

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. IPR2025-01148
U.S. Patent No. 10,810,579

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	Page
I. INTRODUCTION.....	1
II. THE '579 PATENT CLAIMS	2
III. PETITIONER’S ALLEGED PRIOR ART	4
A. Collinge	5
IV. LEVEL OF ORDINARY SKILL IN THE ART	7
V. ARGUMENT	7
A. Petitioner Fails to Meet Its Burden of Showing That Any of Its Proposed Combinations Disclose “Using Said Limited-Use Payment Information in Place of Said Card Issuer Supplied Payment Information”	7
1. All of the Challenged Independent Claims Require That the Generated Limited Use Information Be Used “In Place Of” Issuer Payment Information	8
2. Collinge Does Not Disclose Using Limited-Use Information “In Place Of” Issuer Payment Information	14
a. Collinge Does Not Disclose Using a Cryptogram or CVC3 in Place of Anything, Let Alone Issuer Payment Information as Required by All Challenged Claims	16
b. Collinge Does Not Disclose Using the Cryptogram or CVC3 in Place of a Card Number With 5 or More Digits as Required by Independent Claim 1	27
3. Petitioner’s Other Grounds Fail for the Same Reason	30
VI. PETITIONER OMITTS ITS CONTRADICTORY DISTRICT-COURT INDEFINITENESS ARGUMENTS THAT CLAIM SCOPE ALLEGEDLY CANNOT BE ASCERTAINED	31
VII. CONCLUSION	33

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Ecolochem, Inc. v. S. Cal. Edison Co.</i> , 227 F.3d 1361 (Fed. Cir. 2000)	22
<i>Energizer Holdings, Inc. v. Int’l Trade Comm’n</i> , 435 F.3d 1366 (Fed. Cir. 2006)	29
<i>Microchip Tech. Inc. v. Aptiv Techs. AG</i> , IPR2024-00558, Paper 12 (PTAB Oct. 7, 2024)	32
<i>Salazar v. AT&T Mobility LLC</i> , 64 F.4th 1311 (Fed. Cir. 2023)	28
<i>Summit 6, LLC v. Samsung Elecs. Co., Ltd.</i> , 802 F.3d 1283 (Fed. Cir. 2015)	29
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	22

Regulations

37 C.F.R. § 11.18	32
37 C.F.R. § 42.11	32
37 C.F.R. § 42.12(b)	32

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 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)

No.	Exhibit Description
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-cv00446-ADA (W.D. Tex. Aug. 29, 2025)

I. INTRODUCTION

On June 24, 2025, Apple Inc. (“Apple” or “Petitioner”) filed a Petition requesting *inter partes review* of claims 1-23 (“Challenged Claims”) of U.S. Patent No. 10,810,579 (“the ’579 Patent”) (EX1001), entirely on 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, which generally relate to methods and systems for reducing the risk of fraud in connection with completing payment transactions. The ’579 Patent includes 3 independent claims: claims 1, 15, and 19. Petitioner’s arguments regarding Ground 1 (which challenges independent claims 1 and 19 and dependent claims 2-3, 7, 10, 11, 12, 20 and 23) and Ground 5 (which challenges independent claim 15 and dependent claims 16-18) are representative of the Petition’s main flaw: none of the references cited by Petitioner disclose using generated limited-use information *in place of* issuer provided payment information, as required by every Challenged Claim. Indeed, as Petitioner seemingly concedes, Collinge—the sole reference relied upon for this limitation—does not actually disclose using any information in place of anything else, let alone that the alleged limited-use information is used in place

of issued provided payment information. Instead, Collinge exclusively discloses *adding* a payment cryptogram (the alleged limited-use information) to payment credentials (the issuer provided payment information) and transmitting *both together* as part of a complete transaction—which is the opposite of what the claims require.

This same problem exists with Ground 2 (challenging dependent claims 5-6), Ground 3 (challenging claims 4, 21, and 22), Ground 4 (challenging claims 8-9), Ground 6 (challenging dependent claim 13), and Ground 7 (challenging dependent claim 14) at least because Petitioner relies on the same combination of references and disclosure as Grounds 1 and 5 (as relevant to independent claims 1, 15, and 19), plus additional references, Lin, Phillips, Kranzley, Smith, Abbye, Pisula, and Fadell (addressing only additional limitations in the dependent claims).

Accordingly, for these reasons and those explained below, Patent Owner respectfully submits that Petitioner has failed to show a reasonable likelihood of success that any Challenged Claim is unpatentable, and the Board should therefore decline to institute.

II. THE '579 PATENT CLAIMS

When David Wyatt conceived of the invention claimed in the '579 Patent over a decade ago, there were “several different types of credit cards available in the marketplace.” EX1001, 1:31-32.

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, 1:32-40.

The claims of the '579 Patent generally relate to systems and methods for reducing fraud during payment transactions. Independent claims 1, 15, and 19 share several limitations. For purposes of this POPR, independent claim 1 is illustrative and is directed to a method of performing a payment transaction via a near-field communication (NFC) interface of an electronic device. EX1001, 18:58-19:18 (claim 1). The method involves receiving a priming operation from an identified user and a request for a transaction payment at an electronic device via an NFC interface. EX1001, 18:60-19:6. The electronic device then displays "images of: a card issuer payment method selection" including at least a portion of an original account number (such as a traditional credit card number). EX1001, 19:3-6. The method then "generat[es], by the processor, a limited-use payment information" for use "in place of said card issuer supplied payment information." EX1001, 19:9-12. In other words,

a “selection” from one of multiple payment methods is made, and then the claimed method generates a limited-use payment information for that particular selected payment method that is used in place of the selected payment information. EX1001, 19:9-12.

The “limited-use payment information,” which is used in place of issuer provide payment information, is then transmitted from the electronic device via NFC interface and a status of the transaction is visually conveyed on the device’s touch screen display. EX1001, 19:13-16.

The various cryptographic techniques of the ’579 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 8 references in its Grounds (Collinge, Lin, Phillips, Kranzley, Smith, Abbye, Pisula, and Fadell). In each of Petitioner’s Grounds, Petitioner relies upon Collinge as the primary reference (and as relevant to this POPR) for similar elements in the independent claims of the ’579 Patent.

More particularly, in Ground 1, Petitioner presents the combination of Collinge in view of Lin and Phillips to challenge independent claims 1 and 19 and dependent claims 2-3, 7, 10-12, 20 and 23. Pet., 19-63. In Ground 2, Petitioner relies upon Collinge in view of Lin, Phillips, and Kranzley to challenge dependent claims

5-6. Pet., 64-68. In Ground 3, Petitioner relies upon Collinge in view of Collinge, Lin, Phillips, Smith, and Kranzley to challenge dependent claims 4, 21, and 22. Pet., 70-82. In Ground 4, Petitioner relies upon Collinge in view of Lin, Phillips, and Aabye to challenge dependent claims 8-9. Pet., 82-88. In Ground 5, Petitioner relies on Collinge in view of Lin and Aabye to challenge independent claim 15 and dependent claims 16-18. Pet., 89-91. In Ground 6, Petitioner relies on Collinge in view of Lin, Phillips, Aabye and Pisula to challenge dependent claim 13. Pet., 91-96. In Ground 7, Petitioner relies upon Collinge in view of Lin, Phillips, Aabye, Pisula, and Fadell to challenge dependent claim 14. Pet., 96-101.

Patent Owner provides an overview of Collinge, which fails to disclose key elements that are dispositive of this POPR, in this Section III. Patent Owner then explains in the following sections how Petitioner's Grounds using this reference fail to demonstrate a reasonable likelihood of success than any Challenged Claim is unpatentable as obvious over the relied-upon prior art.

A. Collinge

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 to perform its methods. 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].

Per Collinge, this problem is solved 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 storage of the payment credentials. EX1004, [0068]. Collinge describes the payment credentials as “common payment credentials 202 [that] may include *all* data elements common to *any* type of payment transactions, such as both mag stripe and m/chip payment transactions.” EX1004, [0049] (emphasis added). 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 (*i.e.*, both of the cryptogram and the payment credentials are transmitted together). EX1004, [0070] (emphasis added). Based on

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

IV. 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.

V. ARGUMENT

A. Petitioner Fails to Meet Its Burden of Showing That Any of Its Proposed Combinations Disclose “Using Said Limited-Use Payment Information in Place of Said Card Issuer Supplied Payment Information”

Each of Petitioner's Grounds includes the same fundamental flaw: Petitioner fails to show that its proposed obviousness combinations include using limited-use payment information *in place of* card issuer supplied payment information as required by independent claims 1, 15, and 19 of the '579 Patent:

1. 1(e), requiring “generating, by the processor, a limited-use payment information, and *using said limited-use payment information in place of said card issuer supplied payment information;*”

EX1001, claim 1 (emphases added),

2. 15(d), requiring “generating a limited-use number at said electronic device, and *using said limited-use number in place of at least a portion of selected account issuer payment information;*”

EX1001, claim 15 (emphasis added),

3. 19(h), requiring “responsive to receiving an NFC transaction payment request, *generating a limited-use payment information for use in place of card issuer payment information,*”

EX1001, claim 19 (emphasis added).

1. **All of the Challenged Independent Claims Require That the Generated Limited Use Information Be Used “In Place Of” Issuer Payment Information**

Petitioner asserts that each of the three independent claims are obvious over a combination of references, with Collinge as the primary reference in each Ground. Pet., 19, 55, 89. In particular, Petitioner asserts that independent claims 1 and 19 are obvious over Collinge in view of Lin and Phillips (Ground 1), and that independent claim 15 is obvious over Collinge in view of Lin and Aabye (Ground 5). Pet., 19, 55, 89. Petitioner adds additional references for its Grounds challenging certain dependent claims.

Independent claim 1 recites:

[1pre] A method of performing a transaction, the method comprising:

[1a] receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user and

[1b] *wherein the electronic device comprises:*

a processor; a touch screen display coupled to the processor; and a near field communications (NFC) interface coupled to the processor;

[1c] receiving a request for a transaction payment at said electronic device via the NFC interface;

[1d] displaying, on the touch-screen display, images of:
a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card;

[1e] *generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information;*

[1f] transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and

[1g] visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.

EX1001, claim 1 (emphasis added).

At the relevant portions, claim 1 requires an “electronic device” which “comprises a processor” (element [1b]) wherein the processor is configured to “display[] ... a card issuer payment method selection” which “include[es] a last 4-

digit partial number of a card issuer supplied account number of a payment card” (element [1d]) and “generat[e]” a “limited-use payment information” which is used “*in place of said* card issuer supplied payment information” (element [1e]). EX1001, claim 1 (emphasis added). Because “said card issuer supplied payment information” (element [1e]) finds its antecedent basis in “a card issuer payment method selection” (element [1d]) (*infra*, Section V(A)(2)(c)), the generated limited-use payment information is used in place of that “card issuer payment method selection” which is, at least, a number with five or more digits (because it “includ[es] a last 4-digit partial number of a card issuer supplied account number”). EX1001, claim 1.

Independent claim 15 recites:

[15pre] A method of performing a transaction, the method comprising:

[15a] receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient proximity communication request to an NFC interface of the electronic device;

[15b] displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device;

[15c] receiving, from a valid device user, a payment selection and approval authorization input on the electronic device;

[15d] *generating a limited-use number at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and*

[15e] transmitting said limited-use number from said electronic device to a transaction recipient via the NFC interface;

[15f] obtaining a user payment approval through at least one user-interface of the electronic device, of a set of user-interfaces comprising: a touch-screen interface of the touch-screen display user-interface; a touch ID button; input buttons; a touch key-pad; an optical sensor array; a sensor array operable to recognize a swiping of a recognized user skin over the sensor array; a motion detection unit; an accelerometer; a biometric user-sensor;

[15h] a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user while the electronic device is coming within proximity contact of an NFC recipient;

[15i] displaying on said display at least one of a set of information comprising: transaction information;

merchant information; a time; a location of the transaction;
a payment bank logo; a card issuer icon; a payment card
image; an amount; and

[15j] receiving a user input providing for at least one
transaction action, from a set of actions comprising:
approving a transaction; denying a transaction; and
adjusting a transaction.

EX1001, claim 15 (emphasis added).

Like independent claim 1, at the relevant portions, independent claim 15
discloses “generating a limited-use number at said electronic device, and using said
limited-use number in place of at least a portion of selected account issuer payment
information” (element [15d]).

Independent claim 19 recites:

[19pre] An electronic device comprising:

[19a] at least one processor;

[19b] a memory coupled to the at least one processor; a
display operable to present a visual user-interface
comprising device inputs; display output; a device input;
an NFC interface operable to receive a transaction request
when in proximity to an NFC recipient;

[19c] wherein the processor is operable to execute a
program to implement a method comprising:

[19d] accepting a priming action of the electronic device by an identified device user, from the device input;

[19e] enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user;

[19f] displaying a summary of selectable payment account options on the display;

[19g] receiving a payment selection and approval authorization from a valid device user via the device input; and

[19h] responsive to receiving an NFC transaction payment request, *generating a limited-use payment information for use in place of card issuer payment information,*

[19i] wherein the NFC interface is operable to transmit said payment information from said electronic device to the NFC recipient of the transaction; and

[19j] wherein further the processor is operable to cause the display to visually convey a status of the transaction.

EX1001, claim 19 (emphasis added).

Like independent claims 1 and 15, at the relevant portions, independent claim 19 discloses “generating a limited-use payment information for use in place of card issuer payment information” (element [19h]). EX1001, claim 19.

In sum, although all three independent claims use slight linguistic variations, relevant to this POPR, all three challenged independent claims disclose generating limited-use information that is used “*in place of*” issuer provided payment information. As explained below, Collinge fails to disclose this.

2. Collinge Does Not Disclose Using Limited-Use Information “In Place Of” Issuer Payment Information

Petitioner asserts that Collinge in view of Lin and Phillips (Ground 1) renders independent claims 1 and 19 (and others) obvious. Pet., 19. Petitioner also asserts that Collinge in view of Lin and Aabye (Ground 5) renders the sole additional independent claim, claim 15 (and others) obvious. Pet., 89. For each independent claim challenged, Petitioner relies solely on Collinge for the disclosure of generating limited-use payment information that is used in place of issued provided payment information. Pet., 41-42 (relying solely on Collinge for the alleged disclosure of element [1e]); 62 (referring back to elements [1c] and [1e] for [19h], *i.e.*, relevant to the “in place of” requirement, relying on the same disclosure in Collinge for the alleged disclosure of [19h]); 89 (referring back to element [1e] for [15d]). In other words, Petitioner provides no independent analysis for elements [15d] or [19h], and relies exclusively on its discussion of Collinge with respect to element [1e] for every Challenged Claim. Patent Owner thus focuses its analysis in this POPR on element [1e] as representative of Petitioner’s failures across all claims.

Petitioner asserts that Collinge's disclosure of a "payment cryptogram [that] is 'valid for a single financial transaction'" qualifies as limited-use information for element [1e]. Pet., 41 (citing EX1004, Abstract, [0128], Fig. 16). At multiple junctures, Petitioner equates this payment cryptogram with a dynamic card validation code ("CVC3"). Pet., 41 ("It was well-known at the time that an application cryptogram and CVC3 are dynamically generated alternatives to the static card issuer CVC"), 42 ("Collinge teaches generating a payment cryptogram such as a CVC3").

In support of its assertions regarding Collinge for element [1e], Petitioner points to Collinge's Abstract, paragraphs [0041], [0043], [0070], [0077], [0128], and [0145] and Figure 16. Pet., 41-42. But as discussed below, nowhere in the relied-upon portions in Collinge, and indeed nowhere in Collinge, is limited-use payment information used "**in place of said** card issuer supplied payment information" as required by element [1e]. Instead, Collinge consistently discloses that the generated cryptogram/CVC3 is used in addition to (and not instead of) issuer provided payment information. Moreover, Petitioner does not argue, much less show, that the CVC3 of Collinge is used in place of "a card issuer payment method" which includes at least a 5-digit number, as required by independent claim 1.

Patent Owner addresses these failures below.

a. Collinge Does Not Disclose Using a Cryptogram or CVC3 in Place of Anything, Let Alone Issuer Payment Information as Required by All Challenged Claims

All three challenged independent claims require generating limited-use information that is used “*in place of*” issuer provided payment information. EX1001, claims 1, 15, and 19; *supra* Section V(A)(1). But none of the portions of Collinge relied upon by Petitioner disclose using a CVC3 (or other cryptogram) in place of issuer provided payment information. And, in fact, as discussed below, the entirety of Collinge discloses only *adding* a CVC3 (or other cryptogram) to payment credentials. Collinge never discloses using any information “in place of” of any issuer payment information whatsoever. This is dispositive of every Ground in the Petition.

Notably, as Petitioner seemingly concedes—and as discussed below—Collinge does ***not*** actually disclose that the payment cryptogram (CVC3) is used in place of anything (let alone the “CVC” that Petitioner equates with “said card issuer supplied payment information”). Pet., 41-42. Indeed, Petitioner argues only that it was allegedly “well-known” to do so. Pet., 41. This is made plain by a review of the portions cited by Petitioner and its corresponding assertions regarding the same.

Patent Owner explains in this section first, the problems with the portions of Collinge relied upon by Petitioner, and second, that Collinge consistently (and exclusively) discloses *adding* payment credentials and a cryptogram together (and

never using any information in place of anything else, let alone in place of issuer payment information).

To begin, Petitioner points to disclosure regarding Figure 1 to assert that Collinge discloses its mobile payment application is “‘stored in data storage of the mobile device 104 and executed by a processor included in the mobile device 104.’” Pet., 41 (quoting EX1004, [0041]; emphasis omitted). Petitioner also asserts that “[t]he payment cryptogram is generated ‘using the generating key included in the single use key’ that was previously provisioned to the mobile device.” Pet., 41 (citing EX1004, [0077], [0043]). Tellingly, Petitioner does not point to anything in Collinge that discloses that the CVC3 (or any generated cryptogram) is used in place of anything (or even allege as much). *See* Pet., 41-42.

Petitioner also points to Collinge at its Abstract, paragraph [0128], and Figure 16 to argue that Collinge discloses the generation of a cryptogram/CVC3 that is “‘valid for a single financial transaction.’” Pet., 41. Here too, however, Collinge says nothing about using the cryptogram/CVC3 in place of anything (nor does Petitioner so allege). For example, Collinge’s Abstract recites:

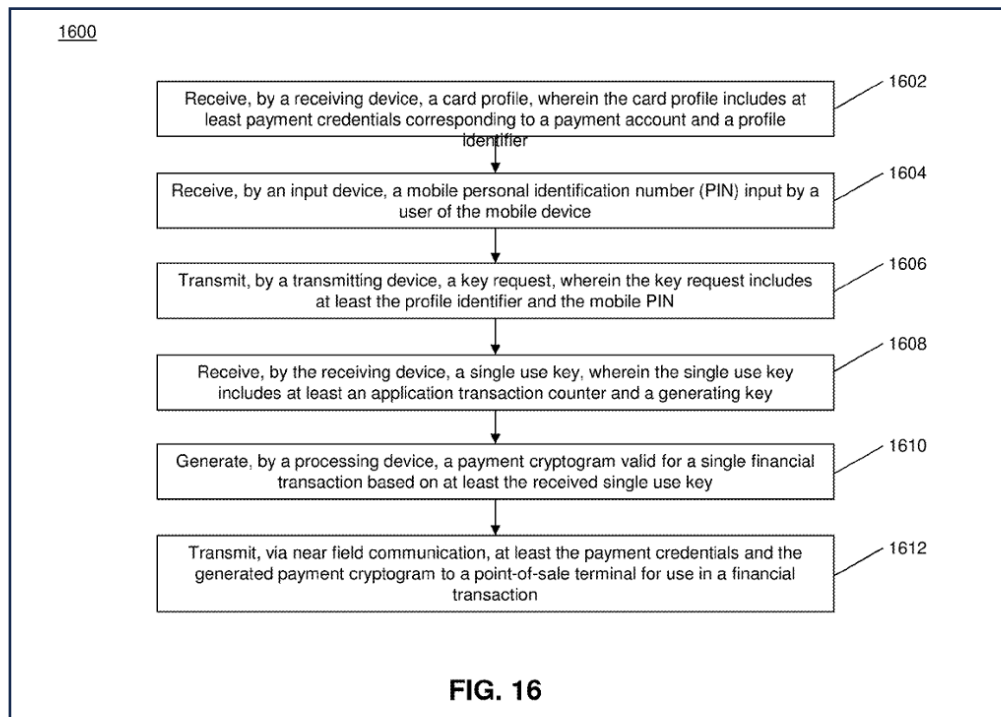
A method for generating and provisioning payment credentials to a mobile device lacking a secure element includes: generating a card profile associated with a payment account, wherein the card profile includes at least payment credentials corresponding to the associated

payment account and a profile identifier; provisioning, to a mobile device lacking a secure element, the generated card profile; receiving, from the mobile device, a key request, wherein the key request includes at least a mobile identification number (PIN) and the profile identifier; using the mobile PIN; generating a single use key, wherein the single use key includes at least the profile identifier, an application transaction counter, and a generating key for use in generating a payment cryptogram *valid for a single financial transaction*; and transmitting the generated single use key to the mobile device.

EX1004, Abstract (emphasis added to show quoted portion of Collinge from page 41 of the Petition). As can be seen from the above, Collinge's Abstract says nothing about using any information "in place of" anything else (nor does Petitioner so allege, focusing only the "valid for a single financial transaction" statement). Similarly, paragraph [0128] includes the same quotation ("valid for a single financial transaction"), EX1004, [0128], which Petitioner string cites for the same proposition. Pet., 41.

As to Figure 16 (reproduced below), it discloses a method for generating a payment cryptogram (here too, Petitioner again focuses on the single financial transaction statement). EX1004, [0131]. In Figure 16, a card profile is sent from a first remote device to a mobile device, which profile includes payment credentials, like payment account information and profile identifiers. EX1004, [0132]. The

mobile device then generates “a payment cryptogram valid for a single payment transaction.” EX1004, [0135]; *see also* Pet., 41 (focusing on same). Then, “at least the payment credentials and the generated payment cryptogram” are **both** transmitted “for use in a financial transaction.” EX1004, [0135], FIG. 6 (step 1612).



EX1004, FIG. 16.

Petitioner also alleges that “Collinge teaches generating a payment cryptogram such as a CVC3 based on at least Collinge’s processor cryptographically combining: ‘the supplied CVC3 value, the session key unpredictable number [(KSUN)], the application transaction counter, and the reader unpredictable number.’” Pet., 42 (citing EX1004, [0145]). However, there is no indication that this generated cryptogram is used **in place of** issuer provided payment information. The

cited disclosure merely reflects the process in Figure 18 for “generating a dynamic card validation code (CVC3) value in a mobile device (e.g., mobile device 104) lacking a secure element.” EX1004, [0142]; *see also* [0143]-[0145] (discussing steps of Figure 18). Collinge discloses that “the processing device may generate a payment CVC3 value based on at least the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” EX1004, [0145]. Then, “the generated payment CVC3 value and the application transaction counter may be transmitted, via near field communication, to the point-of-sale terminal 120 *for including in an authorization request* in a financial transaction.” EX1004, [0145] (emphasis added). There is no indication that this generated value is used in place of issuer provided payment information; instead, it is “includ[ed]” in an “authorization request.” EX1004, [0145]. All Collinge discloses, with respect to Figure 18, is the generation of the CVC3. But as discussed above and below, the CVC3 is used *with* payment credentials (not “in place of” anything). For example, Collinge elsewhere describes this “authorization request”: when mobile device 104 transmits a cryptogram and payment credentials to point-of-sale terminal 120, the point-of-sale terminal may then transmit to an acquirer 122 “an authorization request” (as part of “processing of a financial transaction”). *See, e.g.*, EX1004, [0044]-[0045], FIG. 1. And notably, Collinge does not use the term CVC (or the related term CVV) at all and never

discusses any replacement, *see generally* EX1004, which further confirms it does not actually disclose using a CVC3 in place of a CVV (or anything else).

As one final point to Petitioner's reliance on portions of Collinge: not only does Petitioner point to nothing in Collinge that supports the concept that a cryptogram is used in place of anything, Petitioner all but admits it does *not*. Petitioner includes a two-sentence argument that "complete payment information including payment credentials + the generated payment cryptogram" is also limited-use information that is then allegedly "used in place of the card issuer supplied payment information (e.g., complete payment credentials including a PAN+CVC)." Pet., 42. But this only serves to confirm that Collinge discloses *adding* a cryptogram *together with* the card issuer supplied payment information, not using the cryptogram in place of such card issuer supplied payment information. Moreover, there is nothing used in place of anything in this scenario. The payment credentials are still used in their entirety; the cryptogram is simply added as well. That is the opposite of using limited-use payment information *in place of* card issuer supplied payment information, as required by the claims (*i.e.*, the card issuer supplied payment information is *still* used).

To attempt to overcome the clear defects in Collinge's actual disclosure, Petitioner's only retort is to assert that "[i]t was well-known at the time that an application cryptogram and CVC3 are dynamically generated alternatives to the

static card issuer CVC.” Pet., 41. However, just because something was allegedly “well known” does not in any way demonstrate that the cryptogram (CVC3) in Collinge would have been substituted for a CVC, nor does it provide any motivation as to why (or how) a POSITA would have done so in Collinge’s system, which is itself a complete system for secure transactions (including building in user-identification biometrics and the like, which already prevents fraudulent use by an authorized party, *see, e.g.*, EX1004, [0081], [0139], [0143]). There is simply no reason (or showing) as to why such an undisclosed replacement would be made—especially when Collinge consistently discloses *adding* a CVC3 to payment credentials. At best, Petitioner appears to have improperly used the ’579 Patent as a blueprint in its Grounds. *See also, e.g., Ecolochem, Inc. v. S. Cal. Edison Co.*, 227 F.3d 1361, 1372 (Fed. Cir. 2000) (“In this case, the district court used the [] patent as a blueprint, with the Houghton process as the main structural diagram, and looked to other prior art for the elements present in the patent but missing from the Houghton process. The district court opinion does not discuss any specific evidence of motivation to combine, but only makes conclusory statements. ‘Broad conclusory statements regarding the teaching of multiple references, standing alone, are not evidence.’”) (cleaned up); *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1361 (Fed. Cir. 2019) (“We repeatedly expressed concerns that crediting such testimony risks allowing the challenger to use the challenged patent as a roadmap to reconstruct

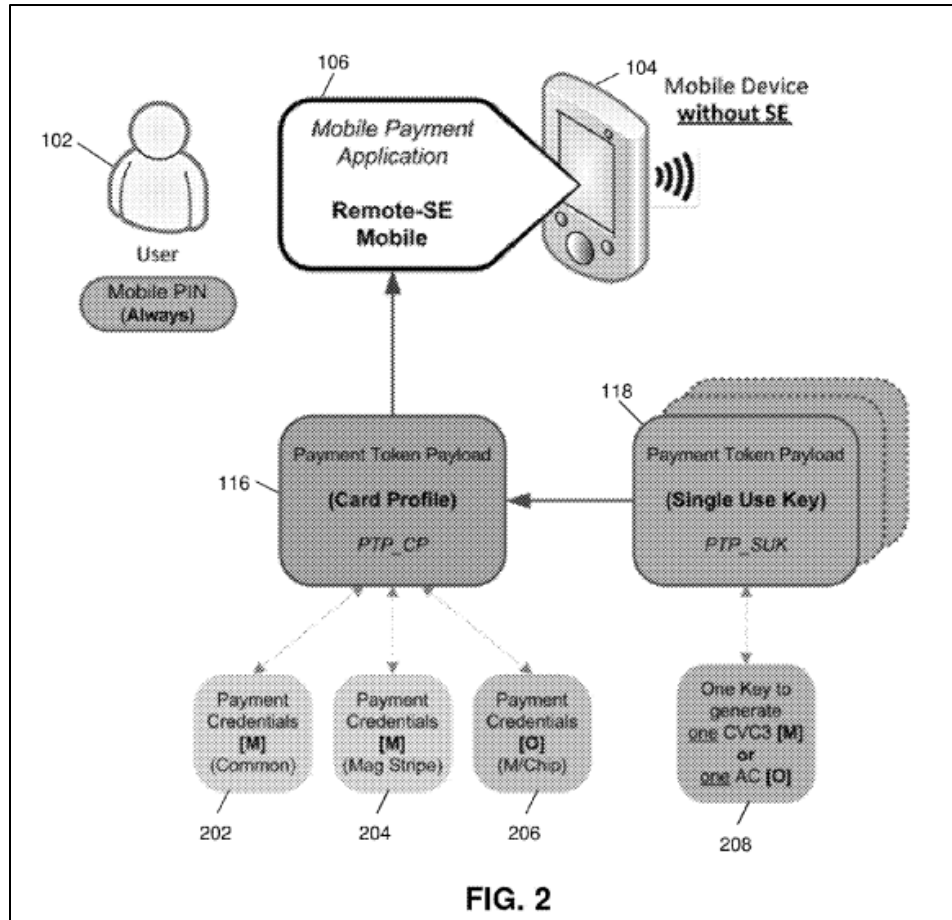
the claimed invention using disparate elements from the prior art - i.e., the impermissible *ex post* reasoning and hindsight bias that *KSR* warned against.”).

And even assuming others substituted a CVC with a CVC3 (which Patent Owner does not concede), that is irrelevant here. To assert that its proposed combinations disclose this limitation, Petitioner relies solely on the disclosure of Collinge, which does *not* disclose that the cryptogram replaces any information during the financial transaction. Instead, a review of Collinge confirms that it consistently discloses transmitting **both** the “cryptogram **and** payment credentials” together. EX1004, [0070] (emphasis added), [0044] (same). Collinge also explains that its disclosed payment credentials are “*static* payment credentials” that are “associated with a payment account.” EX1004, [0013] (“The provisioning device is configured to provision, to the mobile device, at least the storage key, an authentication component, and static payment credentials, wherein the static payment credentials are associated with a payment account.”); *see also* EX1004, [0014] (“static payment credentials” are used); [0138] (“static payment credentials may be provisioned to the mobile device 104, wherein the static payment credentials are associated with a payment account”); [0143] (“In step 1802, at least a storage key, authentication component, and static payment credentials may be received by a receiving device. In step 1804, at least one additional credential may be received by an input device (e.g., of the mobile device.”); cl. 20 (“static payment credentials are

associated with a payment account”); [0042] (“The user 102 may have a payment account with an issuer 108, such as a credit card account. The user 102 may desire to use their mobile device 104 to conduct payment transactions using their payment account with the issuer 108 for funding of the transactions. Payment credentials corresponding to the payment account may be stored by a remote-SE (remote secure element) system 110 for provisioning to the mobile device 104.”).

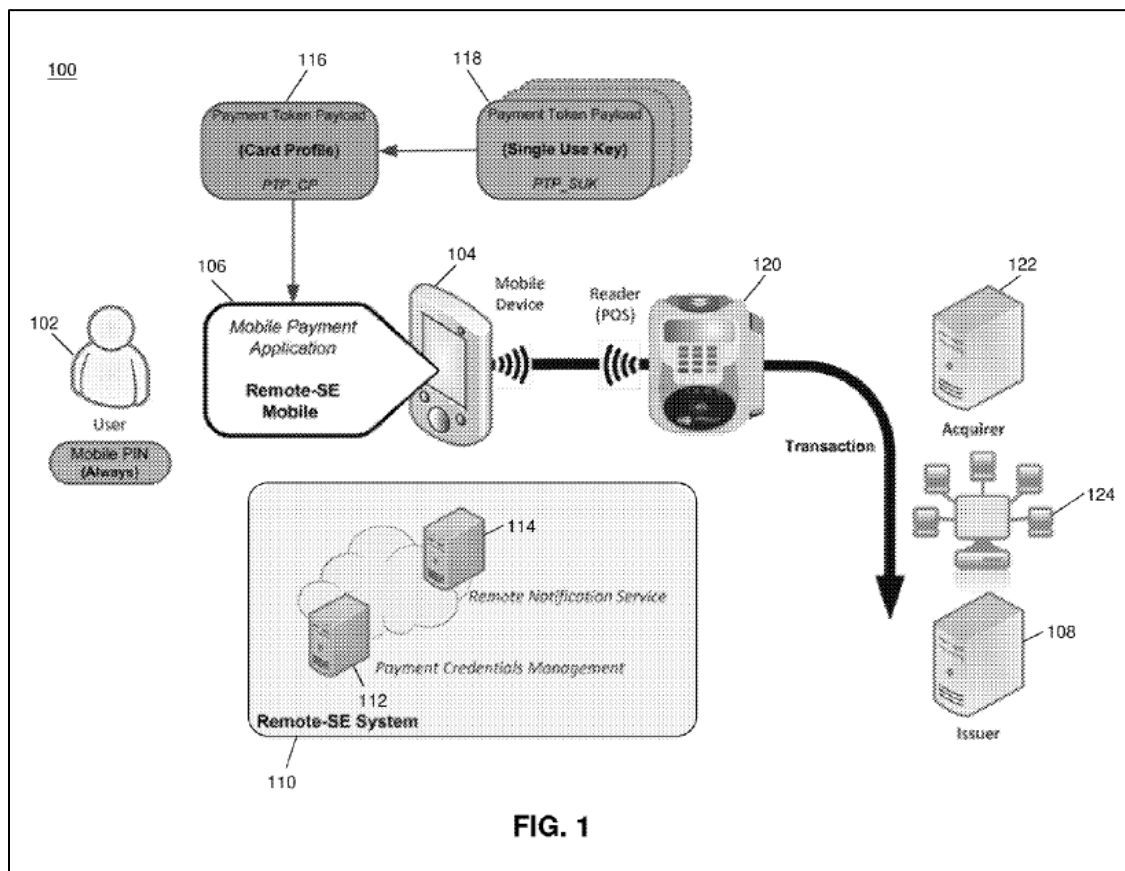
Collinge further discloses that “card profile 116 may include common payment credentials 202, magnetic stripe (mag stripe) payment credentials 204, and m/chip payment credentials 206.” EX1004, [0048]; FIG. 2 (depicting same, below). Collinge continues to explain that “common payment credentials 202 may include *all* data elements common to *any* type of payment transactions, such as both mag stripe and m/chip payment transactions” and that “[s]uch data elements may include payment account number, tracking number, and card layout description data.” EX1004, [0049] (emphasis added); *see also id.* (discussing mag stripe and m/chip transactions); *see also* [0037]-[0038] (describing “Payment Account” and “Payment Card”); Abstract (“generating a card profile associated with a payment account, wherein the card profile includes *at least* payment credentials corresponding to the associated payment account and a profile identifier”) (emphasis added); [0007]-[0008], [0043], [0048], [0068], [0074], [0127] (disclosing same). Indeed, Collinge consistently discloses that the cryptogram is *added to* the payment credentials; it

never discloses that the cryptogram is used in place of anything else. This is illustrated, for example, in Figure 2, below, which shows “the payment token payload provision[s] to the mobile device 104 in additional detail.” EX1004, [0047]. In Figure 2, the common payment credentials (202, 204, 206) are part of the card profile (116) and sent, along with the single use key (118), to the mobile device (104). EX1004, [0047]-[0051]. Nowhere here—or elsewhere—does Collinge disclose (or depict) using anything in place of anything else.



EX1004, FIG. 2.

Figure 1, reproduced below, similarly discloses that “mobile device 104 may be further configured to transmit a generated payment cryptogram **and** payment credentials to a point-of-sale terminal 120 at a merchant” (*i.e.*, again, there is nothing using in place of anything else disclosed in Collinge). EX1004, [0044]; *see also* [0039]-[0046] (describing Figure 1), [0070] (explaining same in context of Figure 5).



EX1004, FIG. 1.

Further demonstrating the problems with Petitioner’s assertions, according to Petitioner, a CVC number is a “*static*” number associated with “a traditional

payment card,” Pet., 41, 70 (emphasis added), the same sort of “static payment credentials” discussed above, that, per Collinge, are sent (along with the cryptogram) in each transaction. Also, as discussed above, such “static payment credentials” are, as Collinge explains, “common to any type of payment transactions.” EX1004, [0049]. In other words, Collinge does *not* disclose using the CVC3 to replace a CVC. Instead, as explained, Collinge discloses sending the CVC3 *together with* the issuer provided information (logically, as discussed, the disclosed “static payment credentials” such as a CVC and account number), to complete the transaction. Furthermore, Petitioner does not combine Collinge with any other pieces of art to meet this limitation, nor does Petitioner offer any reason why a POSITA would fundamentally change Collinge to replace the CVC (or any payment information).

In sum, Petitioner fails to show that Collinge discloses the generation of limited-use information that is used in place of issuer provided payment information, which is dispositive of Petitioner’s Grounds (and the Petition as a whole).

b. Collinge Does Not Disclose Using the Cryptogram or CVC3 in Place of a Card Number With 5 or More Digits as Required by Independent Claim 1

Even assuming that Petitioner is correct (which Patent Owner does not concede and Petitioner has failed to show) in asserting that “[i]t was well-known at the time that an application cryptogram and CVC3 are dynamically generated alternatives to a card issuer CVC” and that a POSITA would have been motivated

to modify, and had a reasonable expectation in modifying Collinge to replace a CVC with a CVC3 (which Petitioner has failed to do), Collinge still does not disclose using generated information “in place of said card issuer supplied payment information” as required by element [1e]. EX1001, claim 1. In particular, Petitioner does not (and cannot) allege that Collinge replaces a number with 5 or more digits with the generated information, as claim 1 requires. *See* Pet., 41; EX1001, claim 1.

Independent claim 1 recites (in part):

[1d] *displaying*, on the touch-screen display, images of:
a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card;

[1e] generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of *said card issuer supplied payment information*;

EX1001, claim 1 (emphasis added).

Claim 1 discloses the generation of a “limited-use payment information” used “in place of said card issuer supplied payment information.” EX1001, claim 1. The use of the word “said” indicates that the term “card issuer supplied information” refers back to a previously disclosed information. *See Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1315 (Fed. Cir. 2023) (“[T]he use of the term ‘said’ indicates

that this portion of the claim limitation is a reference back to the previously claimed ‘term’) (quoting *Summit 6, LLC v. Samsung Elecs. Co., Ltd.*, 802 F.3d 1283, 1291 (Fed. Cir. 2015)). The only previously recited “*card issuer supplied information*” in claim 1 is the “*a card issuer payment method*” (e.g., a credit card number) which must “includ[e] a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card.” EX1001, claim 1.¹ Therefore, the antecedent basis for “said card issuer supplied payment information” is the previously recited “card issuer payment method” which must include (amongst other things) a “4-digit partial number of a card issuer supplied account number of a payment card.” EX1001, claim 1. It follows that the “card issuer payment method” must be (at least in part) a number with 5 or more digits because the 4-digit number that it includes is described as a “*partial number*.” EX1001, claim 1 (emphasis added). In sum, to meet the limitations of claim 1, the dynamically generated limited-use information must be used in place of a number with 5 or more digits.

¹ Antecedent basis need not be explicit, it can also be implicit. *Energizer Holdings, Inc. v. Int’l Trade Comm’n*, 435 F.3d 1366, 1371 (Fed. Cir. 2006). The use of slightly different language does not affect how the claim should be read.

But, as discussed above, *supra* V(A)(2)(A), Petitioner relies exclusively on Collinge’s generation of a cryptogram/CVC3, not just any type of replacement information, to meet the limitations of claim 1. *See* Pet., 41. Petitioner argues that “[i]t was well-known at the time that an application cryptogram and CVC3 are dynamically generated *alternatives to the static card issuer CVC* found on the back of a traditional payment card” and therefore Collinge discloses replacing the CVC with the CVC3. Pet., 41 (emphasis added). Petitioner’s expert also explains the limitations of CVC/CVC3 values: “the dynamic code is a *three or four digit code* that may be used in place of a ‘CVV’, ‘CVC’ or other code (a code generally used in payment card systems and used to verify that a cardholder was in possession of a payment card during a transaction).” EX1003 ¶172 (emphasis added). But, the issuer supplied information that is replaced in independent claim 1 cannot be an issuer supplied CVC or CVV because the information to be replaced includes *at least* a 5-digit number. EX1001, claim 1. Therefore, even if Petitioner is correct that a POSITA would know that a CVC3 is used “in place of” a CVC (it is not), the elements of claim 1 are not met (and its dependents as well).

3. Petitioner’s Other Grounds Fail for the Same Reason

Petitioner asserts that dependent claims 5-6 are obvious over Collinge in view of Phillips, Lin, and Kranzley (Ground 2), that dependent claims 4, 21, and 22 are obvious in view of Collinge, Lin, Phillips, Smith, and Kranzley (Ground 3), that

dependent claims 8-9 are obvious over Collinge in view of Phillips, Lin, and Aabye (Ground 4), that dependent claim 13 is obvious over Collinge in view of Lin, Phillips, Aabye and Pisula (Ground 6), and that dependent claim 14 is obvious over Collinge in view of Lin, Phillips, Aabye, Pisula, and Fadell (Ground 7). Each of these Grounds relies on Collinge for the disclosure of using limited-use information in place of issuer provided payment information. As discussed above, in Section V(A)(2)(b), Collinge does not disclose using limited-use information **in place of** issuer provided payment information. Therefore, Petitioner fails to meet its burden for Grounds 2-4 and 6-7 for the same reason as Grounds 1 and 5.

VI. PETITIONER OMITTS ITS CONTRADICTORY DISTRICT-COURT INDEFINITENESS ARGUMENTS THAT CLAIM SCOPE ALLEGEDLY CANNOT BE ASCERTAINED

In its IPR Petition, Petitioner purports to “adopt[]” Patent Owner’s constructions for two terms “[f]or purposes of this proceeding *only*,” and “Petitioner applies the plain and ordinary meaning of all claim terms as understood by a POSITA” for everything else. 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 asserts one of the terms it seeks to “adopt[]” Patent Owner’s construction (without analysis) is indefinite. EX2016 at 24-26; EX2018 at 14-15; EX2020 at 3. In particular, Petitioner also asserts as part of its district-court claim-

construction that “the method of claim 1 wherein a payment processing authority verifies a limited-user number ... [a]nd rejecting a limited use number” renders claim 6 indefinite. EX2016 at 24-26; EX2018 at 14-15; EX2020 at 3. The district court has now rejected Petitioner’s arguments (*see* EX2023, 4), but regardless, Petitioner’s positions are completely 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 claim is indefinite in district court, and on the other hand, tell the Board that it is amenable to an obviousness challenge, in Petitioner’s words, “[f]or purposes of this proceeding only.” Pet., 5-6. Worse, Petitioner does not even inform the Board about its inconsistent positions.

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 certain claims as the need suits and seeking to adopt (without analysis or support) a construction it believes to be incorrect. *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.”).

VII. CONCLUSION

For the foregoing reasons, the Board should deny institution of the proceeding.

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 6,697 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)