

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INCORPORATED AND MASTERCARD
INTERNATIONAL INCORPORATED.,

Petitioner,

v.

OV LOOP, INC.,

Patent Owner.

Case IPR2023-01289
Patent 10,032,171

PATENT OWNER'S RESPONSE TO THE PETITION

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I. Introduction	1
II. Background	1
III. Person of Ordinary Skill in the Art	4
IV. Petitioner Relies on Portions of Collinge and the Collinge Provisional that are Not Prior Art.....	5
V. Grounds 1 and 2 do not establish that any of claims 1-33 are anticipated by Collinge or rendered obvious by Collinge in view of the knowledge of a POSITA	13
A. Collinge does not anticipate or render obvious claim 1 (or 17)	13
1. Collinge does not disclose or render obvious a “request [for] data associated with the account” (limitation 1.A-3)	13
2. Collinge does not disclose or render obvious a “non- permanent cryptographic key associated with the account” (limitation 1.C)	18
3. Collinge does not disclose or render obvious “the first set of data associated with the account usable by the application to formulate an application protocol data unit response” (limitation 1.C)	20
4. Collinge does not disclose or render obvious “wherein the response cryptogram does not include the local cryptographic key”	22
5. Collinge does not disclose or render obvious a “device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account”	25
B. Collinge does not anticipate or render obvious Claim 10 (or 27)	30
1. Collinge does not disclose or render obvious determining a current non-permanent	

cryptographic key associated with the account using the account identifier	34
2. Collinge does not disclose or render obvious “calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account”	35
C. Collinge does not disclose or render obvious claim 8	37
1. Collinge does not disclose “at the remote computer system ... sending the first non-permanent cryptographic key and the account identifier to the mobile device” (claim 8.A).....	37
2. Collinge does not disclose “after the interrogation, generating the second non-permanent cryptographic key at the remote computer system, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.”	39
D. Collinge does not anticipate or render obvious claim 4 (or 21)	41
1. Collinge does not “wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification” (claims 4 and 21).....	41
E. Collinge does not anticipate or render obvious claim 15 (or 32)	43
1. Collinge does not disclose or render obvious an “application is configured to generate the response cryptogram according to a card specification” (claims 15 and 32)	43
F. Collinge does not anticipate or render obvious claim 6 (or 22)	45

1. Collinge does not disclose or render obvious “generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.”	45
G. Collinge does not anticipate or render obvious claim 16 (or 33)	46
1. Collinge does not disclose or render obvious “wherein the first and second non-permanent cryptographic key are associated with an issuer master key.” (claim 16 and 32)	46
H. Collinge does not anticipate or render obvious claims 17, 24, 25	49
VI. Grounds 3 and 4 do not establish that any of claims 1-33 are anticipated by Fiske or rendered obvious by Fiske in view of the knowledge of a POSITA	50
A. Fiske does not disclose or render obvious “sending ... the account identifier to the mobile device” (claims 8, 9)	50
B. Fiske does not disclose or render obvious any of the “remote computer system” steps (Claims 10-13, 27-30)	53
1. No disclosure in Fiske of an authorization request comprising the account identifier	53
2. No disclosure in Fiske of determining a current non-permanent cryptographic key associated with the account using the account identifier	55
3. No disclosure in Fiske of “calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account”	57
C. Fiske does not disclose or render obvious claim 11 (or 28)	58
1. Fiske does not disclose or render obvious an “the set of inputs comprises unpredictable data; the authorization data comprises the unpredictable	

data; and the calculated cryptogram is calculated using the unpredictable data.” (claim 11).....	58
D. Fiske does not anticipate or render obvious claim 12 (or 29)	60
1. Fiske does not disclose “wherein the POS command communications comprise the unpredictable data.” (claims 12 and 29)	60
E. Fiske does not anticipate or render obvious claim 13 (or 30)	61
1. Fiske does not disclose or render obvious “wherein the authorization data further comprises values from the transaction”	61
F. Fiske does not disclose or render obvious claim 1 (or 17)	63
1. No disclosure in Fiske of “wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram”	63
2. Fiske does not disclose or render “at least one response application data protocol unit containing the response cryptogram and an account identifier for the account” (claim 1.E-3)	65
3. “EMV mode Visa transactions” relied upon by Petitioner are not compatible with Fiske (claim 1.E-3)	67
G. Fiske does not disclose or render obvious claims 4 (20) and 5 (21)	72
1. Fiske does not disclose or render obvious “wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification” (claim 4) or “wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device	

response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.” (claim 5)	72
H. Fiske does not disclose or render obvious claim 6 (or 22)	73
1. Fiske does not disclose or render obvious a “generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output.” (claim 6 and 22)	73
I. Fiske does not disclose or render obvious claim 15 (or 32)	74
1. Fiske does not disclose or render obvious a “wherein the application is configured to generate the response cryptogram according to a card specification.” (claims 15 and 32)	74
J. Claims 17, 24, 25	75

TABLE OF AUTHORITIES

Cases

<i>Amgen Inc. v. Sanofi</i> , 872 F.3d 1367 (Fed. Cir. 2017)	6, 7
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	58
<i>Comcast Cable Commc'ns, LLC v. Promptu Sys. Corp.</i> , IPR2018-00345, Paper 10 (P.T.A.B. July 2, 2018)	7
<i>Cox Communications, Inc. v. AT&T Intellectual Property I, L.P.</i> , IPR2015-01227, Paper 70 (P.T.A.B. Nov. 16, 2015)	6
<i>Dominion Dealer Sols., LLC v. AutoAlert, Inc.</i> , IPR2014-00684, 2014 WL 5035359 (P.T.A.B. Oct. 6, 2014)	22
<i>Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.</i> , 800 F.3d 1385 (Fed. Cir. 2015)	6, 7
<i>Ex parte Mann</i> , 2016 WL 7487271 (P.T.A.B. Dec. 21, 2016)	7
<i>Ex parte Yamaguchi</i> , 88 USPQ2d 1606 (BPAI 2008))	8
<i>Gen. Elec. Co. v. Brenner</i> , 407 F.2d 1258 (D.C. Cir. 1968)	8
<i>In re Giacomini</i> , 612 F.3d 1380 (Fed. Cir. 2010)	6, 7
<i>In re Heritage</i> , 182 F.2d 639 (C.C.P.A. 1950)	9

<i>In re Lund</i> , 376 F.2d 982 (C.C.P.A. 1967)	8
<i>Teva Pharmaceuticals, LLC v. Corcept Therapeutics, Inc.</i> , No. 21-1360 (Fed. Cir. 2021).....	17
<i>Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.</i> , 97 F.4th 882 (Fed. Cir. 2024)	58
<i>Yeda Rsch. v. Mylan Pharms. Inc.</i> , 906 F.3d 1031 (Fed. Cir. 2018)	21
 <u>Statutes</u>	
35 U.S.C. § 112	9
35 U.S.C. § 122	7
35 U.S.C. §102	7

TABLE OF EXHIBITS

Exhibit No.	Description
2001	Declaration of Spencer Hosie in support of Motion for <i>Pro Hac Vice</i> Admission
2002	Declaration of Diane S. Rice in support of Motion for <i>Pro Hac Vice</i> Admission
2003	Declaration of Darrell Atkinson in support of Motion for <i>Pro Hac Vice</i> Admission
2004	Wikipedia Article – Host Card Emulation
2005	NFCW Article, “SimplyTapp proposes secure elements in the cloud”, dated Sept. 19, 2012
2006	Android KitKat (https://developer.android.com/about/versions/kitkat)
2007	NFCW Article, “Google gets around the carriers with Host Card Emulation for NFC payments”, dated Oct. 31, 2013
2008	Visa Inc. Press Release - Visa to Enable Secure, Cloud-Based Mobile Payments
2009	Declaration of Dr. Chuck Easttom Ph.D., D.Sc.
2010	Multisystem Technologies, Acquiring: EMV Transaction Flow. Part 4: PDOL and Contactless Cards, Characteristic Features of qVSDC and qUICS, Nov. 22, 2020
2011	Multisystem Technologies, Acquiring: EMV Transaction Flow. Part 3: GET PROCESSING OPTIONS with and without PDOL, Aug. 14, 2020
2012	Bankrate, What is EMV compliance law and should your business worry about it?, Dec. 06, 2023
2013	Minimum EMV Chip Card and Terminal Requirements
2014	Fiserv, What is EMV?
2015	EMVCo, A Guide to EMV Chip Technology, Nov. 2014
2016	SPA, Instant Issuance, A SPA White Paper, Dec. 2013
2017	AlphaCard, What’s the difference between HiCo and LoCo magnetic stripe cards?
2018	SPA, Private Label Payment Systems, Nov. 15, 2011

2019	Payment Card Industry (PCI) Data Security Standard, Oct. 05, 2010
2020	Epordo, Smart Card Technology
2021	MasterCard, M/Chip 4 Issuer Guide to Debit and Credit Parameter Management, Dec. 2004
2022	quick Visa Smart Debit/Credit Intelligent Reader Testing Process, Oct. 2008
2023	NordVPN, Session key definition
2024	Microsoft Learn, Glossary
2025	VISA, Visa Best Practices for Data Field Encryption Version 1.0, Oct. 05, 2009
2026	Cisco, Next Generation Cryptography
2027	Anderson, et al., <i>Serpent: A Proposal for the Advanced Encryption Standard</i>
2028	Anderson, et al., <i>Serpent and Smartcards</i>
2029	FasterCapital, Encryption Techniques For Financial Transactions
2030	New Softwares, How do Banks Encrypt Data?
2031	Enisa, Algorithms, Key Sizes and Parameters Report, Oct. 2013
2032	Global Payments, What is EMV Contactless?, Mar. 06, 2019
2033	SC Media, The long and winding road: EMV Adoption, Jun. 1, 2015
2034	EMV in the U.S. (2020 Update)
2035	Deposition Transcript excerpts of Dr. Stuart Fiske
2036	Discover Financial, Emvco Membership Grows with Discover
2037	CV of Dr. Chuck Easttom Ph.D., D.Sc.

I. Introduction

Patent Owner respectfully requests that the Board find all of Petitioner's challenges to the claims of U.S. Patent No. 10,032,171 ("the '171 patent") without merit. Petitioner relies on references that disclose payment systems that differ markedly from the claims of the '171 patent. In many instances, the Petition ignores those differences and omits critical claim limitations from its analysis. The Petition is also flawed because of its reliance on an unpublished provisional application (Exhibit 1009), which Petitioner improperly uses to support its arguments as to challenged claim limitations not present in the asserted reference.

II. Background

The '171 patent was invented by Douglas Yeager who is a pioneer in the secure payments space who has been widely recognized for his contributions to the field and credited as the inventor of a technique called Host Card Emulation (HCE). EX2004. HCE has been described as a technique that "enables near field communication (NFC) information transfer between a terminal configured to exchange NFC radio information with an NFC card and a mobile device application configured to act or pretend to emulate the functional responses of an NFC card.

HCE requires that the NFC protocol be routed to the main operating system of the mobile device instead of being routed to a local hardware-based secure element (SE) chip configured to respond only as a card, with no other functionality.” EX2004. Mr. Yeager was the founder of a company called SimplyTapp, aimed at commercializing HCE and NFC cloud based payments. EX2005. Mr. Yeager’s HCE technique, has been widely praised in the payment technology industry and was officially adopted into the Android KitKat operating system in 2013. EX2006; EX2007. Even competitors in the payment space, such as Visa, were quick to praise and adopted HCE. “The Android HCE feature provides us with a platform to evolve the Visa PayWave standard, support the development of secure, cloud-based mobile applications, while at the same time offer greater choice to our clients.” EX2008, 1. “Visa's move to enable NFC payments with Android devices is welcome news and will guide the way for the payments industry.” *Id.*, 2.

Mr. Yeager’s company SimplyTapp was later acquired by Patent Owner OV Loop. Using the technology described in the ’171 patent, Patent Owner has been developing software to implement a full digital

wallet solution along with hardware supporting various forms of contactless payments. The '171 patent has been cited in patent applications assigned to companies such as Paypal, Ebay Inc., Intuit Inc., Capital One Services, LLC, Square Inc., and Groupon Inc.. *See, e.g.*, U.S. Patent No. 10,380,577; Intl. Pub. No. WO2009/017754; U.S. Patent No. 10,275,752; and U.S. Patent No. 10,546,444.

The '171 patent teaches and claims a foundational technique for enabling contactless payments using a mobile device. As the specification explains, some payment technologies rely on a microchip called a Secure Element ("SE") embedded into a payment card, cellular phone, or other mobile device. EX1001, 1:34-38. To use a payment card equipped with a Secure Element, an interrogator or reader must interact electrically with the SE. *Id.*, 1:50-52. With conventional secure element payment systems, the user is required to have physical possession of a "card" (e.g., a physical card or a mobile device with a secure element microchip) that matches the authorization capabilities of a merchant's system where a purchase is made. *Id.*, 1:57-60. In this conventional approach, prior to a card being issued, the SE is typically injected with personalization or

“credential” data that is generated from a hardware security module (HSM). EX1002, 804. The HSM typically injects a permanent cryptographic key into the SE that is used throughout the life of the SE. *Id.* During a typical interrogation, a POS terminal sends a command communication to the SE requesting a cryptogram, which the SE generates using the permanent cryptographic key. However, this technique is limited because many mobile devices do not have an SE microchip, and even if they do, the SE may be limited in the number of card specifications or accounts that it can support. *Id.*

III. Person of Ordinary Skill in the Art

The field of technology for the '171 patent is secure payment systems. A person of ordinary skill in the art of the subject matter of the '171 patent would have the equivalent of an undergraduate degree in electrical and computer engineering (or a related field) and approximately two years of work experience in the field of secure payment system. Additional education in the field could be substituted for industry experience, and vice versa.

IV. Petitioner Relies on Portions of Collinge and the Collinge Provisional that are Not Prior Art

Grounds 1 and 2 are legally flawed. The basis for these grounds is U.S. Publication 2013/0262317A1, filed here as Exhibit 1011 (“Collinge”), which was a patent application filed on March 14, 2013. Because Collinge was filed after the August 30, 2012 priority date of the ’171 patent, Petitioner alleges that Collinge is prior art based on its claim of priority to a provisional patent application, filed here as Exhibit 1009 (“Collinge Provisional”), which Petitioner alleges “provide[s] written description support for all elements of at least one independent claim of Collinge.” Pet. 28.¹ The Petitioner includes a chart purporting to map claim 20 of Collinge to the Collinge Provisional. *Id.*, 29-33.

However, to demonstrate that a reference patent application is entitled to the benefit of its provisional application’s filing date for prior

¹ Petitioner also alleges that Exhibit 1010 (referred to as the ’248 Provisional) enables and provides written description support for Collinge. But Petitioner has provided no argument or evidence to support that contention, so Patent Owner does not address it further here.

art purposes, a petitioner must meet two requirements. **First**, a petitioner must show that at least one claim of the reference patent application is sufficiently supported by the provisional application. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1385, 1382 (Fed. Cir. 2015) (“A provisional application’s effectiveness as prior art depends on its written description support for the claims of the issued patent of which it was a provisional.”); *Amgen Inc. v. Sanofi*, 872 F.3d 1367, 1380 (Fed. Cir. 2017) (applying *Dynamic Drinkware* to patent applications).

Second, a petitioner must show that the provisional application provides sufficient support for the subject matter relied upon for prior art purposes in the reference patent application. *See In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010) (relied upon subject matter must be “carried forward from an earlier U.S. provisional application or U.S. non-provisional application”); *Cox Communications, Inc. v. AT&T Intellectual Property I, L.P.*, IPR2015-01227, Paper 70 at 29 (P.T.A.B. Nov. 16, 2015) (“[T]he material relied upon as teaching the subject matter of the challenged claims must be carried through from that earlier filed

application to the reference patent being used against the claim.”) (citing *Giacomini*, 612 F.3d at 1383); *Ex parte Mann*, 2016 WL 7487271, at *5 (P.T.A.B. Dec. 21, 2016) (explaining that “[t]his subject matter test is in addition to the comparison of claims required by Dynamic Drinkware,” and that “absurd results would be reached if a subject matter test were not required”) (emphasis added); *Comcast Cable Commc’ns, LLC v. Promptu Sys. Corp.*, IPR2018-00345, Paper 10 at 25-26 (P.T.A.B. July 2, 2018) (finding Petitioner’s analysis insufficient to show “how the [provisional application] provides support for the subject matter relied upon [in the asserted reference]”). Accordingly, Petitioner must show that the subject matter it relies upon in Collinge is also found in Collinge’s provisional applications. Here, Petitioner fails to do so.

In addition, as the Federal Circuit has recognized, “provisional applications are not themselves prior art under § 102(e)(1) because they are not applications published under § 122(b).” *Amgen Inc. v. Sanofi, Aventisub LLC*, 872 F.3d 1367, fn 5 (Fed. Cir. 2017). As a result, the proponent of a provisional application, in a ground based on § 102(e), must show that “the critical disclosures relied upon in the provisional

application are also present in a corresponding patent, or application published under § 122(b).” *Sequenom, Inc. v. Bd. of Trustees of Leland Stanford Junior Univ.*, IPR2014-00337, Paper 14 at 3-4 (citing *Ex parte Yamaguchi*, 88 USPQ2d 1606, 1612–1614 (BPAI 2008)) (emphasis added).

Any argument by Petitioner that Collinge’s incorporation by reference of the Collinge Provisional changes this requirement is unfounded. If Petitioner were allowed to rely on subject matter found only the Collinge Provisional, this would establish, for the first time, that nonpublic information solely disclosed in a provisional application qualifies as prior art because it is later “incorporated by reference.” This is without precedent and contrary to established law. *In re Lund*, 376 F.2d 982, 991 (C.C.P.A. 1967) (finding that subject matter only in the earlier abandoned application is insufficient for qualification under 102(e) for the patentee not done “all that he could do to make his description public”). Effective incorporation has always been predicated on public disclosure of the incorporated material. *Gen. Elec. Co. v. Brenner*, 407 F.2d 1258, 1262 (D.C. Cir. 1968) (“total incorporation by

reference cannot be accomplished under [35 U.S.C. §] 112 ... is limited to reference to material available to the public.") (emphasis added); *In re Heritage*, 182 F.2d 639, 643 (C.C.P.A. 1950) ("[R]eference to a disclosure which is available to the public is permissible.") (emphasis added).

As admitted by Petitioner's expert, much of the critical subject matter relied upon in the Petition can be found only in the Collinge Provisional. It was not carried forward into Collinge and, therefore, was not publicly available at the time of filing of Collinge. Because Collinge's attempt to incorporate the Collinge Provisional by reference could not—for the purposes of prior art—be effective until its relevant disclosure became publicly available, the disclosures found solely in the Collinge Provisional do not qualify as "described in" Collinge under 102(e).

As the Board recognized in its Institution Decision, there are instances throughout grounds 1 and 2 where Petitioner has cited to the Collinge Provisional in parallel with Collinge. *See, e.g.*, Pet. 40. The Board suggests that these citations could provide sufficient support for the subject matter requirement if the merits of those disclosures are sufficient. ID 19. Here, as explained below, they do not.

Petitioner relies on both subject matter in Collinge that is not carried forward from the Collinge Provisional and, conversely, subject matter in the Collinge Provisional that was not carried forward into Collinge. Patent Owner addresses some examples of these instances below. Additional examples are explained as part of Patent Owner's analysis of individual challenged limitations.

First, as to limitation [1.C] in grounds 1 and 2, Petitioner alleges that a variable called KS_{UN} in Collinge is *associated with the account*.² To support this allegation, Petitioner argues that KS_{UN} uses the account-specific ATC and an account-specific key (KD_{UN}) in its generation. Pet. 43. But, these contentions regarding the ATC and KD_{UN} do not appear in Collinge. Petitioner cites only to the Collinge Provisional. *Id.* (citing EX1009, [0068]-[0071]). Indeed, Petitioner's expert plainly acknowledged that he could not identify any disclosure in Collinge showing how Collinge's KS_{UN} is derived and that Collinge itself lacks the detail for him to understand how KS_{UN} is derived:

² Patent Owner's use of italicized text, other than as part of section headings or citations, is used to indicate recited claim language.

Q: I see. So what you found was that Collinge, Exhibit 1011, by itself does not describe in enough detail for you to understand how KSUN is derived. Right?

A: That's correct. I needed – in order to fully understand, I needed to refer to the provisional, which is, I think, Exhibit 1009.

EX2035 at 78:25-79:7; *see also id.* at 103:10-16. Thus, Petitioner's contentions regarding KS_{UN} being generated using KD_{UN} and the ATC are unsupported by Collinge. The disclosures in the Collinge Provisional that Petitioner relies on (i.e., EX1009, [0068]-[0071]) were not carried forward into Collinge, could not have been ascertained by reading Collinge alone.

Second, as to limitation 1.E-2 in grounds 1 and 2, Petitioner again cites to the Collinge Provisional, but not Collinge itself to support its contention that Collinge discloses *wherein the response cryptogram does not include the local cryptographic key*. Pet. 47 (first full paragraph). Petitioner relies on paragraph [0071] from the Collinge Provisional as evidence of how Collinge calculates the value of CVC3 (the alleged *response cryptogram*). But Petitioner provides no corresponding

disclosure in Collinge, and there is none. As confirmed by Petitioner's expert, Collinge does not disclose how the CVC3 value is calculated. EX2035 at 105:2-5.

Third, as to claim 4, Petitioner alleges that Collinge's reference to "m/chip payment transactions" would be understood by a POSITA "to refer to known EMV-compliant payment system specifications defining sets of inputs and responses." Pet. 54 (citing EX1011, [0044], EX1006 ¶ 117). Petitioner cites to no portion of the Collinge Provisional disclosing "m/chip" or "m/chip payment transactions" and Patent Owner can find no such disclosure in the Collinge Provisional. Thus, Collinge's "m/chip" disclosure is subject matter that was not carried forward from the Collinge Provisional.

V. Grounds 1 and 2 do not establish that any of claims 1-33 are anticipated by Collinge or rendered obvious by Collinge in view of the knowledge of a POSITA

A. Collinge does not anticipate or render obvious claim 1 (or 17)³

1. *Collinge does not disclose or render obvious a “request [for] data associated with the account” (limitation 1.A-3)*

Petitioner alleges that Collinge’s disclosure that “mobile payment application 106 may transmit [a] CAP token to the remote-SE system 100” (EX1011, [0082]) would be understood as a request by the mobile payment application for the server to return payment credentials. Pet. 38-39. This is incorrect. The chip authentication program (CAP) token in Collinge is not a request for data associated with the account. The CAP token’s purpose is simply to authenticate the mobile device. As Collinge discloses, “the mobile payment application 106 may generate a CAP token **used for authentication.**” EX1011, [0081] (emphasis added); *see also id.*, [0139]. Collinge then explains that “additional **authentication credentials**, such as a gesture, a password, or a biometric identifier”

³ In each instance where independent claims 1 or 17 are not anticipated and not rendered obvious, dependent claims 2-16 and 18-30 are also not anticipated or obvious.

may also be supplied. *Id.* (emphasis added). A POSITA would have understood that authentication (or validation) simply means that Collinge's remote-SE system is able to confirm the authenticity of the mobile payment application before proceeding with the subsequent steps of the transaction. Collinge's disclosures regarding generation and return of "payment credentials in an encrypted payload **after** verification of the CAP token," Pet. 42-43 (emphasis added), do not demonstrate a *request for data associated with the account*. Those disclosures simply illustrate the **relative order** of stages. EX2009 ¶84-87.

In addition, the transaction stages relied on in the Petition (stages 3 and 9) are not consecutive, and are in fact separated by several additional stages not involving mobile payment application 106. Between stages 3 and 9, several additional steps are described in Collinge, including: remote-SE system 100 forwarding the CAP token to a CAP token validation service (CTVS) 702 (stage 4); CTVS 702 validating the CAP token (stage 5); sending validation results to payment credentials management system 704 (stage 6); payment credentials management system 704 generating an encrypted payload (stage 7); payment

credentials management system 704 performing a synchronization process with issuer 108, which “may include defining rules for the validity of the values generated by the mobile payment application **106** [and] ... transmitting at least the KS_{UN} , application transaction counter, and UN_{CLOUD} to the issuer **108** for storage in the issuer database” (stage 8a); and transmitting the encrypted payload to the cloud system 302. EX1011, ¶ [0082]–[0085]. Petitioner’s contention that sending a CAP token constitutes a request for a server to return payment credentials is incorrect and unsupported by Collinge. EX2009 ¶85-90.

Petitioner’s further contention that “a POSA would have found it obvious to configure the mobile application to request [a first set of data]” is also unsupported. Pet. 40. Petitioner alleges that it would be “a waste of bandwidth and resources for the issuer to push information regardless of the status of the user device.” Pet. 40-41. But this allegation is irrelevant to why a POSITA would be motivated to modify Collinge, because Petitioner has not shown that Collinge’s method of provisioning data to the mobile device operates to “push information regardless of the status of the user device.” As Dr. Easttom confirms, a POSITA would not

understand Collinge's technique to be a waste of bandwidth and resources. EX2009 ¶96. In addition, even if a POSITA were motivated to modify Collinge, there are many ways the data could arrive at the mobile device application that do not involve data being retrieved by the mobile application, or sent in response to a request from the mobile application. EX2009 ¶94. For example, a remote system can simply send data at a certain point in its processing without any request from the mobile payment application; a remote system could send data over a wireless network that is not separate from the first communication channel; or data could be sent from the payment processing service to the POS device rather than to the mobile payment application. Each of these alternatives would have alleviated the "waste of bandwidth and resources" concern that Petitioner identifies associated with a "push" from the issuer and are also able to effectively limit the number of keys on the mobile device. *Id.* ¶96-98.

Petitioner's obviousness analysis is flawed for additional reasons as well. First, Petitioner has made no showing that configuring a mobile application to request a first set of data from the remote computer system

was a known option within a POSITA's technical grasp. Pet. 40-41. Indeed, Dr. Fiske's declaration merely repeats verbatim Petitioner's bare assertion that such a request was "one of a finite number of predictable ways to retrieve data" (EX1006, ¶88; Pet. 41) but cites to nothing other than Collinge itself, which does not disclose such a request. *Id.* And Petitioner provides no explanation as to what the other "predictable ways" to retrieve data are. Pet. 40-41.

Second, Petitioner has presented no argument or evidence that a POSITA would have had a reasonable expectation of success in modifying the process disclosed in Collinge to include a *request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, [for] data associated with the account.* *Id.*; see *Teva Pharmaceuticals, LLC v. Corcept Therapeutics, Inc.*, No. 21-1360, at *6 (Fed. Cir. 2021). In particular, Petitioner provides no description of how such a request would be formulated, where it would be sent, or how it would be successful in a transaction with the existing POS and/or issuer systems with which Petitioner alleges Collinge is compatible. Pet. 40-41.

2. *Collinge does not disclose or render obvious a “non-permanent cryptographic key associated with the account” (limitation 1.C)*

Petitioner contends that KS_{UN} is a *non-permanent cryptographic key associated with the account*. In Petitioner’s view, KS_{UN} is associated with the account because (1) it is generated in response to an account-specific request, (2) it uses the account-specific ATC, and (3) it uses an account-specific key (KD_{UN}), which itself comes from the account number, in its generation. Pet. 43. This is incorrect for two reasons. First, as Petitioner’s expert acknowledged, information sent as part of an account-specific request that cannot be used to determine which account it relates to would not be *associated with the account*. EX2035 at 84:19-86:11. And, as Dr. Fiske also recognized, a POSITA would not be able to determine any of the account information, including the PAN, using KS_{UN} . EX2035 at 81:6-13; EX2009 ¶112-113. Second, Petitioner’s contention that KS_{UN} is generated using KD_{UN} and the ATC is entirely unsubstantiated by Collinge, which does not describe how KS_{UN} is generated and makes no reference to KS_{UN} being generated by either the ATC or KD_{UN} . KD_{UN} does not appear in Collinge, and Collinge’s only reference to the ATC is its statement that the single use key may include an application transaction

counter and a generating key. EX1011, [0050]. In fact, Collinge says a POSITA would know of methods to generate unpredictable numbers, which indicates that Collinge is not prescribing a particular way to generate KS_{UN} . EX1011, [0083]. Indeed, Petitioner's expert plainly acknowledged that he could not identify any disclosure in Collinge showing how Collinge's session key KS_{UN} is derived and that Collinge itself lacks the detail for him to understand how KS_{UN} is derived. EX2035 at 78:25-79:7; *see also id.* at 103:10-16. Thus, Petitioner's contentions regarding KS_{UN} being generated using KD_{UN} and the ATC are unsupported by Collinge. EX2009 ¶ 114. The disclosures in the Collinge Provisional that Petitioner relies on (i.e., EX1009, [0068]-[0071]) were not carried forward into Collinge, could not have been ascertained by reading Collinge alone, and cannot be used as prior art disclosures in this proceeding. Accordingly, Petitioner's contention that Collinge's KS_{UN} is associated with the account is unsubstantiated. For this reason, Petitioner has not met its burden as to limitation [1.C] (or [27.C]). Petitioner makes no obviousness argument as to *a first non-permanent cryptographic key associated with the account* and therefore cannot prove

unpatentability as to this limitation under and obviousness theory. Pet. 43-44.

3. *Collinge does not disclose or render obvious “the first set of data associated with the account usable by the application to formulate an application protocol data unit response” (limitation 1.C)*

Petitioner makes no assertion and provides no evidence that Collinge discloses the *first set of data associated with the account usable by the application to formulate an application protocol data unit response*. Pet. 42-43. On this basis alone, Ground 1 (anticipation by Collinge) must fail as to claim 1 and each of its challenged dependent claims. Petitioner’s arguments as to limitation [17.F] rely entirely on its arguments as to limitation [1.C]. Pet. 64. Accordingly, Ground 1 must also fail as to claim 17 and each of its challenged dependent claims. Because every challenged dependent claim depends from either claim 1 or claim 17, Petitioner’s failure to even allege anticipation of limitations [1.C] or [17.F] mean that it has failed to meet its burden under Ground 1 as to every challenged claim.

Petitioner’s obviousness argument as to limitation [1.C] is also deficient. Petitioner alleges that “it is well known in the art that, during

interrogation, commands issued by the terminal and responses from the ‘Card’ are communicated in command- and response-application protocol data units ... and it would be obvious to implement Collinge in this way to ensure interoperability with EMV-standardized devices.” Pet. 43-44. This does not demonstrate obviousness. First, Petitioner cannot prove obviousness simply by asserting that there could be a benefit (e.g., compatibility with “EMV-standardized devices”) to using APDUs for communications between the terminal and the “Card.” Petitioner has not presented any argument or evidence, for example, that a POSITA would have expected success in modifying Collinge to use an *an application protocol data unit response*. *Id.*

In addition, Petitioner cannot rely on Exhibits 1037 and 1021 for a limitation that is clearly not present in Collinge. Petitioner has not shown that either of these references is a prior art patent or printed publication, and therefore they cannot be used, as Petitioner attempts, to supply a limitation that is plainly absent from Collinge. *Yeda Rsch. v. Mylan Pharms. Inc.*, 906 F.3d 1031, 1041 (Fed. Cir. 2018) (“[N]on-prior art evidence of what was known ‘cannot be applied, independently, as

teachings separately combinable’ with other prior art...” (citing *Dominion Dealer Sols., LLC v. AutoAlert, Inc.*, IPR2014-00684, 2014 WL 5035359, at *5 (P.T.A.B. Oct. 6, 2014)). This is **not** an instance where “Petitioner sufficiently shows how it contends Collinge discloses the limitation at issue, and has supported those contentions with citations to additional exhibits as evidence of how a person of ordinary skill in the art would have understood Collinge’s disclosure.” Institution Decision, Paper 15 at 23. Instead, Petitioner is attempting to fill a gap in Collinge’s disclosure with two references it has not shown, or even alleged, to be prior art.

4. *Collinge does not disclose or render obvious “wherein the response cryptogram does not include the local cryptographic key”*

Limitation [1.E-2] recites *generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram*. Petitioner contends that Collinge’s “payment CVC3 value” is a *response cryptogram* that is generated using KS_{UN}, which Petitioner contends is *the local cryptographic key*. Pet. 46-47. As to the

limitation *wherein the response cryptogram does not include the local cryptographic key*, Petitioner does not cite to any disclosure in Collinge to support this. Pet. 47 (first full paragraph) (citing EX1006 ¶ 103, EX1009 [0071], EX1034 at 17-18, and EX1039). Indeed, as Dr. Fiske acknowledged, Collinge does not disclose how the CVC3 value is calculated. EX2035 at 105:2-5. Instead of pointing to any disclosure in Collinge, Petitioner relies on three non-prior art references: Exhibits 1009, 1034, and 1039. But these additional references do not show how KS_{UN} in Collinge is used to generate Collinge's payment CVC3 value. Exhibit 1009, as explained above, is a provisional patent application and not a "patent or printed publication" that can be used for any disclosures that are not carried forward into Collinge itself. Because Collinge itself does not describe the "CVC3 calculation" from Exhibit 1009 that Petitioner relies on, that disclosure cannot be used here. EX2009 ¶¶118-122.

Petitioner's reliance on Exhibit 1034 is also deficient. Petitioner appears to contend that this Exhibit is relevant based on its disclosure of "message authentication code (MAC) generation" (Pet. 47), yet Petitioner

offers no explanation as to how a MAC is relevant to the generation of a payment CVC3 value in Collinge. The cited portions of Exhibit 1034 say nothing of a CVC3 value, and Collinge never mentions a message authentication code or MAC, let alone equate the payment CVC3 value to a MAC.

Finally, Petitioner cites to Exhibit 1039 with its only explanation coming in a parenthetical stating “showing single-use key is not present in the MAC/cryptogram.” Pet. 47. Once again, Petitioner points to no disclosure in Exhibit 1039 of a CVC3 value or Collinge’s KS_{UN}. And Petitioner cites to the entirety of Exhibit 1039 without identifying where, among its twenty pages, one would find support for Petitioner’s argument.

Petitioner’s generalized statement that “[u]sing a single-use key ... to generate a cryptogram results in a cryptogram that does not include the single-use key” is incorrect. Pet. 47. As Dr. Easttom explains, there are numerous ways to generate a cryptogram using a cryptographic key, including techniques that would include the generating key in the cryptogram. EX2009 ¶122; *see* EX2035 at 29:20-30:19. Petitioner’s citation

to Exhibits 1009, 1034, and 1039 do not change this, and, as explained above, are not indicative of how Collinge operates or how a POSITA would understand Collinge. Ex. 1006 ¶103.

5. *Collinge does not disclose or render obvious a “device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account”*

Petitioner offers two potential constructions of limitation [1.E-3] but fails to show unpatentability under either construction. Under the **first construction**, Petitioner says the limitation would include “one or more APDUs collectively containing the response cryptogram and an account identifier for the account.” Pet. 49. Petitioner does not provide any support for its contention that this construction is supported by the specification of the ’171 patent, and Patent Owner does not contend that this construction is consistent with the plain and ordinary meaning of the claim. *Id.* Nonetheless, Petitioner contends that this first construction would be satisfied by “Collinge’s reference to the Paypass card specification in the provisional application.” Pet. 49 (citing EX1009 [0003], [0029]-[0032]). Petitioner cites only to the Collinge Provisional application. But there is no disclosure in Collinge itself of a Paypass card

specification, which means the disclosure in Exhibit 1009 was not carried forward into Collinge and, therefore, cannot be relied upon here. Without any disclosure in Collinge of a Paypass transaction, Petitioner's argument under its first proposed construction cannot prevail, and Petitioner's contentions regarding how a Paypass transaction would have been understood in the art are irrelevant. EX2009 ¶123.

Furthermore, even if disclosure in the Collinge Provisional of "Paypass" were considered as a prior art disclosure, Petitioner has presented no evidence that "Paypass" would indicate to a POSITA that one should look to Exhibit 1026 for the implementation details of "Paypass." Exhibit 1026 includes the word "PayPass" only once, in Figure 3.1 (Ex. 1026, 78), which is part of a section titled "Implementation Options." *Id.* A POSITA would not understand this to indicate that a "Mastercard interrogation" is being implemented. Furthermore, Exhibit 1026 states that "[a]n implementation option allows the vendor to select whether the software behind the option will be implemented in a particular installation." *Id.*, 31. Accordingly, a POSITA would recognize the implementations Petitioner relies on in Exhibit 1026 as a

“Mastercard interrogation” (Pet. 55) are not mandatory for EMV compliance and may not be implemented in a particular installation. Petitioner does not provide any explanation as to why a POSITA would be motivated to choose this optional implementation strategy over other available options.⁴ Petitioner’s reliance on Exhibit 1026 for a “Mastercard interrogation” thus falls far short of its burden to demonstrate obviousness. EX2009 ¶124.

Petitioner further contends that “because a POSA reading Collinge will understand its disclosure as compatible with EMV transactions ... it would have been obvious to a POSA to implement Collinge to carry out EMV transactions.” Pet. 50. But Collinge never mentions EMV transactions, and Petitioner’s only support for its contention that Collinge’s disclosures would be compatible with EMV comes from (1) the disclosure in the Collinge Provisional of PayPass and (2) reference to “CVC3” and “application cryptogram” in paragraph 50 of Collinge. *Id.* As

⁴ Petitioner refers to Exhibits 1019-1029 as “EMV Specifications.” To aid in clarity for the Board, Patent Owner uses the same term to describe these exhibits.

discussed above, the Paypass disclosures in the Collinge Provisional are not carried forward into Collinge and are thus irrelevant here. In addition, Petitioner provides no explanation as to how “CVC3” and “application cryptogram” would inform a POSITA that Collinge is compatible with **any** EMV transactions, let alone the “EMV mode contactless Visa transaction” Petitioner relies upon. Dr. Fiske’s declaration does not change the analysis. He merely repeats verbatim, without any supporting evidence, Petitioner’s contention regarding compatibility with EMV. EX1006 ¶109. And, at his deposition, Dr. Fiske admitted that a POSITA would not have understood “CVC3” to refer to an EMV mode transaction, but instead to a Magstripe transaction. In addition, as Dr. Easttom explains, at the time of the invention of the ’171 patent, a POSITA would not have understood “CVC3” or “application cryptogram” as necessarily indicating an “EMV mode Visa transaction.” EX2009 ¶¶125-126.

Under Petitioner’s proposed **second construction**, this limitation could refer to “one or more APDUs, each of which contains **both** the response cryptogram and an account identifier for the account.” Pet. 50.

Petitioner contends that an EMV mode Visa transaction would satisfy this claim element. However, as explained above, Petitioner provides no explanation as to how “CVC3” and “application cryptogram” would inform a POSITA that Collinge is compatible with **any** EMV transactions, let alone the “EMV mode contactless Visa transaction” Petitioner relies upon. EX2009 ¶¶125-126.

Petitioner’s obvious analysis also fails because it lacks sufficient evidence that a POSITA would have a reasonable expectation of success in modifying the system disclosed in Collinge to adopt the particular interrogation sequence for either a Mastercard Paypass transaction or an EMV mode contactless Visa transaction. Pet. 50. Petitioner also has not identified any problem known in the art that either of these modifications to Collinge would solve. *Id.*

B. Collinge does not anticipate or render obvious Claim 10 (or 27)⁵

Claim 10 recites steps performed *at the remote computer system*. The antecedent basis for *the remote computer system* in claim 10 comes from recitation of *a remote computer system* in claim 1. EX1001, 51:2-3. Thus, claims 1 and 10 recite the same *remote computer system*.

Petitioner's arguments as to claim 10 fail because it has not shown that each of the steps recited in claim 10 are performed at the *remote computer system* Petitioner identified in claim 1. In its analysis of claim 1, which recites, for example, *at a mobile device, executing an application ... configured to request, **from a remote computer system** ... data associated with the account*, Petitioner identifies "remote-SE system 110" as the *remote computer system*. Pet. 38-39. Petitioner's expert, Dr. Fiske, confirmed during his deposition that "remote-SE system 110," as shown, for example in Collinge's Figure 7, is what he identifies as the claimed *remote computer system*. EX2035 at 74:15-75:9.

⁵ In each instance where claims 10 and 27 are not anticipated and not obvious, dependent claims 11-13 and 28-30 are also not anticipated and not obvious.

(i.e., the alleged *remote computer system* in claim 1). This omission is fatal to Petitioner's argument. For example, limitation [10.A] recites *at the remote computer system ... receiving an authorization ... from the POS terminal*. Petitioner contends that Collinge discloses an authorization request transmitted from the POS terminal. Pet. 58 (citing EX1011, [0077]). Cited paragraph [0077] states “[t]he merchant point-of-sale terminal 120 may transmit the received payment information ... to the **acquirer processing server 312** of the acquirer 122.” Thus, Petitioner identifies “acquirer processing server 312,” which is not part of “remote-SE 110” as the *remote computer system* recited in [10.A]. Then, as to limitation [10.B], which recites *at the remote computer system ... determining a current non-permanent cryptographic key*, Petitioner alleges that “Collinge discloses that ‘the **issuer processing server 308** may validate the payment CVC3.’” Pet. 59 (emphasis added). As is evident from, for example, Figure 7 of Collinge, “issuer processing server 308” is also not part of “remote-SE 110.” EX2009 ¶149.

Petitioner provides no explanation here as to what this “payment network” is, but portions of Collinge cited (e.g., EX1011 at [0056]) disclose “payment network 124.” EX1011 at [0056]. Payment network 124 is depicted, for example, in Figure 7 of Collinge, and is also clearly distinct from “remote-SE 110.” See EX1011 [0056], [0057], [0077], [0087], [0120].

1. *Collinge does not disclose or render obvious determining a current non-permanent cryptographic key associated with the account using the account identifier*

Petitioner fails to show that limitation [10.B] (or [27.B]) is disclosed by Collinge because it does not demonstrate the step of *determining a current non-permanent cryptographic key ... using the account identifier*. Petitioner alleges that issuer processing server 308 retrieves (and thus “determines”) the UN_{CLOUD} and KS_{SUN} (i.e., the alleged *cryptographic key*) values that were used to generate the CVC3 value. Pet. 59. But Petitioner ignores that limitation [10.B] recites more than just *determining a current non-permanent cryptographic key*. It also recites the determination is done *using the account identifier*. Yet Petitioner makes no mention of issuer processing server 308 determining KS_{SUN} using the PAN (i.e., the alleged *account identifier*). Indeed, EX1009,

which Petitioner cites for this limitation, discloses in step 19a that the “ATC provided in the Payment Transaction” is “used to retrieve UN_{CLOUD} and KS_{UN} values.” EX1009, 23.⁶ For this reason, Petitioner cannot show that limitation [10.B] is disclosed by Collinge. Further, Petitioner’s obviousness argument fails because it alleges only that “a POSA would have found it obvious to implement Collinge in the manner described above,” which cannot fill the gap in its anticipation argument when “the manner described above” does not disclose a recited limitation. Pet. 60. EX2009 ¶152.

2. *Collinge does not disclose or render obvious “calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account”*

Petitioner’s analysis of limitation [10.C] (and [27.C]) is incomplete. The claim recites *calculating a calculated cryptogram*, but the cited portion of Collinge says “the issuer processing server 308 may **validate** the payment CVC3 value” and that “[m]ethods for validating a CVC3 will

⁶ Patent Owner’s citation to EX1009 here does not change that disclosures in EX1009 not carried forward into Collinge may not be relied upon as prior art disclosures in this matter.

be apparent to persons having skill in the relevant art.” EX1011, [0087]; see Pet. 59. Thus, if Petitioner’s allegation is that “validating” the CVC3 would satisfy *calculating a calculated cryptogram*, Collinge expressly omits details as to how validation of the payment CVC3 is done. If Petitioner’s contention is that Collinge’s Payment Credentials Management System *calculate[s] a calculated cryptogram*, it has provided no evidence of that. Pet. 59. Petitioner cites to paragraph [0087] of Collinge, but that paragraph makes no mention of “Payment Credentials Management System” or any step of “generating” a cryptogram. EX1011, [0087].

Petitioner also cites to paragraph [0061] of EX1009, which states “Payment Credentials Management System to generate the CVC3 value,” however that disclosure is not carried forward into Collinge and therefore cannot be used as a prior art disclosure here. As Dr. Fiske acknowledged, the disclosure in Collinge by itself resulted in “maximum confusion,” so he had to look to the Collinge Provisional. EX2035 at 97:22-98:24. Even if statements in the Collinge Provisional could be used here, Payment Credentials Management System in Collinge (*see, e.g.,* element

704 in Figure 7) is distinct from issuer processing server 308, and Petitioner presents no evidence or argument that these distinct components are part of the same remote computer system. EX2009 ¶153.

C. Collinge does not disclose or render obvious claim 8

1. *Collinge does not disclose “at the remote computer system ... sending the first non-permanent cryptographic key and the account identifier to the mobile device” (claim 8.A)*

Petitioner presents no independent analysis of limitation [8.A] and instead relies entirely on citations to previously presented arguments as to claim 1. Pet. 57 (citing §§ X.A.1.d, X.A.1.f, X.A.1.g, X.A.1.i(3)). But none of these other sections of the Petition demonstrate that Collinge discloses or renders obvious *at the remote computer system ... sending the first non-permanent cryptographic key and the account identifier to the mobile device*. For these reasons, Petitioner’s attack in claim 8 in view of Fiske must fail. Each of the sections of the Petition cited to support limitation [8A] are addressed below.

In § X.A.1.d (limitation [1.A-3]), Petitioner identifies the PAN as the claimed *account identifier*. Pet. 49-50; Fisk Dep. 22:8-14. Petitioner further contends that transmission of a CAP token “causes the remote-

SE system to generate and return payment credentials in an encrypted payload.” Pet. 38-39 (citing EX1011, [0082]-[0083], [0085]). Petitioner says that payment credentials management system 704 generates the encrypted payload, which “may include at least one CVC3 key, the KS_{UN}, and the application transaction counter.” *Id.* But a CVC3 key, KS_{UN}, and the application transaction counter are not account identifiers, and they are not the PAN. EX2009 ¶140. Paragraph [0085] of Collinge states “the encrypted payload may be transmitted to the cloud system 302 for transmitting to the mobile device,” but makes no mention of the encrypted payload including the PAN.

Section § X.A.1.f of the Petition (limitation [1.B]) contends that the application makes a request for a first set of data, which is a digital credential associated with the account, but makes no mention of the PAN. Pet. 42. In § X.A.1.g (limitation [1.C]), Petitioner contends that the mobile payment application can receive payment credentials from the cloud system over a wireless network, but is silent as to the PAN. In § X.A.1.i(3) (limitation [1.E-3]), Petitioner contends that the **mobile device** sends payment credential data, which a POSA would understand to include

generated cryptogram and “other common payment credential information” such as the PAN. Pet. 48-49. This does not satisfy claim 8, which is directed to an account identifier sent *to the mobile device*, not to information sent **from** the mobile device. EX2009 ¶141.

Thus, the only discussion of anything sent **from** the remote-SE to the mobile device is the “encrypted payload,” which does not include the PAN. For this reason, Petitioner has not shown that Collinge discloses or renders obvious *at the remote computer system: prior to the interrogation, ... sending ... the account identifier to the mobile device over the wireless network*. EX2009 ¶142.

For these reasons, Petitioner has not shown that Collinge anticipates or renders obvious claim 8 or dependent claim 9.

2. *Collinge does not disclose “after the interrogation, generating the second non-permanent cryptographic key at the remote computer system, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.”*

Petitioner presents no independent analysis of limitation [8.B] and instead relies entirely on previously presented arguments as to claim 1.

Pet. 57 (citing §§ X.A.1.j). Because this prior section of the Petition does not present any argument or evidence of the steps performed *at the remote computer system* and *after the interrogation*, Petitioner has not met its burden as to this limitation.

Indeed, Petitioner contends that “the new KS_{UN} for a subsequent transaction would be **requested** subsequent to a prior transaction.” Pet. 51 (emphasis added). Any such request would be a request by the application. This does not show that the remote-SE generates a new KS_{UN} value after an interrogation. As a POSITA would recognize, KS_{UN} values could readily be generated prior to interrogation and need not be generated by the remote computer system. EX2009 ¶145.

Petitioner makes no obviousness argument as to this limitation, so it has not shown this limitation would be obvious.

For these reasons, Petitioner has not shown that Collinge anticipates or renders obvious claim 8 or dependent claim 9.

D. Collinge does not anticipate or render obvious claim 4 (or 21)

1. *Collinge does not “wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification” (claims 4 and 21)*

Petitioner alleges that Collinge’s reference to “m/chip payment transactions” would be understood by a POSITA “to refer to known EMV-compliant payment system specifications defining sets of inputs and responses.” Pet. 54 (citing EX1011, [0044], EX1006 ¶ 117). Paragraph [0044] of Collinge does not mention “m/chip” or “m/chip payment transactions,” so it cannot provide any support to Petitioner’s argument. If Petitioner intended to cite paragraph [0049] of Collinge, reliance on that disclosure is unpersuasive. First, the “m/chip” disclosure in Collinge is not prior art. Collinge can only be relied on for disclosures therein that were “carried forward” from the Collinge Provisional.⁷ Petitioner cites to no portion of the Collinge Provisional disclosing “m/chip” or “m/chip payment transactions” and Patent Owner can find no such disclosure in

⁷ Similarly, Petitioner’s reference to “PayPass” disclosure in the Collinge Provisional is not allowed since Collinge does not carry forward that disclosure. Pet. 54.

the Collinge Provisional. Second, even if considered, Petitioner's contention that a POSITA would understand "m/chip" as part of "EMV-compliant payment system specifications" is unsupported. Notably, Dr. Fiske's declaration as to this limitation differs from what Petitioner contends. As to "m/chip payment transactions," Dr. Fiske says "a POSA would understand [them] to refer to known payment system specifications defining sets of inputs and responses. EX1006 ¶ 117. The cited portion of Dr. Fiske's declaration says nothing about "EMV-compliant" payment system specifications. EX2009 ¶ 128.

Furthermore, neither Petitioner nor its expert identify any disclosure in "Mastercard Paypass or EMV Specifications" that the Collinge system is compliant with. Thus, Petitioner has not shown that *the interrogation conforms to a card specification, the set of inputs is specified by the card specification*, or that *the at least one device response is formulated according to the card specification* as claim 4 recites. It is not enough for Petitioner to argue in the abstract that a card specification could specify the sets of inputs and/or the formulation of the device response and that a POSITA would be motivated to make their

systems compliant with such a specification. As Dr. Easttom explains, a POSITA would recognize that card specifications often provide only a loose framework for transactions and often leave many implementation details to the issuer's discretion. EX2009 ¶128. Showing that this claim is obvious in light of Collinge requires Petitioner to demonstrate, at least, that a POSITA would be motivated to modify Collinge and that such modifications would result in Collinge's system performing the recited steps. Petitioner has not done so.

E. Collinge does not anticipate or render obvious claim 15 (or 32)

1. *Collinge does not disclose or render obvious an “application is configured to generate the response cryptogram according to a card specification” (claims 15 and 32)*

Petitioner presents no independent analysis of claims 15 and 32, instead referring to “Claims 4 and 20.” Pet. 62. Petitioner's arguments as to claim 15 (and 32) fail for the same reasons as described above for claim 4 (and 20). In addition, Petitioner's analysis of claim 4 does not establish, or even attempt to establish, that *generat[ion] of the response cryptogram [is] according to a card specification*. Instead, Petitioner merely alleges that “card specifications were well known in the art and a POSA would

have been motivated to make their systems compliant with such specifications.” Pet. 54. This allegation, even if true, does not demonstrate that it would have been obvious, as claim 15 recites, that *the application is configured to generate the response cryptogram according to a card specification*. Petitioner has made no showing that either the Mastercard Paypass or EMV Specifications specify how a response cryptogram is generated. Therefore, Petitioner has not shown that conducting a transaction according to either specification involves generating a response cryptogram according to the card specification. Further, as Dr. Fiske admitted, a transaction could comply with EMV Specifications even when generating a cryptogram using a technique that is **different** from the optional technique disclosed in the EMV Specifications. EX2009 ¶154; EX2035 at 61:1-62:1; *see* EX2035 at 29:20-30:19.

F. Collinge does not anticipate or render obvious claim 6 (or 22)

1. *Collinge does not disclose or render obvious “generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.”*

Petitioner’s analysis of claims 6 and 22 points to no disclosure in Collinge as to any particular technique for generating the alleged *response cryptogram*, let alone any *digital encryption standard*. For this reason, Petitioner cannot show that Collinge anticipates claim 6 (or 22). Pet. 56. As to obviousness, it appears that Petitioner’s argument relies on its assertion that using DES “is the predominant symmetric encryption algorithm in financial applications.” Pet. 56. However, as Dr. Easttom explains, “using an algorithm to encrypt data in financial applications is not the same as using an algorithm to generate a cryptogram.” EX2009 ¶130. And one need not use any symmetric algorithm to generate a cryptogram. There are numerous variations of MAC including AMAC (ANSI Retail MAC); PMAC (a Parallelizable Message Authentication Code); UMAC (Universal Message Authentication Code); KMAC (Keccak Message Authentication Code).

Using a DES based MAC is only one of a wide array of options, many of which are either more efficient and/or more secure than DES. Therefore, it would not have been obvious to a POSA to use DES to encrypt inputs to create a cryptogram. In addition, a cryptogram can be generated with a hash algorithm (including MD5, SHA1, SHA2, SHA3, RIPEMD, HAVAL, Whirlpool, Skein, GOST, BLAKE, etc.), or an HMAC. EX2009 ¶¶131-134.

Thus, Petitioner's obviousness argument falls short. It is not sufficient to show that DES was known. Petitioner has the burden to show that DES would have been chosen by a POSITA implementing Collinge and that a POSITA would have had a reasonable expectation of success in doing so.

For these reasons, Petitioner has failed to demonstrate that claims 6 or 22 are anticipated or obvious in light of Collinge.

G. Collinge does not anticipate or render obvious claim 16 (or 33)

1. *Collinge does not disclose or render obvious “wherein the first and second non-permanent cryptographic key are associated with an issuer master key.” (claim 16 and 32)*

Petitioner has not shown that Collinge discloses or renders obvious claim 16 (or 32). Petitioner alleges that this claim is met because KS_{UN} (i.e., the alleged *cryptogram*) is “generated using an intermediate key (using KD_{UN}) which itself is generated from an issuer master key IMK.” Pet. 62. But this allegation finds no support in Collinge, because Collinge does not specify how KS_{UN} is generated. Petitioner cites to a single paragraph of Collinge, but that paragraph says that “[m]ethods and systems for the generation of unpredictable numbers will be apparent to persons having skilled [sic] in the relevant art,” and says nothing at all about an “intermediate key,” “ KD_{UN} ,” or the “issuer master key” that Petitioner says are used to generate KS_{UN} . EX1011, [0083]. These additional values, by Petitioner’s own admission, are not described in Collinge. Pet. 62. Petitioner identifies them only in the Collinge Provisional in paragraph [0071], and the disclosure there was not carried forward into Collinge. Indeed, Petitioner’s expert plainly acknowledged that he could not identify any disclosure in Collinge showing how Collinge’s session key KS_{UN} is derived. EX2035 at 78:18-79:7. Dr. Fiske also affirmed that Collinge itself lacks the detail for him to understand

how KS_{UN} is derived and that he needed to refer to the Collinge Provisional to understand its derivation:

Q: I see. So what you found was that Collinge, Exhibit 1011, by itself does not describe in enough detail for you to understand how KS_{UN} is derived. Right?

A: That's correct. I needed – in order to fully understand, I needed to refer to the provisional, which is, I think, Exhibit 1009.

EX2035 at 78:25-79:7; *see also id.* at 103:10-16. Without any disclosure in Collinge showing how KS_{UN} is calculated or derived, Petitioner cannot demonstrate that KS_{UN} is *associated with an issuer master key* as recited in claim 16. Accordingly, Petitioner has not shown that Collinge discloses claim 16 (or 32). EX2009 ¶155.

Petitioner's obviousness argument also fails here. Petitioner alleges that “using issuer master keys to generate card-specific and transaction specific keys for generating cryptograms was well-known” and cites to Exhibit 1020 for its alleged disclosure of “derivation of Session Key from ICC Master Key generated from issuer master key.” Pet. 62. But, as Dr. Fiske confirmed, Collinge does not follow the “mechanism [] in EMV” for

generating session keys. EX2035 at 77:12-78:17. In addition, as Dr. Fiske also acknowledged, EMV does not mandate any technique for generating session keys. *Id.*, 62:21-25; EX1020, 142 (Appendix A1.3); EX2009 ¶156. And Petitioner has provided no argument as to why a POSITA would choose to generate session keys in Collinge using an issuer master key. Asserting that a technique was “known” or even “well known” does not demonstrate that it would be obvious to apply that technique to the payment system disclosed in Collinge or that a POSITA would expect such an application to be successful. EX2009 ¶156.

Accordingly, Petitioner has not shown that Collinge renders obvious claim 16 (or 32).

H. Collinge does not anticipate or render obvious claims 17, 24, 25

Petitioner’s analysis of these claims in Grounds 1 and 2 rely on arguments Petitioner made with respect to claims 1, 8, and 17 and fail for the same reasons. *See* Pet. 64-65.

VI. Grounds 3 and 4 do not establish that any of claims 1-33 are anticipated by Fiske or rendered obvious by Fiske in view of the knowledge of a POSITA

A. Fiske does not disclose or render obvious “sending ... the account identifier to the mobile device” (claims 8, 9)

Petitioner has not shown that claim 8 is unpatentable because it has not shown that Fiske discloses the step of *sending ... the account identifier to the mobile device*. Petitioner makes no independent argument for this claim, instead relying entirely on its arguments as to limitations [1.B] and [1.C]. Pet. 78. However, each of those limitations in claim 1 recites steps performed *by the application*, not *at the remote computer system*, as recited in claim 8.

Because Petitioner presents no independent argument as to claim 8, its analysis as to this limitation is limited to its discussion of limitations [1.B] and [1.C]. Pet. 78. But Petitioner’s prior discussion of those limitations is entirely silent as to an *account identifier*, which is not recited in those limitations but is recited in claim 8. Indeed, Petitioner’s only discussion in [1.B] or [1.C] of any information received by the user device references only “single-use payment keys, specifically, an ICC Session Key.” Pet. 69, 70. In particular, as to limitation [1.B], which

recites *a first set of data associated with the account*, Petitioner says “data associated with the account includes the single- use payment keys such as the ICC Session Key” but makes no mention of an account identifier. Pet. 69. In addition, as to limitation [1.C], which recites *receiving ... the first set of data associated with the account*, Petitioner again identifies only the “ICC Session Key” and makes no mention of an *account identifier*. Pet. 70.

Accordingly, Petitioner has not presented any argument or evidence that the alleged *account identifier*—the PAN—is sent by a remote computer system to the mobile device in Fiske. Indeed, the only data element the Petition even arguably identifies as being sent from the issuer to the mobile device, i.e., Fiske’s ICC Session Key, is unquestionably **not** an *account identifier*. EX2009 ¶215; EX2035 at 113:14-17 (Q: “[I]s and ICC session key an account identifier?” A: “No.”); *see also* EX2035 at 22:8-14. Because the Petition fails to make even an allegation that Fiske discloses or renders obvious *the remote computer system ... sending ... the account identifier to the mobile device*, it cannot meet Petitioner’s burden as to claim 8.

Even if one looks to uncited portions of the Petition (not relied on for claim 8), there is still no argument or evidence that the alleged *remote computer system* sends the *account identifier to the mobile device*. For example, in its analysis of limitation [1.A-3], which recites, in part, an application *configured to request ... data associated with the account*, Petitioner identifies only “payment keys” and says nothing about an *account identifier*. Pet. 68 (citing EX1012, 12:45-52, 12:50-57, 13:17-24).

Similarly, limitation [1.E-3] recites *an account identifier* that is sent *from the mobile device to an electronic reader*. In its analysis of that limitation, Petitioner identifies the PAN as part of the information requested by the POS terminal in the READ RECORD command. Pet. 72-73. However, Petitioner’s analysis of this limitation relates to communications between the **mobile device and the POS terminal**. Petitioner again makes no argument and presents no evidence of any *account identifier* sent **from a remote computer system** to a mobile application. *Id.*

Because Petitioner has omitted any argument or evidence of a *remote computer system ... sending ... the account identifier to the mobile*

device, the anticipation challenge to claim 8 (and dependent claim 9) in Ground 3 must necessarily fail. Petitioner has also not made any obviousness challenge to claims 8 or 9—and specifically no assertion that *a remote computer system ... sending ... the account identifier to the mobile device* would be obvious—so its challenge to claims 8 and 9 in Ground 4 must also fail. *See* Pet. 72-73.

B. Fiske does not disclose or render obvious any of the “remote computer system” steps (Claims 10-13, 27-30)

1. *No disclosure in Fiske of an authorization request comprising the account identifier*

Limitation [10.A] recites an *authorization request*, received *at the remote computer system*, comprising two distinct data items: (1) *the response cryptogram* and (2) *the account identifier*. Each of these data items are first recited in claim 1 (or 17, for claim 28).⁸ EX1001, 51:36, 51:50. In Petitioner’s analysis of that claim, Petitioner identifies Fiske’s ARQC as the alleged *response cryptogram* (Pet. 55) and identifies the primary account number (“PAN”) as the alleged *account identifier*. Pet.

⁸ Petitioner presents its analysis of claims 10 and 27 in a combined discussion. Pet. 58-60. Patent Owner addresses these claims in the same manner.

73, 49 n.6; EX2035 at 22:8-14, 24:21-25:3, 110:20-111:13. Yet, in its analysis of claim 10, Petitioner completely ignores the *account identifier* limitation. Indeed, Petitioner's entire analysis of limitation [10.A] consists of a single sentence: "Fiske discloses that '[i]n response to receiving the Application Cryptogram, the terminal identifies the type of Application Cryptogram sent by the user device ... and forwards the ARQC to the issuer ... for authorization of the transaction.'" Pet. 78-79 (citing EX1012, 16:6-10). This argument appears to allege a request that comprises the *response cryptogram* (i.e., the ARQC) but it simply ignores the remainder of the claim limitation, saying nothing about the PAN (i.e., the alleged *account identifier*) being part of any authorization request. *Id.* Petitioner also cites, without explanation, col. 7:30-60 and Figure 7 of Fiske, but these disclosures are also silent about the authorization request including the PAN. *See* EX1012, 7:30-60, Fig. 7. Because anticipation requires Petitioner to show that each element of the challenged claim is disclosed in the prior art, Petitioner has not met its burden here. Accordingly, Petitioner's anticipation challenge to claims 10 and 27 must fail. Because claims 11-13 depend from claim 10 and because

claims 28-30 depend from claim 27, the challenge to those claims fails as well. Finally, because Petitioner has not presented any argument that this limitation would have been obvious, any obviousness challenge to claims 10-13 or 27-30 also fails. Pet. 78-79 (no mention of obviousness as to 10.A or 27.A).

2. *No disclosure in Fiske of determining a current non-permanent cryptographic key associated with the account using the account identifier*

Petitioner's analysis of limitation [10.B] (and corresponding limitation [27.B]) is fatally deficient because it also ignores the recited *account identifier* used to *determin[e] a current non-permanent cryptographic key*. Petitioner simply makes no allegation that the alleged *account identifier* (i.e., the PAN) is used to determine *a current non-permanent cryptographic key* (i.e., the ICC Session Key). Pet. 79. Its single-sentence assertion as to this limitation mentions only a Session Key (i.e., the alleged *non-permanent cryptographic key*) and the ARQC (i.e., the alleged *cryptogram*). *Id.* (citing EX1012, 17:13-14, Fig. 7). Nothing in this assertion ties the PAN (i.e., the alleged *account identifier*) to any step at the remote computer system of determining the Session

Key (i.e., the alleged *non-permanent cryptographic key*). And Petitioner’s citations to Fiske—i.e., col. 17:14-14 and Fig. 7—are meritless as well. Fiske’s disclosure at col. 17:13-14 appears in the middle of a sentence relating to limiting the number of ICC Session Keys that may be generated, and Figure 7 shows only one step performed by the issuing bank, which is “Examine ARQC” as part of step 714. EX1012, 17:13-14, Fig. 7. Neither of these disclosures shows or suggests a PAN being used by the remote computer to determine a cryptographic key. Even if a POSITA looked to the EMV Specifications to understand Fiske’s ARQC—which Petitioner has not alleged a POSITA would do—he/she would find that the ARQC described in the EMV Specifications does not include the PAN. EX2009 ¶¶217-219; EX1028 at 87. There is simply no reading of Petitioner’s argument that shows anticipation or obviousness of this limitation. EX2009 ¶217.

Accordingly, Petitioner’s anticipation challenge to claims 10 and 27 must fail. Because claims 11-13 depend from claim 10 and because claims 28-30 depend from claim 27, the challenge to those claims fails as well. Finally, because Petitioner has not presented any argument that this

limitation would have been obvious, any obviousness challenge to claims 10-13 or 27-30 also fails. Pet. 78-79 (no mention of obviousness as to 10.B or 27.B).

3. *No disclosure in Fiske of “calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account”*

Petitioner’s single-sentence argument for limitation [10.C] (and [27.C]) appears to contend that the ARQC (i.e., the alleged *cryptogram*) **could** be calculated using the Session Key (i.e., the alleged *cryptographic key*). Pet. 79. But limitation [10.C] does not recite how a calculated cryptogram **could** be calculated; it recites *calculating a calculated cryptogram using the current non-permanent cryptographic key*. As evidenced by Petitioner’s assertion only as to how a cryptogram **could** be calculated, combined with Petitioner’s failure to cite any portion of Fiske for this limitation, there is no question Petitioner has not shown this limitation is disclosed by Fiske. If Petitioner intended to make an argument that calculating the ARQC using the Session Key would have been obvious, a bare assertion that such a calculation could have been done is not sufficient. Petitioner cites to no expert testimony supporting

its assertion, and offers no explanation, for example, as to why a POSITA **would** have made such a calculation, nor any argument or evidence that a POSITA would have had a reasonable expectation of success in implementing Fiske in this way. Pet. 79; EX2009 ¶221. *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only could have made but would have been motivated to make the combinations or modifications of prior art to arrive at the claimed invention.”); *Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 888 (Fed. Cir. 2024). For these reasons, Petitioner’s challenge to this limitation fails.

C. Fiske does not disclose or render obvious claim 11 (or 28)

1. *Fiske does not disclose or render obvious an “the set of inputs comprises unpredictable data; the authorization data comprises the unpredictable data; and the calculated cryptogram is calculated using the unpredictable data.” (claim 11)*

Petitioner’s challenge to claim 11 (and 28) fails for several reasons. First, it fails because claim 11 depends from claim 10, for which Petitioner has failed to meet its burden. Second, Petitioner’s argument for anticipation by Fiske additionally fails because it is premised on

Petitioner’s incorrect assertion that “Fiske explicitly incorporates by reference EMV Specifications.” Pet. 80. The Board correctly determined in its decision on institution that Fiske made no such incorporation. ID at 29. Third, Petitioner’s argument is premised on an incorrect assertion that the EMV Specifications “**explicitly require** that input data for generation of the response cryptogram include an ‘Unpredictable Number,’ which is supplied by ‘[POS] Terminal.’” Pet. 80 (citing EX1020 § 8.1.1) (emphasis added). This is false. As Petitioner’s expert readily acknowledged, the techniques for generating a cryptogram disclosed in the EMV Specifications are “not mandatory.” EX2035 at 61:21-62:1; EX1020 at 99; EX2009 ¶202. Indeed, a POSITA would have recognized that a payment card could be used for EMV transactions without adopting EMV’s disclosed methods of generating an application cryptogram. EX2009 ¶156; EX2035 at 61:21-62:1. Thus, even if Petitioner had shown that a POSITA would have been motivated to implement Fiske in a manner compatible with the EMV Specifications, such a showing still does not demonstrate that a POSITA would have chosen to

calculate the cryptogram *using the unpredictable data*, since this step is not needed for EMV compatibility. EX2009 ¶231.

D. Fiske does not anticipate or render obvious claim 12 (or 29)

1. *Fiske does not disclose “wherein the POS command communications comprise the unpredictable data.” (claims 12 and 29)*

Petitioner’s challenge to claim 12 (and 29) fails for several reasons. First, it fails because claim 12 depends from claims 10 and 11, for which Petitioner has failed to meet its burden. Second, Petitioner’s argument for anticipation by Fiske additionally fails because it is premised on Petitioner’s incorrect assertion that “Fiske explicitly incorporates by reference EMV Specifications.” Pet. 80. The Board correctly determined in its decision on institution that Fiske made no such incorporation. ID at 29-30. Third, Petitioner’s analysis of claim 12 makes no mention of *the POS command communications* recited in claim 12. And Petitioner’s only contention as to an “unpredictable number” states that it would be included in “the authorization request,” Pet. 80, which does not demonstrate that *the POS command communications comprise the unpredictable data*. Claim 11 recites *at the remote computer system ...*

receiving an authorization request to authorize the transaction from the POS terminal, but the claimed POS command communications are recited in claim 1 as being received **by the mobile device** from the POS terminal. Petitioner offers no explanation as to how its identification of communications between the alleged remote computer system and the POS terminal are relevant to communications between the mobile device and the POS terminal. For this additional reason, Petitioner's arguments as to unpatentability of claim 12 must fail. EX2009 ¶232.

E. Fiske does not anticipate or render obvious claim 13 (or 30)

1. *Fiske does not disclose or render obvious “wherein the authorization data further comprises values from the transaction”*

Petitioner's challenge to claim 13 fails for several reasons. First, it fails because claim 13 depends from claims 10, 11, and 12, for which Petitioner has failed to meet its burden. Second, Petitioner cites to no disclosure in Fiske in its analysis of this claim and therefore fails to show that Fiske discloses that *the authorization data further comprises values from the transaction*. Pet. 80-81. Third, Petitioner contends only that data objects necessary to reproduce the transaction claim “**usually**

include information such as amount and currency code,” *id.*, but does not explain the circumstances in which this information would be included or why a POSITA would have chosen to include this data as part of *the authorization data*. And Petitioner’s contention that a POSITA would have “otherwise found this obvious because it is well established practice in the art” is stated with no explanation or substantive evidence. Petitioner cites only to Dr. Fiske’s declaration, which simply repeats verbatim the statement in the Petition without any supporting evidence, and should thus be given little weight. EX1012 ¶ 214. As Dr. Easttom explains, “[a] POSITA would have recognized that validation of a cryptogram (e.g., using the response cryptogram) would not require any ‘values from the transaction’ and that if ‘values from the transaction’ were needed for a different purpose, e.g., to determine if a payment amount is within acceptable limits, that information need not be included as part of an ‘authorization request’ with the ‘response cryptogram and the account identifier,’ as claimed. EX2009 ¶234.

F. Fiske does not disclose or render obvious claim 1 (or 17)

1. *No disclosure in Fiske of “wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram”*

Petitioner contends that Fiske’s “application cryptogram” is a *response cryptogram* that is “generated based on inputs, such as ‘data sent to the ICC in the data field of the GENERATE AC command’ and the ICC Session Key,” which Petitioner contends is *the local cryptographic key*. Pet. 72 (quoting EX1012 at 8:22-24). As to the limitation *wherein the response cryptogram does not include the local cryptographic key*, Petitioner contends that “it is well understood in the art that the Application Cryptogram would not include the ICC Session Key itself because the cryptogram is generated using the Session Key as encryption key.” Pet. 72. (citing EX1006 ¶ 181, EX1034 at 17-18, and “[Rabah]”). Dr. Fiske’s statements in paragraph 181 of his declaration merely parrot verbatim the language of the Petition, and should be given little weight. That is especially true where, as here, the references that he and Petitioner rely on do not show **how** Fiske’s Application Cryptogram is generated. For example, Petitioner appears to contend

that Exhibit 1034 is relevant based on its disclosure of “message authentication code (MAC) generation.” Pet. 72. Yet Petitioner ignores that the techniques for generating a MAC in the EMV Specifications are “not mandatory.” EX2035 at 61:21-62:1; EX1020 at 99; EX2009 ¶202. Indeed, as both experts agree, a POSITA would have been familiar with many different techniques for cryptogram generation, and a payment card could be used for EMV transactions without adopting EMV’s disclosed methods of generating an application cryptogram. EX2009 ¶214; EX2035 at 61:21-62:1. Accordingly, a POSITA would not understand Fiske’s disclosure of an Application Cryptogram to disclose or imply any particular technique for generating it or any particular format/structure for the resulting cryptogram. EX2009 ¶214.

Finally, Petitioner cites to “[Rabah]” without an exhibit number or page citations. Petitioner and the Board should not be required to hunt through the record to determine the meaning of this citation. Dr. Fiske also cites to Exhibit 1039—a document 20 pages in length—without any page reference. Exhibit 1039 makes no mention of an Application Cryptogram, and in fact never uses the term “cryptogram.” EX1039.

Because Petitioner relies on an optional feature in the EMV specifications without any explanation as to why a POSITA would have chosen to implement that feature in Fiske, it has not met its burden to show that Fiske discloses or renders obvious a *response cryptogram [that] does not include the local cryptographic key*.⁹

To the extent Petitioner attempts to argue that a cryptogram inherently does not include the cryptographic key used to generate it, that argument is inconsistent with the claim language. Such an interpretation would render the entirety of the “wherein” clause of limitation [1.E-2] meaningless.

2. *Fiske does not disclose or render “at least one response application data protocol unit containing the response cryptogram and an account identifier for the account” (claim 1.E-3)*

Fiske does not disclose communications between a mobile device and an electronic reader using response application protocol data units. Petitioner says that “responses from the device or card are response

⁹To the extent Petitioner attempts to argue that a cryptogram necessarily does not include the cryptographic key used to generate it, that argument is inconsistent with the claim language. Such an interpretation would render the entirety of the “wherein” clause of limitation [1.E-2] meaningless.

APDU messages,” but this is incorrect and unsupported. Pet. 73 (referencing [1.E] and [1.E-1]). Section [1.E-1] says nothing about APDUs, so that discussion is irrelevant here. Pet. 71-72. In [1.E], Petitioner contends that command- and response-application data protocol units are well known in the art for “EMV transactions referred to by Fiske.” Pet. 71 (citing EX1037 at 46-48). However, the cited pages of Exhibit 1037 say nothing about EMV specifications. Instead, they purport to describe ICC functionality based on the standard ISO/IEC 7816. EX1037, 46. And, as Dr. Fiske acknowledges, “APDUs are not an EMV concept” and “EMV itself uses the concept from an international standard, ISO 7816.” EX2035 at 90:11-24. ISO 7816 is mentioned in the Fiske reference, but this is with respect to “**contact** ICCs [that] are powered by the PoS terminal.” EX1012, 1:45-51 (emphasis added). A POSITA would readily recognize that Fiske’s “user device” is different from a **contact** ICC powered by the POS terminal. EX2009 ¶205; see, e.g., EX1012 at Figure 5 (depicting “use device” 502). As to **contactless** cards, Fiske discloses that they conform to a different standard, i.e., ISO/IEC 1443 or ISO/IEC 15693. EX1012, 1:45-51. Accordingly,

Petitioner's reliance on statements in Exhibit 1037 relating to ISO 7816 do not demonstrate that the wireless communications between Fiske's user device and POS utilize APDUs.

Also, Exhibit 1037 bears a copyright date of 2003, which is five years **before** the date marked on the "EMV specifications" (Exhibits 1019-1029) on which Petitioner relies. Petitioner offers no explanation of how references to "EMV" in a book from 2003 could possibly inform a POSITA as to EMV 4.2 protocols that had not yet been written. Even if they could, nothing in the cited section of Exhibit 1037 (i.e., chapter 3) says anything about EMV transactions, and Petitioner has offered no explanation as to why this section of Exhibit 1037 would inform a POSITA as to communications between Fiske's user device and POS.

3. *"EMV mode Visa transactions" relied upon by Petitioner are not compatible with Fiske (claim 1.E-3)*

Fiske discloses two separate commands issued by the POS terminal to the user device. First, Fiske discloses a "READ RECORD" command, which Petitioner alleges includes a request for "the primary account number (PAN)." Pet. 72-73. Petitioner further alleges that Fiske discloses that an Application Cryptogram is returned in response to a

“GENERATE AC” command. *Id.* Petitioner offers two distinct constructions for the “R-ADPU Term” and contends that the second construction is “likely correct.” Pet. 24-25. Under Petitioner’s second construction the Term would be construed as “one or more response application data protocol units, each of which contains both the response cryptogram and an account identifier for the account.” Pet. 25.

Petitioner contends that the limitation would be met under its second construction only in an EMV mode contactless Visa transaction. Pet. 73. Petitioner does not offer any explanation in Grounds 3 or 4 for this contention and instead simply says “the Term is disclosed by Fiske carrying out a contactless EMV transaction, for the same reasons stated in [1.E-3] above.” Pet. 73. This contention is flawed for several reasons. First, Petitioner’s reference to “the same reasons stated in [1.E-3] above” is ambiguous. When asked during his deposition about the identical statement appearing in his declaration, Dr. Fiske stated that it was “referring to the paragraph in bold at the top of Page 93 and is a quotation from the '171 patent.” EX2035 at 114:16-115:11. In other words, Dr. Fiske testified that the claim language itself provided the basis for his opinion

that limitation [1.E-3] was satisfied. Such circular reasoning is entirely insufficient.

To the extent that Petitioner argues, in contradiction to Dr. Fiske's sworn testimony, that the "same reasons stated ... above" refer to its discussion of limitation [1.E-3] in grounds 1 and 2, that argument also fails. First, Petitioner does not adequately explain how an obviousness argument based on combining Collinge with the knowledge of a POSITA would apply to a wholly separate argument based on combining Fiske with the knowledge of a POSITA. In its Grounds 1/2 discussion of limitation [1.E-3], Pet. 48-50, Petitioner alleges "it would have been obvious to a POSA to implement Collinge to carry out EMV transactions to expand their market opportunity by allowing interoperability with existing and expected future payment infrastructure." Pet. 50 (emphasis added). This contention is inapplicable to the Fiske reference in Grounds 3/4.

Second, even if Petitioner had successfully argued that it would be obvious to implement Fiske to authorize EMV payment transactions, Petitioner provides no evidence or argument as to why a POSITA would

choose—among the many available options within EMV—to implement Fiske for an “EMV mode Visa” transaction. As Dr. Fiske acknowledged, a contactless transaction could be compatible with EMV specifications **without** implementing “EMV mode” transactions. EX2035 at 59:18-25. As Dr. Easttom further explains, the EMV specifications provide a general framework for an issuer’s card to interact with a POS terminal and for the POS terminal to interact with the issuer’s systems. The EMV specifications leave many implementation decisions (e.g., cryptogram generation algorithms, session key generation algorithms, EMV/magstripe mode) in the hands of the issuers. EX2009 ¶205; *see also* EX2035 at 60:12-62:1 (“As far as EMV is concerned, all it is doing is providing a globally interoperable mechanism whereby that issuer’s card can interact with any EMV terminal and information can get through to the issuer.”).

Third, Petitioner’s reliance on purported commands and responses in an “EMV mode contactless Visa transaction” ignores the fact that those commands are inconsistent with the commands and responses disclosed in Fiske that Petitioner relies upon. In particular, Petitioner contends

that the mobile device responds to the “GENERATE AC” command disclosed in Fiske by returning an Application Cryptogram. Pet. 73 (citing EX1012 at 3:26-46, 2:63-67, 5:28-30, 7:30-41). Yet the EMV specification on which Petitioner relies to satisfy its second construction expressly states “there is no GENERATE AC command.” EX1027 at 84 (Section 6.1).

6.1 Issuer Update Processing Commands

To facilitate Issuer Update Processing, support for the EXTERNAL AUTHENTICATE command and issuer script processing is required.

Requirements – Issuer Update Processing Commands

6.1.1.1 (EXTERNAL AUTHENTICATE Command) [5.88]

The kernel shall support the EXTERNAL AUTHENTICATE command, as defined in section D.3.

6.1.1.2 (Issuer Scripts) [5.89]

The kernel shall support Issuer Scripts according to [EMV 4.2 Book 3], section 10.10, and [EMV 4.2 Book 4], section 6.3.9, except for the following:

- Unlike [EMV 4.2], Issuer Script Templates with Tag '71' or Tag '72' are processed and issued by the kernel in the same manner. There is no GENERATE AC command, and Issuer Script Templates with Tag '71' and '72' are both processed during Issuer Update Processing.
 - No processing is performed on the Transaction Status Information (TSI) or Terminal Verification Results (TVR).
-

The Petition fails to address this inconsistency and provides no argument as to why a POSITA would be motivated to change the system disclosed in Fiske to implement a different command scheme.

G. Fiske does not disclose or render obvious claims 4 (20) and 5 (21)

1. *Fiske does not disclose or render obvious “wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification” (claim 4) or “wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.” (claim 5)*

As the Board recognized in its Institution Decision, Petitioner’s arguments as to claim 4 (and 20) and claim 5 (and 21) are premised on its incorrect assertion that the EMV specifications are incorporated by reference in Fiske. Pet. 76-77; ID at 29-30. Fiske does not incorporate by reference the EMV Specifications (i.e., any of Exhibits 1019-1029). Accordingly, regardless of whether the EMV specifications “describe the inputs and responses by the card to be compatible with EMV transactions,” Petitioner cannot show that any of claims 4 (or 20) or claim 5 (or 21) are anticipated by Fiske because the disclosures in the EMV specifications are not part of Fiske.

As to obviousness, Petitioner provides only its conclusion that these claims would have been obvious. Pet. 76-77. The law requires more. By

providing no explanation as to why a POSITA would have found these claims obvious, Petitioner has not met its burden. Dr. Fiske's declaration at paragraphs 196-197 should be given no weight here because it simply repeats Petitioner's conclusory assertions without any explanation or citation to evidence. EX1006 ¶¶196-197; EX2009 ¶¶209-212.

H. Fiske does not disclose or render obvious claim 6 (or 22)

1. *Fiske does not disclose or render obvious a “generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output.” (claim 6 and 22)*

Petitioner appears to acknowledge that Fiske itself makes no mention of the algorithm used to generate the Application Cryptogram. Indeed, Fiske expressly states that “[h]ow the Session Key is used to generate the application cryptogram is specific to the payment system being implemented.” As discussed in relation to limitation [1.E-2], techniques for generating a MAC in the EMV specifications are “not mandatory.” EX2035 at 61:21-62:1. Thus, Petitioner's contention that “the AC in an EMV transaction **is generated** using a 3DES algorithm,” Pet. 77 (emphasis added), is simply incorrect. As Dr. Fiske acknowledged,

a POSITA would have been familiar with many different techniques for cryptogram generation, and a payment card could be used for EMV transactions without adopting EMV's disclosed methods of generating an application cryptogram. EX2009 ¶214; EX2035 at 61:21-62:1; EX2035 at 29:20-30:19.

Petitioner again provides no explanation for its contention that this limitation is obvious, and has therefore failed to meet its burden as to claims 6 and 22. Pet. 89.

I. Fiske does not disclose or render obvious claim 15 (or 32)

1. *Fiske does not disclose or render obvious a “wherein the application is configured to generate the response cryptogram according to a card specification.” (claims 15 and 32)*

Petitioner presents no independent analysis of claims 15 or 32, instead referring to “Claims 4 and 20.” Pet. 81. Petitioner's arguments as to claim 15 (and 32) fail for the same reasons as described above as to claim 4 (and 20). In addition, the analysis of claim 4 Petitioner relies on for claim 8 does not establish, or even attempt to establish, that *generat[ion] of the response cryptogram [is] according to a card specification*. Instead, Petitioner merely alleges that EMV Specifications

“describe the inputs and responses by the card to be compatible with EMV transactions” and that it would have been “obvious to make the device inputs and responses conforming to ... EMV Specification.” Pet. 76. But nothing in this contention shows that conforming to, or being compatible with, EMV Specifications involves *generat[ing] the response cryptogram according to* EMV Specifications. As Dr. Fiske admitted, a transaction could comply with EMV Specifications even when generating a cryptogram using a technique that is **different** from the optional technique disclosed in the EMV Specifications. EX2009 ¶236; EX2035 at 61:21-62:1; EX2035 at 29:20-30:19.

J. Claims 17, 24, 25

Petitioner’s analysis of these claims in Grounds 3 and 4 rely on arguments Petitioner made with respect to claims 1 and 8 and fail for the same reasons. *See* Pet. 82-83.

Respectfully submitted,

Dated: June 28, 2024

/s/ Seth Lindner

Seth Lindner, Reg. No. 68,119

BC Law Group, P.C.

200 Madison Avenue, 24th Floor

New York, NY 10016

(212) 951-0100

CERTIFICATE OF WORD COUNT (37 C.F.R. § 42.24(d))

The undersigned hereby certifies that the word count in this Patent Owner Response is 13,595, as counted by the word-processing program Microsoft Word that was used to generate this Patent Owner Response, where such word count excludes the table of contents, table of authorities, mandatory notices, certificate of service, appendix of exhibits, claim listing, and this certificate of word count. This Patent Owner Response is in compliance with the 14,000-word limit set forth in 37 C.F.R. § 42.24(b)(1).

Date: June 28, 2024

/Seth Lindner/

BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100

Seth Lindner
Reg. No. 68,119
Attorney for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

The undersigned hereby certifies that the above document was served on June 28, 2024, by filing this document through the Patent Trial and Appeal Case Tracking System as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

Eliot D. Williams (Reg. No. 50,822)
Baker Botts L.L.P.
700 K Street, N.W.
Washington, D.C. 20001
Telephone: (202) 639-1334
eliot.williams@bakerbotts.com

Jennifer Tempesta (Reg. No. 59,021)
Baker Botts L.L.P.
30 Rockefeller Plaza
New York, NY 10112
Telephone: (212) 408-2571
jennifer.tempesta@bakerbotts.com

Date: June 28, 2024

/Seth Lindner/

BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100

Seth Lindner
Reg. No. 68,119
Attorney for Patent Owner