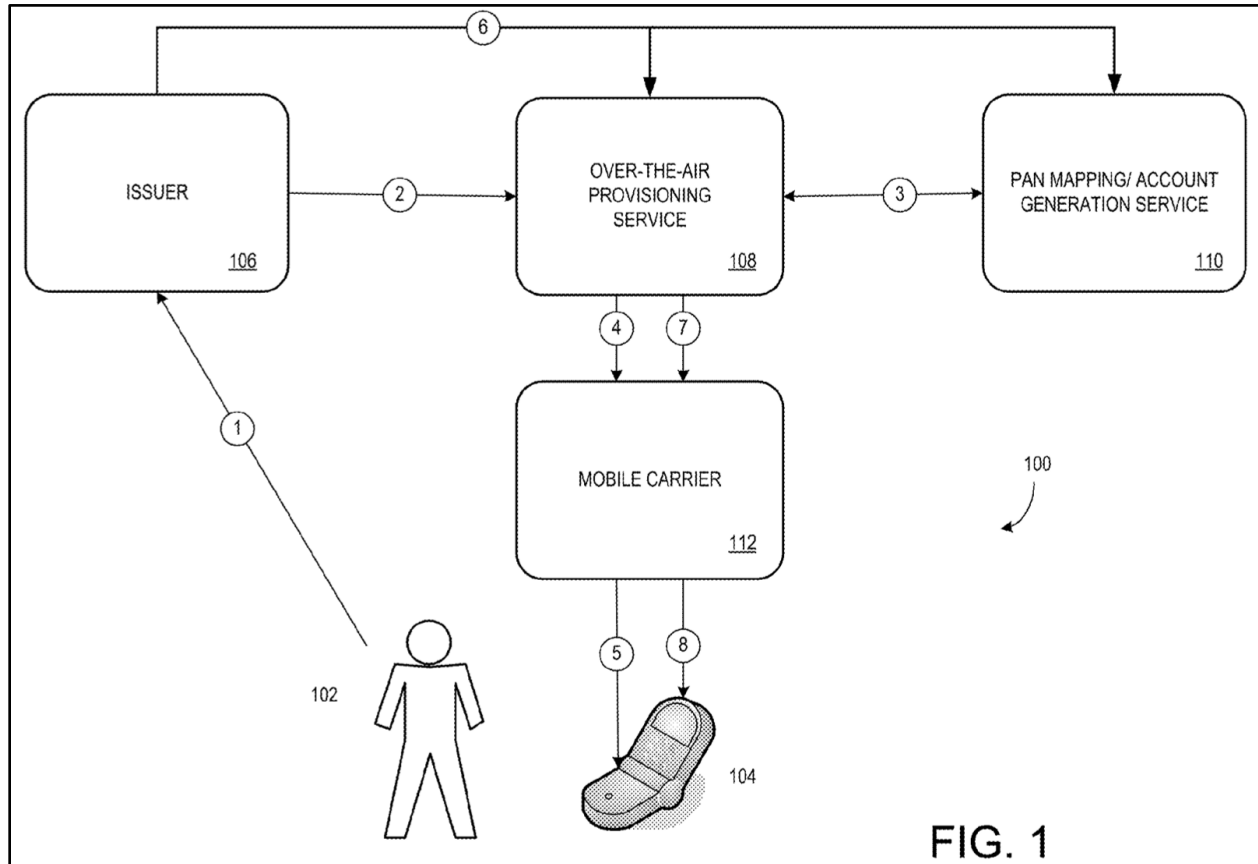
stored on-card and on-device. To address this skimming problem, *Sahota* discloses a method for “dynamically generating a verification value for a transaction and for utilizing such value to verify the authenticity of the payment service application.” EX1011, Abstract. “The dynamically generated Card Verification Value (referred to herein as the ‘dCVV’) is generated on the payment device, embedded into the payment data, and transmitted to a point of sale terminal.” EX1011, [0021].

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, Fig. 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.

IV. LEVEL OF ORDINARY SKILL IN THE ART

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

V. ARGUMENT

A. Petitioner Fails to Show a Reasonable Likelihood of Success on All Grounds Because *Collinge* Teaches Away from a Sequential Parameter Originating From the Electronic Device.

Three of the four independent claims of the '634 Patent (spanning Grounds 1 and 3-5) require limited-use payment information that is dynamically generated based on a per-transaction sequential parameter “*originating from the electronic device*.” Claim 29 (Ground 2) includes very similar language with the same import (“based on a sequential counter count *from the* electronic device.”). In every such Ground, Petitioner asserts that this is met by the combination of *Collinge* in view of *Sahota*.

Petitioner is wrong because *Collinge* specifically teaches away from a transaction counter originating *from the electronic device*; to the contrary, the whole idea of *Collinge* is to offboard all payment information such as the transaction counter, to minimize security vulnerabilities associated with mobile devices lacking a secure element. According to *Collinge*, secure elements are necessary to “securely store payment account credentials.” EX1004, [0003]. *Collinge*’s basic premise is that without this secure element, the stored information is vulnerable to fraud, cloning and hacking.

Collinge addresses this problem (*i.e.*, payments using mobile devices without secure elements) with a “remote secure element” or “remote-SE” that provisions a

“payment token payload” to the mobile device. EX1004, [0043]. That payload includes an application transaction counter and “enable[s] the user 102 to use the mobile device 104 to conduct NFC payment transactions without the use of a secure element.” EX1004, [0046], [0050].

There is no reason that a POSITA would generate limited-use payment information using a per-transaction sequential parameter *originating from the electronic device* of *Collinge*. Not surprisingly, in every embodiment where *Collinge* discusses an application transaction counter, the count is stored in the remote-SE and is provisioned *to* the mobile device. It does not originate from the mobile device. Indeed, originating the transaction count *from* the mobile device would defeat the whole purpose of *Collinge*. In *Collinge*’s universe, that would make the transaction counter vulnerable to theft because of the lack of a secure element. Petitioner never mentions this issue or acknowledges the fact that *Collinge* is specifically directed to offboarding the payment information such as the transaction counter because of the lack of a secure element.

* * * *

Petitioner’s Ground 1 is based on a proposed combination of *Collinge*, *Lin*, and *Sahota*, but Petitioner relies entirely on *Collinge* and *Sahota* as it concerns limitation 1(f) requiring “wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating

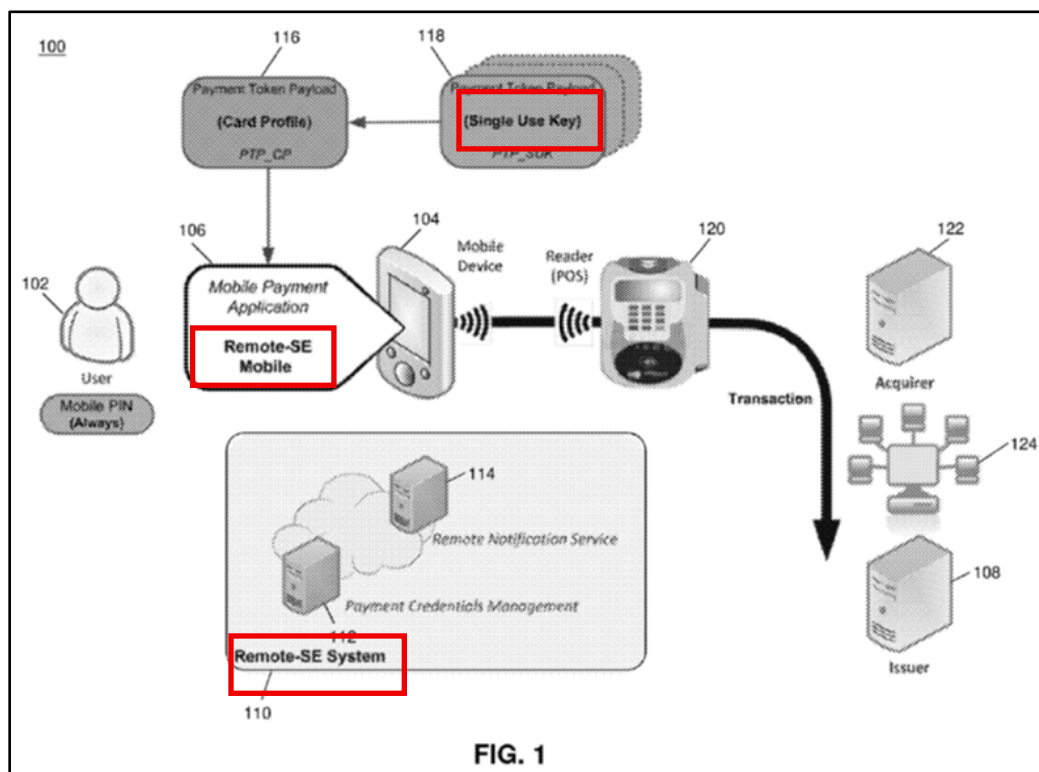
from the electronic device.” Pet., 41-42. Petitioner does the same as it concerns the remaining grounds, and, for each limitation relating to the sequential parameter or transaction count, incorporates-by-reference its discussion on pages 41-42 as it concerns *Collinge* and *Sahota*. Pet., 59 (re: claim limitation 39(i)); Pet., 64 (re: claim limitation 56(i)²), and Pet., 67 (re: claim limitation 29(f)).

Petitioner argues that *Collinge* discloses a payload that includes “the application transaction counter,” but acknowledges that this comes from the “cloud system” and that it is “transmitted ‘to the mobile device 104 for use in generating a CVC3 value.’” Pet. at 41. In other words, Petitioner acknowledges that *Collinge* does not disclose a sequential parameter “originating from the electronic device.” Instead, Petitioner relies on *Sahota*, citing a single sentence where *Sahota* states that the “payment device will also maintain an application transaction counter (ATC).” Pet., 42. Petitioner argues that “[a] POSITA would have been motivated to modify mobile device 104 to maintain its own application transaction counter,” citing its expert (and only its expert). Pet., 42.

This assertion directly contradicts the point of *Collinge*’s invention; the idea of *Collinge* is to offboard the transaction counter and other payment-related

² Per the Claim Listing Appendix, Petitioner’s limitation 56(i) corresponds to the “dynamically generate” limitation.

information to the cloud because of security risks *on the device*. EX1004, Abstract, [0002]-[0005]. This is shown, for example, in Figures 1, 2, and 5, which each show how the single use key is provisioned *to* the mobile device. The single use key can include the application transaction counter. EX1004, [0007]-[0008], [0050]. In other instances, the transaction counter comes from a remote source and is provisioned *to* the device. *See id*; *see also* EX1004, [0083]-[0085].



EX1004, FIG. 1.

There is no credible reason, and Petitioner has not articulated any, why a POSITA would onboard the application transaction counter when *Collinge's* entire invention is about doing the opposite.

Petitioner asserts that “[h]aving an ATC in sync in two different places was a known technique, and would have prevented possible fraud in Collinge’s payment system in the same way as Sahota’s payment system.” Pet., 42. But, *Sahota* is a 2003 reference (pre-dating *Collinge* by a decade) and concerned with “skimming,” which “refers to the electronic copying of the card’s magnetic stripe data to create counterfeit cards.” EX1011, [0003]. *Sahota* discusses various skimming technologies, including “line tapping,” as well as examples where skimmers have tapped into issuers’ computers. EX1011, [0004]. *Sahota* explains that skimming is “predominately a phenomenon afflicting magnetic stripe based transactions” given its nature as “passive media,” EX1011, [0005], but in all instances concerns risks of intercepting real (issuer-provided) credit card numbers. In other words, *Sahota* is directed to the problem whereby the payment credentials are the original fixed issuer numbers stored on the reader interface of the device itself, either in magnetic stripe data or in some other form. That was the nature of the technology in 2003; *Sahota* does not address security problems beyond skimming, including the hacking vulnerabilities associated with mobile devices lacking a secure element.

In other words, what Petitioner is missing is that *Collinge* is directed to a more sophisticated problem—it is effectively directed to problems associated *with* the *Sahota* system, including risks of storing payment credentials, and originating transaction information, from the device. A decade after *Sahota*, the art still needed

to solve problems associated with hacking, cloning and other types of fraud beyond skimming. *Collinge* is directed to just those problems. In other words, it was not enough to just add a dCVV and ATC to an in-store transaction; there was still a risk that payment credentials and a transaction count could be compromised if they were stored on a device lacking a secure element. Accordingly, *Collinge* is an *advance* on *Sahota*; Petitioner's proposed modification would actually take *Collinge* backwards a decade and expose the transaction count to the exact fraud risks that *Collinge* is trying to avoid (*i.e.*, those associated with devices lacking a secure element).

Petitioner's argument that an ATC in sync in two different places would have prevented possible fraud is a non-sequitur. An ATC is *always* in sync in two different places; that is the whole point of an ATC—to authenticate a transaction by comparing two counters. The relevant question is just *where* those places are and how secure are they? *Collinge* tells us that neither of those places should be *on the device* because that is a security risk. There is no reason that a POSITA would ignore *Collinge's* invention entirely and put the transaction counter back on the device itself.

Petitioner's expert does not actually address the issue of why a POSITA would want to have an on-device ATC in connection with *Collinge*. Petitioner's expert asserts that the ATC “provides an additional security barrier because even if a bad actor managed to intercept the encrypted payload provisioned to *Collinge* mobile

device, they would need to know the next transaction count number to be able to use the credentials in any way.” EX1003 ¶164. Petitioner’s expert is correct that an ATC provides an additional security barrier. But this does not address the issue because *Collinge* already discloses an ATC; *Sahota* does not add anything in this regard. The question is *where* the ATC is originated. Petitioner’s expert never addresses this issue. Moreover, *Collinge* says that it should come from the remote-SE. That is not random; *Collinge* generated the ATC remotely because, in the context of his invention, it was more secure than keeping it on the device itself (as per the decade-old approach of *Sahota*). Petitioner’s expert does not address this and instead advocates doing a modification that conflicts with *Collinge*’s teachings.

Accordingly, Petitioner has failed to demonstrate a reasonable likelihood of success as it concerns all Grounds.

B. Petitioner Fails to Meet Its Burden as to Ground 2.

1. Petitioner Fails to Meet Its Burden of Showing That Its Proposed Combination has “static device-specific user account information” as recited in limitations 29(g) and 29(h).

Ground 2 in the Petition additionally fails because Petitioner fails to show that its proposed obviousness combination includes a “static *device-specific* user account information” as required by the following limitations in independent claim 29 of the ’634 Patent:

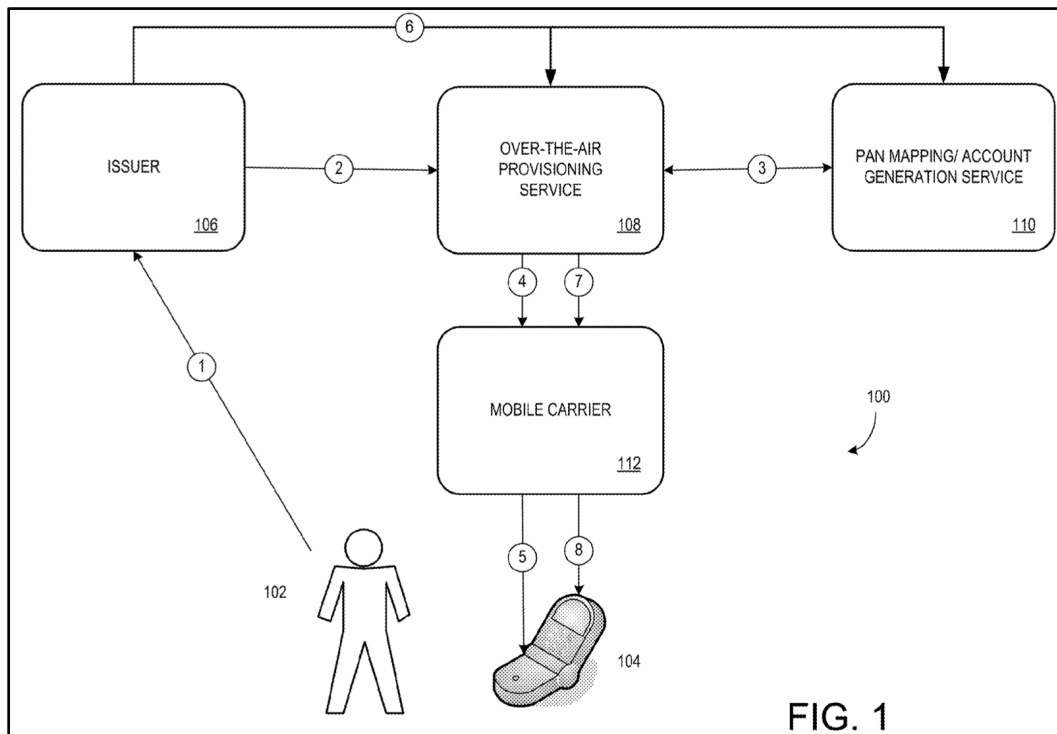
1. 29(g), requiring “wherein the electronic device is operable to store a static *device-specific* user account information;”
2. 29(h), requiring “wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static *device-specific* user account information to an NFC recipient”

EX1001, 23:7-41 (emphases added).

Petitioner relies solely on *Smith* as allegedly disclosing the claimed “static *device-specific* user account information” Pet., 68-76. In particular, Petitioner asserts that the “PPAN” of *Smith* is the “device-specific user account information” Pet., 69 (“The PPAN is, therefore, a *device-specific account number*.” (emphasis in original)); *see also* Pet., 72 (“A POSITA would have found it obvious and been motivated to use Smith’s PPAN in place of Collinge’s PAN.”). Petitioner’s assertion is incorrect. *Smith* never once says that the PPAN is a “device-specific” 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. *See* EX1010, [0014]. 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

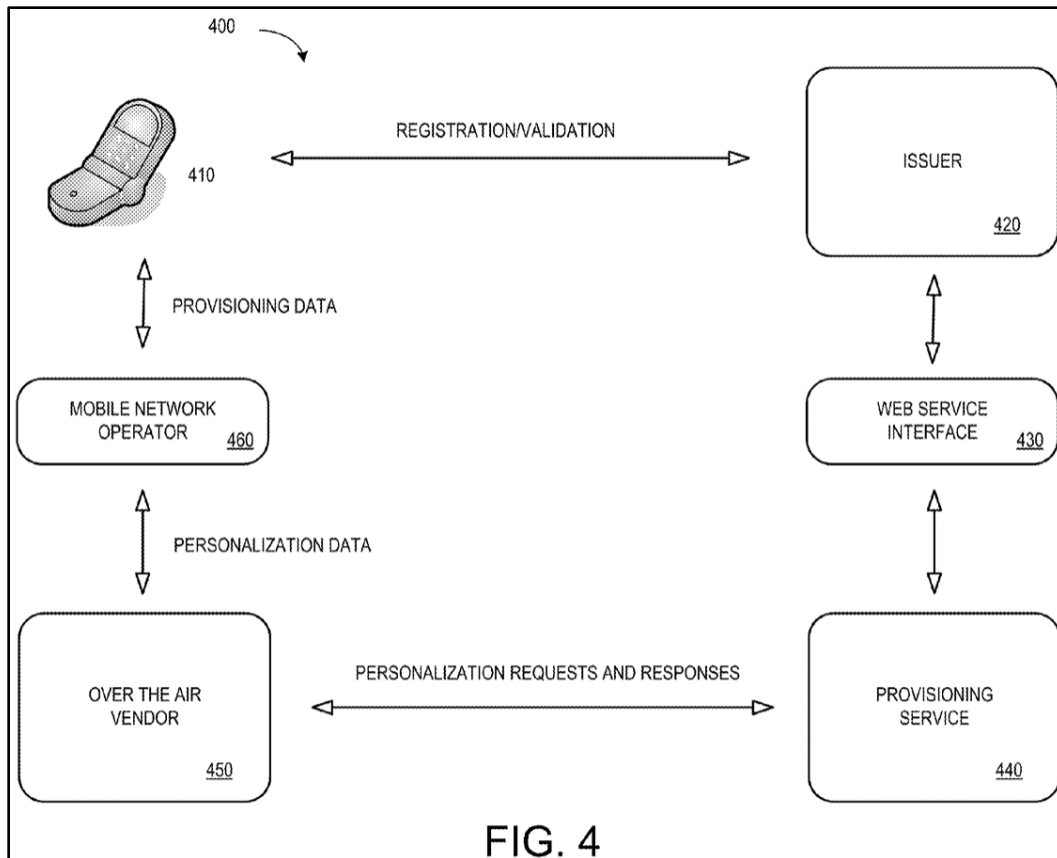
service 110 so that a PayPass PAN (or ‘PPAN’) may be assigned to the mobile device 104.” EX1010, [0016]; Pet., 69. “The PAN mapping/account generation service 110 assigns a PPAN to the device 104, and also maps the newly-assigned PPAN to the temporary PAN provided by the issuer 106.” EX1010, [0016]. These two sentences in *Smith* effectively constitute the entirety of Petitioner’s argument that the PPAN is a “static device-specific user account information.” Pet., 69 (citing EX1010, [0016]). Petitioner misinterprets *Smith*’s disclosure and, notably, omits any contextual explanation of this paragraph or Smith’s actual invention in its discussion of the “static device-specific user account information.” See Pet., 12-13, 67-72.

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. EX1005, [0028]. Notably, there is no discussion of inputting a Device ID. 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.*”) (emphases 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 static device-specific user account information. Pet., 67-72. 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 “static *device-specific* user account information” as required by limitation 29(g) and 29(h). This is dispositive of Petitioner’s Ground 2 and demonstrates that Petitioner has not shown a reasonable likelihood of success that any of Challenged Claims 29-38 is obvious. However, for completeness, Patent Owner notes that *Collinge* also fails to disclose a “static *device-specific* user account information”—nor does Petitioner so argue. *See* Pet., 68. *Collinge* uses a VPAN in transactions, which is not “device-specific.” *See supra* Section III.A.

For at least the foregoing reasons, Petitioner fails to meet its burden of showing that its proposed combination has “static *device-specific* user account information” as required in limitations 29(g) and 29(h).

VI. CONCLUSION

For the reasons stated above, Petitioner's proposed combinations fail to disclose key limitations of the Challenged Claims of the '634 Patent. Petitioner has also failed to show a motivation to combine or reasonable expectation of success in combining the references in its Grounds. Therefore, Petitioner has failed to show a reasonable likelihood of success that any Challenged Claim is unpatentable for any Ground. Patent Owner respectfully submits that institution should be denied.

Dated: October 10, 2025

Respectfully submitted,

/Matt Berkowitz/

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

mberkowitz@reichmanjorgensen.com

REICHMAN JORGENSEN

LEHMAN & FELDBERG LLP

100 Marine Parkway, Suite 300

Redwood Shores, CA 94065

Telephone: (650) 623-1401

Facsimile: (650) 560-3501

Lead Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE

I hereby certify that this paper complies with the type-volume limitation of 37 C.F.R. §42.24 (as determined by the Microsoft Word word-processing system used to prepare this paper) because it contains 5177 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)