

IN THE 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

U.S. Patent No. 10,032,171

Inter Partes Review No. IPR2023-01289

PETITIONER'S REPLY

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

Submitted Electronically

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Collinge and Fiske are prior art	1
A.	Collinge Is Prior Art and Includes Disclosures From the Collinge Provisionals	1
III.	Petitioner’s Reliance on Emv and Other Payment Standards as Evidence of a POSITA’s Knowledge Is Appropriate	4
A.	EMV And PayPass Are Critical Background References That Even The ’171 Patent Relies on To Supply Necessary Disclosures	5
B.	Collinge and Fiske Both Are Written for POSITAs With Knowledge of the Background Standards.....	8
IV.	Grounds of Invalidity.....	8
A.	Grounds 1 and 2: Collinge in View of Knowledge of a POSITA	8
1.	Claim 1/17.....	8
a.	[1.A-3]	8
b.	[1.C]:.....	10
c.	[1.C]/[17.F]:.....	11
d.	[1.E-2]:.....	12
e.	[1.E-3]:.....	13
2.	Claim 10/27.....	16
a.	[10.B]/[27.B].....	18
b.	[10.C]/[27.C]:	18
3.	Claim 8/9.....	19
a.	[8.A]:.....	19
b.	[8.B]:.....	20
4.	Claims 4/20:	21
5.	Claim 15/32:.....	21
6.	Claims 6/22:	21
7.	Claims 16/33:	22

B.	Grounds 3 and 4: Claims 1-33 Are Anticipated and Obvious by <i>Fiske</i> in View of Knowledge of a POSITA	23
1.	Claim 8, 9.....	23
2.	Claims 10-13, 27-30.....	24
	a. “authorization data comprises the response cryptogram and the account identifier”	24
	b. “determining a...key associated with the account”	24
	c. “a calculated cryptogram”	24
3.	Claims 11/28, Claims 12/29:.....	25
4.	Claims 13/30:	25
5.	Claims 1/17	26
	a. [1.E-2]:.....	26
	b. [1.E-3]:.....	27
	c. [1.E-3]: EMV mode Visa transactions	28
6.	Claims 4, 5, 20, and 21	29
7.	Claims 6, 15, 22 and 32	30

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Advanced Display Sys., Inc. v. Kent State University</i> , 212 F.3d 1272 (Fed. Cir. 2000)	2
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359	4, 7
<i>C.R. Bard, Inc. v. Medline Indus., Inc.</i> , No. 2020-1900, 2021 WL 3574043 (Fed. Cir. Aug. 13, 2021)	19
<i>Comcast Cable Commc'ns, LLC v. Rovi Guides, Inc.</i> , No. IPR2017-01065, Paper 35 (P.T.A.B. Oct. 15, 2018)	4
<i>DeGeorge v. Bernier</i> , 786 F.2d 1318 (Fed. Cir. 1985)	4
<i>Dish Network L.L.C. v. Broadband Itv, Inc.</i> , IPR2020-01267, Paper 25 (P.T.A.B. Apr. 1, 2021)	7, 25
<i>Ex Parte Gary K. Michelson</i> , No. APPEAL 2012-004146, 2015 WL 5118373	4
<i>General Electric Co. v. Brenner</i> , 407 F.2d 1258 (D.C. Cir. 1968)	2
<i>Harari v. Lee</i> , 656 F.3d 1331 (Fed. Cir. 2011)	3
<i>Hybritech Inc. v. Monoclonal Antibodies, Inc.</i> , 802 F.2d 1367 (Fed. Cir. 1986)	18
<i>In re Hawkins</i> , 486 F.2d 569 (C.C.P.A. 1973)	2
<i>In re Lundak</i> , 773 F.2d 1216 (Fed. Cir. 1985)	2
<i>In re Paulsen</i> , 30 F.3d 1475 (Fed. Cir. 1994)	4, 19

<i>Intel Corp. v. Pact XPP Schweiz AG</i> , 61 F.3d 1373 (Fed. Cir. 2023)	9
<i>Intel Corp. v. Qualcomm Inc.</i> , 21 F.4th 784 (Fed. Cir. 2021)	9
<i>Paice LLC v. Ford Motor Co.</i> , 881 F.3d 894 (Fed. Cir. 2018)	3
<i>Randall Mfg. v. Rea</i> , 733 F.3d 1355 (Fed. Cir. 2013)	5, 7
OTHER AUTHORITIES	
37 C.F.R. § 1.14(a)(1)(iv)	3
37 C.F.R. § 1.14(a)(1)(iv)-(v)	3
37 C.F.R. § 1.14(a)(1)(v)	3

EXHIBIT LIST

Exhibit No.¹	Description
1001	U.S. Patent No. 10,032,171 (the “’171 Patent”)
1002	File History of the ’171 Patent
1003	U.S. Provisional App. No. 61/685,863
1004	U.S. Provisional App. No. 61/573,476
1005	U.S. Provisional App. No. 61/575,846
1006	Expert Declaration of Stuart Fiske
1007	Curriculum Vitae of Stuart Fiske
1008	Reserved
1009	U.S. Provisional App. No. 61/619,095 (“the ’095 Provisional”)
1010	U.S. Provisional App. No. 61/635,248 (“the ’248 Provisional”)
1011	U.S. Publication No. 2013/0262317 A1 to Collinge (“Collinge”)
1012	U.S. Patent No. 11,080,693 to Fiske (“Fiske”)
1013	Reserved
1014	U.S. Patent Publication No. 2010/153721 A1 to Mellqvist
1015	U.S. Patent Publication No. 2010/0252624
1016	U.S. Patent Publication No. 2012/0011070 A1 to Ward
1017	Reserved
1018	Declaration of Brian Byrne (“Byrne Declaration”)
1019	<i>EMV Integrated Circuit Card Specifications for Payment Systems, Book 1: Application Independent ICC to Terminal Interface Requirements</i> , Version 4.2 (June 2008) (Attachment A to Byrne Declaration)
1020	<i>EMV Integrated Circuit Card Specifications for Payment Systems, Book 2: Security and Key Management</i> , Version 4.2 (June 2008) (Attachment B to Byrne Declaration)
1021	<i>EMV Integrated Circuit Card Specifications for Payment Systems, Book 3: Application Specification</i> , Version 4.2 (June 2008) (Attachment C to Byrne Declaration)

¹ Citations to patents are made by column and line cite; citations to patent publications are made by paragraph number; citations to other exhibits are made with reference to the Bates-stamped pagination or inherent section numbers.

Exhibit No.¹	Description
1022	<i>EMV Integrated Circuit Card Specifications for Payment Systems, Book 4: Cardholder, Attendant, and Acquirer Interface Requirements</i> , Version 4.2 (June 2008) (Attachment D to Byrne Declaration)
1023	<i>EMV® Contactless Specifications for Payment Systems, Book A: Architecture and General Requirements</i> , Version 2.1 (March 2011) (Attachment E to Byrne Declaration)
1024	<i>EMV® Contactless Specifications for Payment Systems, Book B: Entry Point Specification</i> , Version 2.1 (Attachment F to Byrne Declaration)
1025	<i>EMV® Contactless Specifications for Payment Systems, Book C-1: Kernel 1 Specification</i> , Version 2.1 (March 2011) (Attachment G to Byrne Declaration)
1026	<i>EMV® Contactless Specifications for Payment Systems, Book C-2: Kernel 2 Specification</i> , Version 2.1 (March 2011) (Attachment H to Byrne Declaration)
1027	<i>EMV® Contactless Specifications for Payment Systems, Book C-3: Kernel 3 Specification</i> , Version 2.1 (March 2011) (Attachment I to Byrne Declaration)
1028	<i>EMV® Contactless Specifications for Payment Systems, Book C-4: Kernel 4 Specification</i> , Version 2.1 (March 2011) (Attachment J to Byrne Declaration)
1029	<i>EMV® Contactless Specifications for Payment Systems, Book D: EMV Contactless Communication Protocol Specification</i> , Version 2.1 (March 2011) (Attachment K to Byrne Declaration)
1030	Reserved
1031	Reserved
1032	Expert Declaration of Dr. Sylvia Hall-Ellis dated August 11 (“Hall-Ellis Declaration”) and Attachments
1033	Curriculum Vitae of Dr. Sylvia Hall-Ellis
1034	Carl H. Meyer, Stephen M. Matyas, <i>Cryptography: A New Dimension In Computer Data Security. A Guide for the Design and Implementation of Secure Systems</i> (1982)
1035	Reserved
1036	Reserved
1037	Cristian Radu, <i>Implementing Electronic Card Payment Systems</i> (2003)

Exhibit No.¹	Description
1038	Reserved
1039	Kefa Rabah, <i>Theory and Implementation of Data Encryption Standard: A Review</i> , Inform. Technol. J., 4: 307-325 (Apr. 2005)
1040	Smart Card Alliance, <i>Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?</i> A Smart Card Alliance Payments Council White Paper (Feb. 2011)
1041	Dom Morea, <i>EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions, A First Data White Paper</i> (2011)
1042	EMVCo FAQ webpage (Aug. 3, 2023, 11:43 AM), https://web.archive.org/web/20110920080137/http://www.emvco.com/faq.aspx?id=37
1043	Newton's Telecom Dictionary (25th ed. 2009)
1044	Ofcom: <i>Mobile not-spots. An update on our research</i> (Nov. 5, 2010)
1045	<i>OV Loop, Inc. v. Mastercard Inc.</i> , No. 7:23-cv-01773-CS, D.I. 31 (S.D.N.Y. June 8, 2023)
1046	Mike Clark, <i>SimplyTapp picks up contactless payments award</i> , NFCW (Aug. 25, 2015), https://www.nfcw.com/2015/08/25/337201/simplytapp-picks-up-contactless-payments-award/
1047	Payal Shukla, Jim Jarvie, <i>SimplyTapp Wins Best Contactless Payments Solution as Future Digital Awards</i> (Aug. 13, 2015), https://www.prweb.com/releases/2015/08/prweb12903489.htm
1048	U.S. Patent Pub. No. 2010/0190437A1
1049	Transcript of Deposition of Stuart Fiske
1050	Supplemental Expert Declaration of Stuart Fiske
1051	Transcript of Deposition of Chuck Easttom
1052	U.S. Patent No. 10,956,899
1053	U.S. Patent No. 8,370,258
1054	U.S. Patent No. 7,357,309
1055	U.S. Patent No. 6,718,314
1056	U.S. Patent Publication No. 20070012763
1057	U.S. Patent Publication No. 20030097344
1058	PayPass – Mag Stripe Technical Specifications, Version 3.3, December 2007

Exhibit No.¹	Description
1059	PayPass – M/Chip 4 Card Technical Specification, Version 1.3.1 - September 2008
1060	U.S. Patent Publication No. 20120160921
1061	U.S. Patent No. 10,902,399
1062	U.S. Patent Publication No. 20120185394
1063	International Standard ISO/IEC 14443-4 (2008)
1064	International Standard ISO/IEC 7816-4 (2005)
1065	International Standard ISO/IEC 7813 (2006)

I. INTRODUCTION

Patent Owner (“PO”)’s arguments reduce to three fallacies. First, PO argues that the disclosures of the Collinge Provisionals, which are expressly incorporated by reference in Collinge, are not part of Collinge’s disclosure. Second, PO argues that a person of ordinary skill in the art (“POSITA”) would not have used their background knowledge when reading and implementing the disclosures of the prior art, which expressly reference that background knowledge. Finally, PO argues that because the implementation approaches explicitly discussed in the most well-known payment card specifications in existence are described as “not mandatory,” a POSITA would not find those approaches obvious when implementing the prior art’s teachings. All of these arguments are legally flawed.

The ’171 Patent itself extensively cites existing payment standards and characterizes its invention as using a non-permanent key for generating response cryptograms in accordance with those standards. Ex[1002] 617-618. Both Collinge’s and Fiske do exactly that.

II. COLLINGE AND FISKE ARE PRIOR ART

A. Collinge Is Prior Art and Includes Disclosures From the Collinge Provisionals

PO’s argument that Collinge and its Provisionals (Exs[1009]-[1010]), which are expressly incorporated by reference into Collinge, are not prior art borders on the frivolous. PO’s argument appears to be that the material in the Collinge

Provisionals is “nonpublic information” and thus cannot be incorporated. POR, 8. PO relies on *General Electric Co. v. Brenner*, but that case supports Petitioner, not PO. 407 F.2d 1258 (D.C. Cir. 1968). There, the D.C. Circuit *reversed* the PTO’s ruling that the applicant could not incorporate materials from other patents, noting the Patent Office’s “[f]iling cabinets abhor redundancy.” *Id.* at 1263. Indeed, the Federal Circuit has expressly interpreted *Brenner* to mean material incorporated in patents becomes an invalidating disclosure. *See Advanced Display Sys., Inc. v. Kent State University*, 212 F.3d 1272, 1282-83 (Fed. Cir. 2000) (citing *Brenner* and holding that “[m]aterial not explicitly contained in the single, prior art document may still be considered for purposes of anticipation if that material is incorporated by reference”).

The CCPA and Federal Circuit have also rejected PO’s argument that incorporating allegedly “nonpublic” information is ineffective, holding that such information need only be public on publication/issuance. *See In re Hawkins*, 486 F.2d 569, 574 (C.C.P.A. 1973) (“the function of section 112 ...is only violated if the **disclosure** is not complete **at the time it is made public**, i.e., at the issue date”) (emphasis in original); *In re Lundak*, 773 F.2d 1216, 1222 (Fed. Cir. 1985) (disclosure requirements satisfied by “public access after grant” of the patent). The Collinge Provisionals have been public since at least publication of Collinge. Patent Office Rule 1.14 establishes that unpublished provisional applications become

publicly available either (1) if they are “identified in...a U.S. patent application publication,” or (2) “if the benefit of the [provisional] application is claimed...in...a U.S. application publication...”. 37 C.F.R. § 1.14(a)(1)(iv)-(v). Because both are true here, the provisionals are public information. Ex[1011], 1, 21.

Also flawed is PO’s argument that Collinge Provisionals’ disclosures were not sufficiently “carried forward” into Collinge. Collinge expressly identifies the provisionals by application number, filing date, and title, and states that the provisionals “are each ***incorporated by reference in their entirety.***”² Ex[1011] [0001]. The Federal Circuit has found even less clear incorporation language effective. *See Harari v. Lee*, 656 F.3d 1331, 1335 (Fed. Cir. 2011) (holding incorporation statement that read “The disclosures of the two applications are hereby incorporate[d] by reference” was “broad and unequivocal” and thereby sufficient to incorporate the entirety of the two patent applications into the document); *Paice LLC v. Ford Motor Co.*, 881 F.3d 894, 907 (Fed. Cir. 2018) (holding language identifying patent by number with statement that it “is incorporated herein by this reference” was “plainly sufficient to incorporate [the disclosure] in its entirety”).

More specifically, this Board routinely relies on disclosures of provisional applications so long as they are properly incorporated into and asserted together with

² Emphasis supplied throughout, unless noted.

the non-provisional application. For example, in *Comcast Cable Commc'ns, LLC v. Rovi Guides, Inc.*, No. IPR2017-01065, Paper 35 (P.T.A.B. Oct. 15, 2018), the Board rejected the arguments made by PO here. *Id.* at 19-21; *accord Ex Parte Gary K. Michelson*, No. APPEAL 2012-004146, 2015 WL 5118373, at *3-4 (P.T.A.B. Aug. 27, 2015).

PO's argument that Collinge or Collinge Provisionals are not prior art should be rejected.³

III. PETITIONER'S RELIANCE ON EMV AND OTHER PAYMENT STANDARDS AS EVIDENCE OF A POSITA'S KNOWLEDGE IS APPROPRIATE

Patents need not “explain every detail since [the author] is speaking to those skilled in the art.” *DeGeorge v. Bernier*, 768 F.2d 1318, 1323 (Fed. Cir. 1985). Because of that, prior art references must always be “considered together with the knowledge of one of ordinary skill in the pertinent art.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). The Federal Circuit has often held this to require the Board to consider background prior art provided to show how a POSITA would have read and understood the prior. As the court summarized in *Ariosa Diagnostics v. Verinata Health, Inc.*: “Art can legitimately serve to document the knowledge that skilled

³ Patent Owner has not reasserted its POPR argument regarding *Dynamic Drinkware* and does not argue that the relevant disclosures are missing in the provisionals.

artisans would bring to bear in reading the prior art identified as producing obviousness.” 805 F.3d 1359, 1365 (Fed. Cir. 2015); *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362-63 (Fed. Cir. 2013).

A. EMV And PayPass Are Critical Background References That Even The '171 Patent Relies on To Supply Necessary Disclosures

A POSITA reading Collinge and Fiske would have done so in light of their knowledge of common payment specifications, especially EMV,⁴ (Exs[1019]-[1029], collectively, “EMV Specifications”) and the brand-specific implementations of those EMV standards, such as Mastercard’s PayPass specification. Ex[1050] ¶12.

Indeed, the '171 Patent itself expressly relies on the POSITA’s knowledge of EMV and PayPass to provide necessary disclosure. For instance, the '171 Patent notes that the “details of an interrogation between a point-of-sale and a digital credential...are defined in ‘card specifications’... . Examples ...at the time of this filing are MASTERCARD *PAYPASS-Mag Stripe v3.3*, Contactless *EMV... .*” Ex[1001] 26:50-27:33, 49:32-39; 31:57-64; 25:50-62.

⁴ PO expert’s argument that EMV had low adoption in the U.S. is irrelevant. Ex[2009] ¶¶37-43. A POSITA would be motivated to build EMV-compliant products, due to its worldwide importance and expected adoption in U.S. terminals. Ex[2009] ¶37; Ex[1050] ¶13; Ex[1041], 2.

A POSITA would understand the '171 Patent's reference to "PayPass Mag Stripe v3.3" and "MCHIP", to refer to MasterCard contactless payment standard (compliant with the EMV Specifications)⁵ known as the "PayPass Specifications," including, for a POSITA around the time of the priority date, both the PayPass-MagStrip⁶ Technical Specification version 3.3 ("PayPass-MagStripe") and PayPass-M/Chip Card Technical Specification version 1.3.1 ("PayPass-M/Chip"). Ex[1050] ¶16, Exs[1058]-[1059]. Both PayPass Specifications were published by 2008, and a POSITA reading either the '171 Patent or Collinge would be familiar with them. Ex[1058], 1; Ex[1059], 1; Ex[1050] ¶¶16-17. The PayPass specifications were provided, upon request, to "[Mastercard] members and their authorized agents," as well as "[c]ustomers and vendors" and others in the field. Ex[1058], 9; Ex[1059], 5. A POSITA's knowledge of the PayPass Specifications is corroborated by numerous contemporary patent publications. See Ex[1053] 10:47-52; Ex[1060] [0001];

⁵ PayPass-MagStripe states that "[i]t is *assumed that readers ...already have an understanding of... EMV...*" Ex[1058], 9. PayPass-M/Chip is similar. Ex[1059], 35. The PayPass Specifications are EMV-compliant. Ex[1050] ¶15, Annex A.

⁶ A POSITA would understand "MagStripe" here refers to EMV-compliant transactions conducted in EMV "MagStripe *mode*." Ex[1050] ¶16; Ex[1058], 1, 9; Ex[1026] §§1.5.7, 3.4.2; Ex[1058], 36.

Ex[1061] 6:60-66, 7:40-60; Ex[1062] [0134]. Indeed, '171 Patent ***repeatedly refers to, and in some cases outright copies***, excerpts from the PayPass Specifications into its specifications. See Ex[1001] 7:2-20; 24:50-54, 26:55, 29:30-33; Fig.2., Ex[1050] Annex B.

The POSITA's familiarity with EMV is also corroborated by contemporaneous patents. See *e.g.* Ex[1052] 4:56-57; Ex[1053] 5:14-40, 10:47-52; Ex[1054] 3:33-44; Ex[1055] 45:33-35; Ex[1056] [0045]; Ex[1057] [0287].

Accordingly, a POSITA would be expected to already have background knowledge regarding the EMV standard and would find implementing payment systems using those techniques obvious. Ex[1050] ¶20.

Thus, contrary to PO's argument (POR, 21-22) EMV standard practices and implementations of those practices in known commercial standards must be considered here. *Id.* ¶21. See *Dish Network L.L.C. v. Broadband Itv, Inc.*, IPR2020-01267, Paper 25 at 15 (P.T.A.B. Apr. 1, 2021) ("we do not see why, even if the CableLabs specification is not incorporated by reference in Gonder itself, it cannot be considered as showing the background knowledge that a [POSITA] would have had in reading Gonder"); *Randall*, 733 F.3d at 1362-63 (holding that Board erred in "ignoring the additional record evidence ... to demonstrate the knowledge and perspective of one of ordinary skill art," describing such evidence as "critical background information" the Board must consider); *Ariosa Diagnostics v. Verinata*

Health, Inc., 805 F.3d 1359, 1365 (Fed. Cir. 2015) (holding Board cannot refuse to consider background art teachings “simply because [the background art] had not been identified [as] defining a combination for obviousness”).

B. Collinge and Fiske Both Are Written for POSITAs With Knowledge of the Background Standards

The Collinge Provisionals state the disclosures therein are intended to be used in a “standard” PayPass transaction. Ex[1009] 8, 14-15, 22-23. Therefore, a POSITA would consider the PayPass Specification (and EMV Specifications, with which the PayPass Specification complies) when reading Collinge. Ex[1050] ¶22.

Similarly, Fiske explicitly informs the reader that it provides “improved methods ... *without requiring modification of the EMV infrastructure...*” and notes the techniques are to be used in conducting “an EMV transaction”. *Id.* 2:54-59; Abstract; 1:20, 57-64; 2:54-59, 67; 3:1-25, 46-62; 6:54-60; 7:20-23, Fig. 3; 8:40-42, Fig. 4; col.9, *passim*; 10:54-56; 12:49-52; 13:32-42; 15:55-58; 17:10-15. Accordingly, a POSITA reading Fiske would have invoked background knowledge about EMV Specifications when reading and implementing Fiske’s disclosures. Ex[1050] ¶23.

IV. GROUNDS OF INVALIDITY

A. Grounds 1 and 2: Collinge in View of Knowledge of a POSITA

1. Claim 1/17

a. [1.A-3]

PO argues that Collinge’s request for payment credentials, which includes the CAP token, is somehow not a request. POR, 13-17. This argument is irrelevant and technically flawed. It is irrelevant because the Petitioner did not rely solely on the CAP token transmission, but also on Collinge’s disclosure that credentials are sent in response to a “pull **request** from the mobile device,” Pet., 40 (citing Ex[1009], cl.19), and that requesting information necessary to conduct a transaction was an obvious way to obtain that data among the finite, predictable options. Pet., 40, 42.

As to the latter point, PO’s does not rebut Petitioner’s showing, but merely speculates about some other purported “alternatives.”⁷ POR, 15-16. That is insufficient to overcome Petitioner’s showing of obviousness. *See Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 800 (Fed. Cir. 2021) (“It’s not necessary to show that a combination is the best option, only that it be a suitable option.”) (cleaned up); *Intel Corp. v. Pact XPP Schweiz AG*, 61 F.4th 1373, 1380-81 (Fed. Cir. 2023).

PO’s argument is technically flawed because the CAP token transmission **is** a request for the payment credentials. The CAP token does not trigger any process at the server other than one for generating and returning the encrypted payment credentials to the device. Ex[1011] [0081]-[0085]; Ex[1050] ¶25. The fact that the

⁷ A POSITA would likely find flaws in PO’s purported alternatives. Ex[1050] ¶¶27-28; Ex[1044] ¶¶ 4.41-4.43.

multiple steps are performed before responding (including authenticating the CAP token to verify that the mobile device is authorized to receive the requested payment credentials), does not take the request outside the scope of the claims. *Id.*

b. [1.C]:

PO argues that Collinge's non-permanent cryptographic key (KS_{UN}) is not "associated with the account" because a POSITA could not recover the account number from the key. POR, 18. This argument is not commensurate with the scope of the claims, which do not require that the account number be known or recoverable from the key, but only require that the key be "associated with the account." Ex[1050] ¶29. The Petition sets forth three separate ways in which Collinge's key is associated with the account, none of which PO substantively addresses.

KS_{UN} is uniquely, mathematically, and deterministically associated with the account, because it is generated from a card-level key KD_{UN} , which is in turn generated from the account number (PAN).⁸ Ex[1050] ¶30; Ex[1009] [0069]-[0071]. In other words, a POSITA would know, mathematically, that a different PAN would

⁸ PO's expert appears to assert that KS_{UN} is not associated with an account because the PAN is truncated in Collinge. The only digits truncated are not part of the account identifier, so the truncated value ***still uniquely identifies the account***. Ex[1009] 26-27; Ex[1050] ¶31; Ex[1021], 45, 150; Ex[1065] §7.4.1.

result in a different KD_{UN} , which would in turn result in a different KS_{UN} , even if other variables (e.g. the transaction counter ATC) are the same. *Id.*

c. [1.C]/[17.F]:

Contrary to PO's assertion (POR, 20), the Petition points to the encrypted payload in Collinge for this limitation. Pet. 43. In particular, as the Petition explains in §[1.A-3], referred to in §[1.C], the remote-SE system would “generate and return payment credentials in an encrypted payload,” which includes a single use key for generation of a CVC3 cryptogram or Application Cryptogram (AC). *Id.* 39, 43. Details of how it is used to formulate an APDU response are explained where that is separately claimed. Pet., 48-50 (addressing [1.E-3]).

Further, as Collinge is enabling a PayPass (EMV-compliant) transaction (*supra* §III.B,) a POSITA would know to use APDU messages (nearly all smart card payment systems at that time did and still do globally). *Supra* §III.A; Ex[1058] §§III.3.1, III.3.3; Ex[1059] §2.4.1; Ex[1021] §§6.1-6.2; Ex[1037], 46-47; Ex[1050] ¶33. A POSITA would know that APDUs are simply standardized messages exchanged between smart cards and smart card POS terminals, that any response message, including the cryptogram, would be conveyed via an APDU. Ex[1050] ¶34. Accordingly, as explained in the Petition, “it would be obvious to implement Collinge” using “command-and-response-application protocol data units” to “ensure interoperability” with the payment network. Pet., 43-44.

d. [1.E-2]:

PO again relies on its flawed argument about incorporation of the Collinge Provisional disclosures into Collinge. POR, 23. Collinge, via its incorporation of the Collinge Provisionals, recites an explicit formula for CVC3⁹ generation by using KS_{UN} as an encryption key to perform DES3 cryptographic operation:¹⁰

2. Calculate T as follows:

$T := DES3(KS_{UN})[M]$

The two least significant bytes of T are the $CVC3_{TRACK1/2}$

⁹ PO's assertion that "Petitioner offers no explanation as to how a [Message Authentication Code] is relevant to the generation of a payment CVC3 value" is frivolous. Multiple pages of the petition are devoted to that analysis. *See* Pet., 18-19, 56; Ex[1020], 100 (equating the "Application Cryptogram" with a "Message Authentication Code (MAC)"); 141 (describing MAC generation); 149 (approving DES3 for MAC generation).

¹⁰ Collinge improved upon PayPass-MagStripe by using a one-time cryptographic key KS_{UN} , rather than static key (e.g. KD_{CVC3}) for generation of the application cryptogram/MAC (CVC3), while maintaining compatibility with the existing PayPass-MagStripe terminal infrastructure/payment messaging. Ex[1058] §III.3.8.1; Ex[1009], 28; *compare* Ex[1009] 29-30 (CVC3 generation) *with* Ex[1058] §III.3.8.2; Ex[1050] ¶35.

Ex[1009], 29-30. As explained by Dr. Fiske and further demonstrated by the step-by-step analysis of DES generation of a cryptogram in Exhibit 1039, Collinge's CVC3 would not contain KS_{UN} . Ex[1050] ¶35.¹¹

Indeed, it is also only common sense that the result of cryptographic calculations like DES3 would not include the key—otherwise anyone with the cryptogram could use the included key to create a valid yet fraudulent payment request—undermining the entire purpose of using encryption for this in the first place. Ex[1050] ¶36. Therefore, a POSITA would understand or find it obvious that Collinge's CVC3 does not include the cryptographic key.

e. [1.E-3]:

Other than its flawed premise that Collinge Provisionals' disclosures are not prior art, PO's argument here is based purely on a lack of the POSITA's common knowledge. PO argues that a POSITA would not know that PayPass, which Collinge enables, is EMV-compliant or that Exhibit 1026 describes a "Mastercard" card interrogation. POR, 25-28.

¹¹ Patent Owner attacks the relevance of Ex[1034] and Ex[1039]. POR, 23-24. Ex[1034] demonstrates that it was common knowledge that MACs (which include CVC3) are calculated using DES algorithms, while Ex[1039] shows that DES (used for MAC) generates an output that excludes the key. Ex[1050] ¶35 n.2.

As to the first issue, CVC3 and Application Cryptogram (AC) are well known in the art to be names of response cryptograms generated by the payment application for authorization of a transaction in an EMV-compliant transaction. Ex[1050] ¶38; Ex[1037], 54, 57; Ex[1052], 14:63-65. As to the second issue, a POSITA would know that Ex[1026], which relates to “Kernel 2,” describes POS terminal interactions with a Mastercard-branded smart card. See Ex[1026], 23 (“this document defines the behavior of the Kernel used in combination with card supporting a MasterCard brand...”); Ex[1050] ¶38.

A POSITA reviewing Collinge would be familiar with the PayPass Specification, and know that PayPass is Mastercard’s implementation of contactless EMV-compliant transactions (*supra* §III.A; Ex[1050] ¶15, Annex A), and/or find it obvious to implement Collinge to be EMV-compliant (Ex[1050] ¶39; Ex[1026], §§3.4.2, 3.4.3, 3.8.1–3.8.3, 5.2, 5.3). This is corroborated by the PayPass Specifications, which provide the same response APDUs including the ones satisfying the first construction.¹² Ex[1050] ¶39; Ex[1058] §II.3.1 (steps 6 & 8). Further, a POSITA would also know that in Visa transactions under EMV, in

¹² Both parties agree for this proceeding that claim term “application data protocol unit” (ADPU) should be read as an “application protocol data unit” or APDU. Ex[1050] ¶39 n.3; Ex[1051] 85:25-86:17.

response to the GPO command, the “card” may return an AC in the same message with the Track 2 Equivalent Data with the PAN, satisfying the second construction. Ex[1050] ¶39; Ex[1027] §§2.4.1, 5.2.2.3, 5.4.3.2, Table E-6.

Finally, a POSITA could easily implement Collinge based on knowledge of PayPass and EMV, since Collinge itself specifically informs the reader to conduct PayPass (which is EMV-compliant) transactions. *Supra* §III.B. Once the mobile device (card) receives KS_{UN} , it can generate a response cryptogram ([1.E-2]), whether it is CVC3 (explicitly disclosed by Collinge and EMV MagStripe-mode, Ex[1009] 29-30; Ex[1026] §3.4.2), or an EMV-mode Application Cryptogram.¹³ Ex[1050] ¶40. Once the card generates the response cryptogram, it is only a matter of following practices well known in the art to decide whether to send it back to the POS terminal in a separate message (when conducting a Mastercard transaction) or include it in the same response as Track1/2 data (Visa). Ex[1050] ¶41; Ex[1058] §II.3.1; Ex[1027] §§2.4.1, 5.2.2.3, 5.4.3.2, Table E-6. Accordingly, a POSITA

¹³ KS_{UN} is a 16-byte value, Ex[1020] §A1.3.1, and thus a POSITA would understand the author’s intent was to (and would be motivated to/can successfully) use KS_{UN} directly as the 16-byte AC Session Key in the EMV AC computation process, without modification. Ex[1050] ¶40; Ex[1020] § 8.1.2.

would reasonably expect success when implementing Collinge’s techniques for PayPass or EMV-mode transactions. Ex[1050] ¶41.

2. Claim 10/27

PO’s argument appears to be that the “remote computer system” in Collinge is limited to the red box in the PO-supplied annotation below:

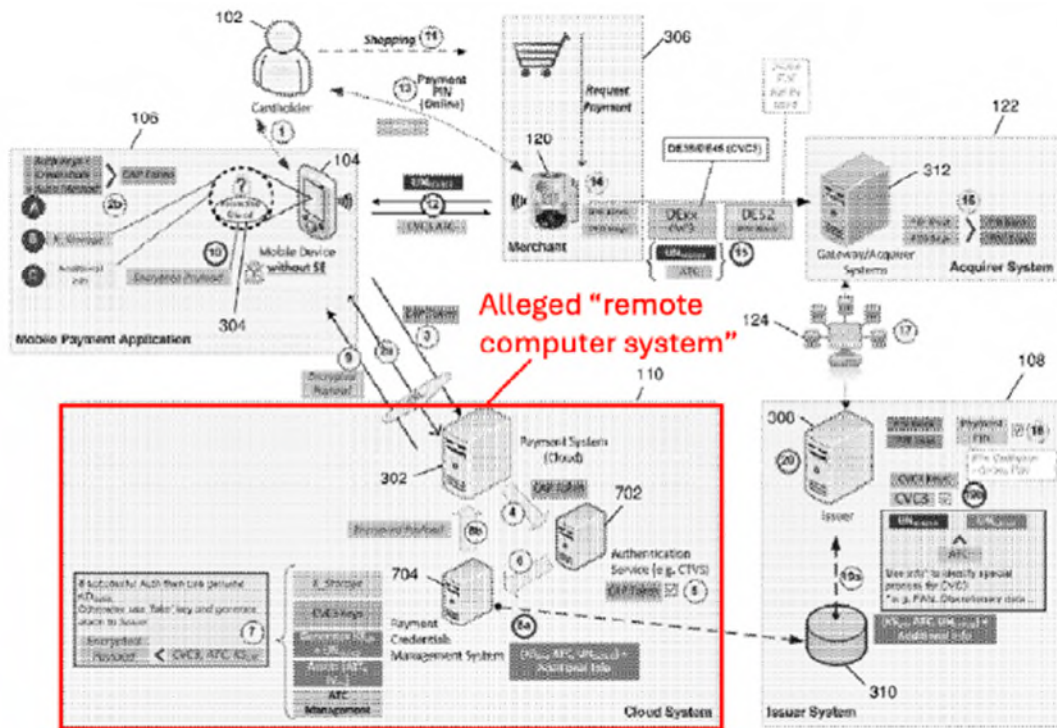


FIG. 7

POR, 31. However, the Petition never limited the mapping of the claimed “remote computer system” to PO’s red box. To the contrary, the Petition mapped functionality performed in at least the structures identified below in the blue box (which are expressly stated and shown to share a “connection 178” therebetween) as corresponding to the functions of the remote computer system:

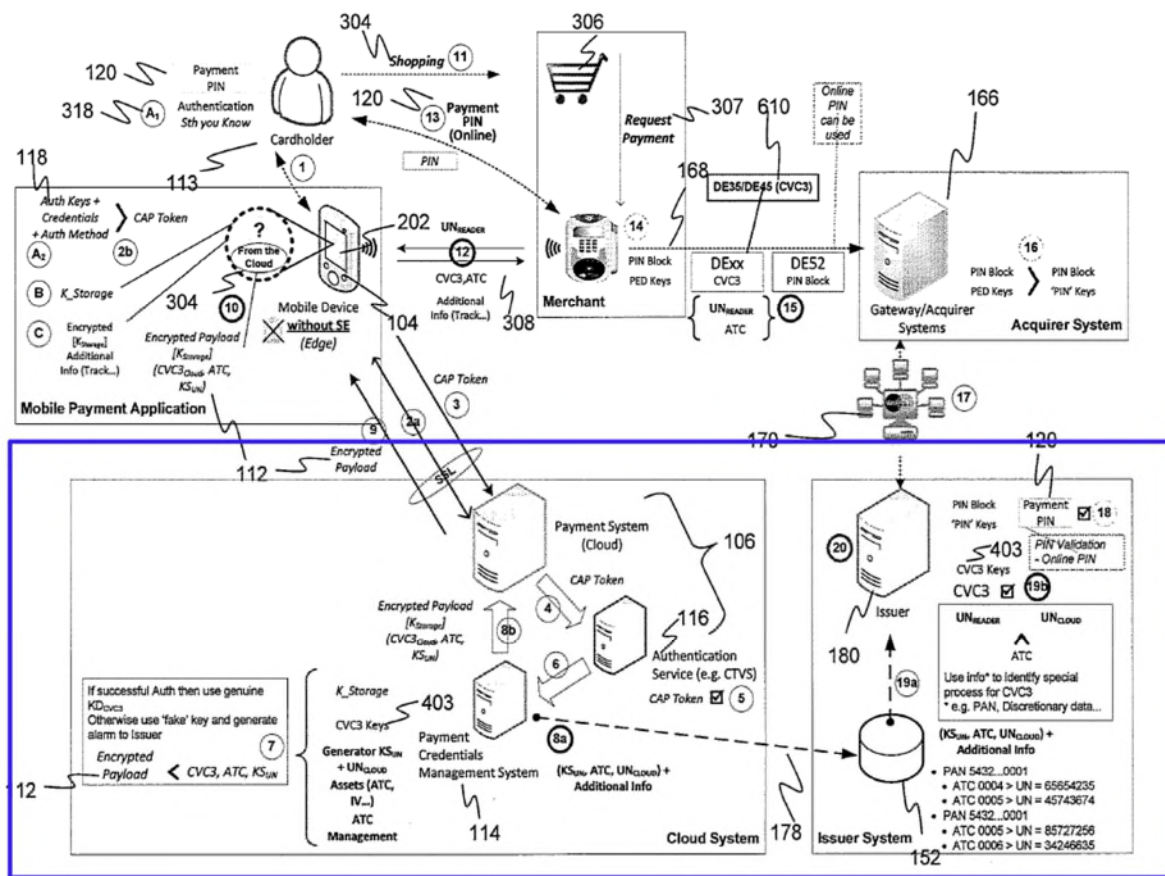


FIG. 7

Ex[1009] [0046] and Fig. 7; Pet., 38-41 (mapping functions of claim 1 performed by the “remote computer system” to the “remote system” on the bottom of the figure), 58-59 (mapping functions of claim 10 performed by the “remote computer system” to the part of the “payment network” that allows the “issuer to authorize the transaction and associate it with the correct account” which is in the blue-boxed portion).

Nor did Dr. Fiske limit his analysis of the “remote computer system” to the red-boxed area during his deposition. Dr. Fiske explained, “computer system” is a very loose term and there is no fixed number of computers such that one computer system can or should include. Ex[1049], 25:25-26:8; Ex[1050] ¶44. He merely acknowledged that the functionality expressly recited in claim 1 was performed in Collinge’s remote-SE, which, as shown above, is in the blue-boxed portion of the remote computer system. *Id.*; Ex[1049] 73:3-75:9.

a. [10.B]/[27.B]

Contrary to POR’s assertions, POR 34-35, Collinge Provisionals do not teach that retrieval of KS_{UN} is done using **only** the ATC. Ex[1009] 23. A POSITA would understand that the issuer must use an account identifier such as a PAN to retrieve or re-calculate (“determine”) the correct key because, as explained, KS_{UN} is generated uniquely with and for a PAN and is specific to a PAN. *Supra* §IV.A.1.b; Ex[1050] ¶45.

b. [10.C]/[27.C]:

PO argues that Collinge’s statement that “[m]ethods for validating a CVC3 will be apparent to persons having skill in the relevant art,” Ex[1011] [0087], serves to “expressly omit[]” details of validation. POR, 36. This is without merit because a patent “need not teach, and preferably omits, what is well known in the art,” *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1384 (Fed. Cir. 1986);

C.R. Bard, Inc. v. Medline Indus., Inc., No. 2020-1900, 2021 WL 3574043, at *6 (Fed. Cir. Aug. 13, 2021) (Board erred when it “demanded express guidance from individual references and did not consider the knowledge and creativity of a skilled artisan.”); *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (prior art “need not ... explain every detail...”).

Collinge’s statement that the technique for validating a message authentication code, such as CVC3, was “apparent” to a POSITA, is corroborated by the cited payment-textbook, showing this technique for verifying a cryptogram is so basic as to defy misunderstanding. Ex[1050] ¶47; Ex[2037] 57-58. Regardless, as explained in the Petition, the most obvious way to implement Collinge would be to recalculate the CVC3 and verify that value matches the received one. Pet., 59.

3. Claim 8/9

a. [8.A]:

PO argues that Collinge does not explicitly mention the PAN as part of the encrypted payload. *Id.* 38-39. As explained in the Petition, Collinge discloses receiving from a remote-SE all necessary “payment credentials” to create a transaction request message including “account information (e.g. PAN)” (Pet., 38-39). Indeed, the Petition specifically cites to Collinge [0009] as explaining what “payment credentials” are received from the remote computer system. Pet., 43. That paragraph also suggests that the remote system sends “static payment credentials”

(which a POSITA would understand include the account number) as well as the dynamic KS_{UN} .

Moreover, because the non-permanent cryptographic key is specific to an account and only usable for the associated account, *see also supra* §IV.A.1.b, it would be obvious to send an account identifier along with the key, so that the mobile device knows which account's key it is receiving, which a POSITA would understand would be useful when designing a card capable of being used with multiple accounts or a credential wallet usable with multiple accounts. Ex[1050] ¶48.

b. [8.B]:

For this, the Petition refers back to §X.A.1.j of the Petition, which describes that a new KS_{UN} is required for each transaction (interrogation). Pet., 51-52, 57. Contrary to PO's assertions (POR, 40), KS_{UN} in Collinge is not generated by the mobile device (and indeed could not be, because the mobile device does not know UN_{CLOUD} —an input to the KS_{UN} generation formula) (Ex[1009], 27-28 (“ UN_{CLOUD} is **not** sent to the Mobile device”), and is instead generated at the remote computer system. Ex[1011] [0083]. Therefore, a POSITA would readily understand that, logically and obviously, when the mobile device uses up the one-time key KS_{UN} ***after an interrogation*** (i.e. transaction), it should request a new KS_{UN} for the next transaction, and in response, the remote computer system would generate and send a new KS_{UN} for that account. Ex[1050] ¶49; Pet., 38-40.

4. Claims 4/20:¹⁴

The Collinge Provisionals state that the invention enables PayPass transactions, where interrogation is standardized, including by the PayPass Specification (*supra* §III.B), which a POSITA would understand, as evidenced by the '171 Patent itself. Ex[1050] ¶50; Ex[1058] §II.3. PO's argument ignoring the Collinge Provisionals, again, is without merit. *Supra* §II.A.

Similarly, PO's argument that the Collinge Provisionals fail to mention "m/chip" is irrelevant. A POSITA at that time understood that PayPass Specifications include PayPass-M/Chip, published in September 2008. *Supra* §III.A. Ex[1050] ¶51. Also, the PayPass-M/Chip specification is admitted contactless prior art. Ex[1001] at 25:50-63, 31:55-60.

5. Claim 15/32:

Supra §IV.A.4.

6. Claims 6/22:

The Petition showed how the Collinge Provisionals' disclose the "DES3" algorithm is used to calculate the cryptogram. Pet., 56 (citing Ex[1009], [0071]):

2. Calculate T as follows:

$$T := \text{DES3}(KS_{UN})[M]$$

¹⁴ Petitioner assumes PO meant claim 20, not 21.

PO's argument that other algorithms might be used is irrelevant. A POSITA need not, as PO argues, "cho[o]s[e]" DES, when the standard specifications already did. POR 46, Ex[1050] ¶¶55-56.

7. Claims 16/33:

PO relies again on its incorrect argument that Collinge's incorporated disclosures are not prior art. (POR, 46-48). *See supra* §II.A. Also, the use of Issuer Master Keys to derive keys used to generate MAC cryptograms is a fundamental principle known to POSITAs. Pet., 62; Ex[1011] [0083]; Ex[1020] §§8.1.2, A1.3.1, A1.4; Ex[1037], 58; Ex[1050] ¶¶57-58.

Contrary to PO's mischaracterizations, Dr. Fiske did not say that Collinge departed from EMV's key derivation approach of using issuer master keys in session key derivation. *Cf.* POR, 48-49. He merely noted that Collinge uses ***an additional piece of data*** (UN_{CLOUD}) in that process, which is not prohibited by the EMV standard. Ex[1049] 77:12-78:17; Ex[1020] §§8.1.2, A1.3-A1.4; Ex[1050] ¶58. Fundamentally, a POSITA would understand or find this element obvious because the issuer must control the ultimate key (IMK) used to derive all other keys for security and efficiency reasons. Ex[1050] ¶58.

B. Grounds 3 and 4: Claims 1-33 Are Anticipated and Obvious by Fiske in View of Knowledge of a POSITA¹⁵

1. Claim 8, 9

PO's argument that Fiske does not disclose sending the account identifier to the mobile device is without merit. The Petition expressly notes that Fiske (like Collinge in Ground 1), involves receiving "'digital credential data' required for authorization" including the "primary account number (PAN)" from the remote server. Pet., 66-67. Moreover, the Petition explains how this PAN would be included with the cryptogram by the card when requesting payment authorization. *See* Pet., 50, 72-73; Ex[1012] at 11:34-44 (discussing provisioning the user device with data sufficient to make a purchase); 3:44-46 (discussing PAN sent to terminal from the mobile application); 4:49-41 (discussing the mobile application sending the account number to the terminal during a transaction).

Like Collinge, the non-permanent cryptographic key in Fiske (ICC Session Key) is specific to an account and only usable for that account. Pet. 59-70; *see also* Ex[1012], 12:45-52, 12:50-57, 13:17-24. Therefore, a POSITA would find it obvious to send an account identifier to the mobile device along with the key, so that the mobile device knows which account's key it is receiving. Ex[1050] ¶60; *see supra* §IV.A.3.a.

¹⁵ Petitioner follows PO's order of arguments.

2. Claims 10-13, 27-30

a. “authorization data comprises the response cryptogram and the account identifier”

PO ignores the analysis of this element incorporated the analysis of claim 1. The Petition explains that the device receives all data necessary to perform a transaction, including the PAN (needed by the issuer to associate the transaction with an account for financial tracking) and the cryptogram/MAC (needed by the issuer to verify the request’s authenticity). *See supra* §IV.B.1; Ex[1037] 57; Ex[1050] ¶¶61-62.

b. “determining a...key associated with the account”

The Petition noted that Fiske discloses that the issuer identifies “which Session Key was used” when determining whether to authorize the transaction. Pet., 79 (citing Ex[1012], 16¹⁶:13-14;Fig. 7). Figure 7, in turn, shows the issuer examining the received ARQC, an Application Cryptogram for authorization. This claim element requires nothing more. Ex[1050] ¶63.

c. “a calculated cryptogram”

The issuer’s verification of the received MAC/cryptogram by recalculating the expected cryptogram and comparing it to the received one is ancient and obvious.

¹⁶ The Petition inadvertently cited to 17:13-14. The correct citation was clear from the quoted passage.

Ex[1050] ¶64; Ex[1037] 58; *supra* §IV.A.2.b. The Petition’s analysis of this point was clear.

3. Claims 11/28, Claims 12/29:

The EMV specifications are clearly part of the POSITA’s background knowledge and must be considered when interpreting Fiske’s disclosure. *Supra* §§III.A-III.B; *Dish Network L.L.C.*, IPR2020-01267, Paper 25 at 15; Ex[1012] 2:54-59 (Fiske stating his invention works “without requiring modification of the EMV infrastructure.”); Ex[1050] ¶65.

Also, regardless of whether the portions of the EMV specification are mandatory or merely suggested, they teach this claim element: listing “Unpredictable Number” among input data from the terminal used to generate the cryptogram (Ex[1020] §8.1.1), which is repeated by the issuer when verifying the cryptogram. Ex[1037] 57-58. Ex[1050] ¶66. A POSITA understands that the “response cryptogram” is the cryptogram generated by the mobile device (card) in response to a COMPUTE CRYPTOGRAPHIC CHECKSUM, a GENERATE AC, or a GPO command. Ex[1050] ¶66; Ex[1026] §§3.4.2, 3.4.3, 5.2, 5.3; Ex[1027] §2.4.1. This knowledge is further corroborated by EMV Specifications cited above and renders this element known or obvious to a POSITA. Ex[1050] ¶66.

4. Claims 13/30:

PO's argument here again borders on the frivolous. The entire point of the authorization in any "payment system" (the title of Fiske's invention) is for the account issuer to authorize a transaction, which means the issuer must receive the transaction data, such as the amount user is attempting to spend, and in which currency, to determine whether to permit the payment. Pet., 80-81; Ex[1006] ¶214; Ex[1050] ¶67. This is textbook knowledge. *Id.*; Ex[1037] 58 (Authorization request includes "[a]ll the data objects necessary to **reproduce the transaction claim.**"). PO's expert is of no help to it, as he ignores the claim language, which speaks of what is included in the authorization data, not what is required for validation of cryptogram, and he is wrong in any event in asserting that validation of cryptogram does not require transaction values, not to mention that these values are necessary for authorization. Ex[1050] ¶68 (citing Ex[2009] ¶234); Ex[1020] §§8.1.1-8.1.2.

5. Claims 1/17

a. [1.E-2]:

Because the Application Cryptogram (AC) is generated using the Session Key as **encryption key** (Pet., 72), a POSITA would know, even without knowing **how** the AC is generated, that the encryption key will not be included in the resulting cryptogram; otherwise anyone with the cryptogram could use the included key to create a fraudulent payment request—undermining the entire purpose of using cryptography. Ex[1050] ¶69. In any event, a POSITA knows that EMV uses DES3

to generate AC, which does not contain the key. Ex[1050] ¶70; Ex[1020] §§A1.2, B1.1. Ex[1039] 9, 14 (showing DES algorithm resulting in a cryptogram not including the key).

b. [1.E-3]:

PO's argument ignores the well-known fact that it is essentially a ***universal practice*** to communicate with payment terminals using APDUs. Ex[1050] ¶71; Ex[1058] §II.3.1; Ex[1021] §6.5; Ex[1026] Table 2.2; Ex[1037] 55-56. PO failed to provide any evidence to the contrary.

EMV contactless transactions use these long-established communication protocols. Ex[1050] ¶72; *compare e.g.* Ex[1026] §5 and Ex[1058] §§III.2-III.3 with Ex[1021] §6.5 (using contact APDU commands and responses for contactless). Contactless cards still depend on APDUs from ISO/IEC7816-4, Ex[1064], for messaging, as reflected in the contactless EMV Specifications. Ex[1050] ¶72; Ex[1063], 6; Ex[1024], 9. Even the '171 Patent itself acknowledges this. Ex[1001] Table 1 (annotated).

TABLE 1

	ISO/IEC 7816 (contact)	ISO/IEC 14443 (contact less)	+	OSI- Layer
Application commands (APDUs)	7816-4			7
Transport protocols, Activation, Bit Transmission, Powersupply	7816-3	↔ 14443-4	Transport- protocol	4
		↔ 14443-3	Anticollision, Activation	2
		↔ 14443-2	Powersupply, Bit Transmission	1
Contacts	7816-2	↔ 14443-1	Phys. properties	
Phys. properties	7816-1			

c. [1.E-3]: EMV mode Visa transactions

EMV mode Visa transactions satisfy this element under the second construction of the R-APDU Term, Pet., 50, 73. Both the Petition and Dr. Fiske’s testimony made clear that “[f]or similar reasons, *as Grounds 1-2, [1.E-3]*, a POSA would have found this element obvious.” Pet. 73, Ex[1006] ¶184. The Petition explained in Grounds 1-2, [1.E-3] how an EMV mode Visa transaction worked—specifically, the mobile device (card) would return both account number information (track data) and the cryptogram in the same R-APDU message in response to a GPO command. Pet. 50. This explanation applies to Collinge as well as to Fiske, because it explains how *EMV* works, and Fiske enables EMV transactions. *Supra* §III.B.

PO's purported ignorance as to "why" a POSITA would choose to implement Fiske (a patent assigned to Visa) to conduct an EMV mode Visa transaction shows the meritlessness of its position. POR, 69-70. Aside from Fiske's explicit teaching, Ex[1012], 2:54-59, POSITA would recognize the benefit of offering a system that would be interoperable with one of the most prevalent payment brands in the world, such that Visa card issuers and card holders could take advantage of the offering easily. Ex[1050] ¶74.

Finally, PO argues that EMV mode Visa transaction is not consistent with Fiske, pointing to a section of the standard that is neither cited by Petitioner nor relevant to any issue here. The section PO points to (§6.1 of Ex[1027]) relates to a processing flow where the payment card is required to be presented twice to the terminal in order to perform "update processing." Ex[1027], 83-84; Ex[1050] ¶75. PO fails to explain how "update processing" has any relevance to Petitioner's arguments. Regardless, Petitioner's mapping involving Visa-mode contactless transactions relies on the cryptogram generation occurring in response to the Get Processing Options (GPO) command. *See* Pet., 50, 73.

6. Claims 4, 5, 20, and 21

As explained above, a POSITA reading Fiske would understand it was meant to be implemented using standard EMV practices and, thus knows or finds it obvious to conform with EMV Specifications. *Supra* §III.B.

7. Claims 6, 15, 22 and 32

PO's argument that portions of the EMV Specification that are "not mandatory" somehow does not render those implementations obvious is legally erroneous. *See supra* at 9 (citing both *Intel* cases).

Date: September 20, 2024

Respectfully submitted,

/ Eliot D. Williams /
Eliot D. Williams (50,822)

CERTIFICATE OF SERVICE

The undersigned hereby certifies on this 20th day of September, 2024, that true and correct copies of the foregoing Reply and supporting exhibits were served in their entirety on the following parties via electronic mail:

Seth Lindner (Reg. No. 68,119)
Email: slindner@bc-lawgroup.com
Brett Cooper (Reg. No. 55,085)
Email: bcooper@bc-lawgroup.com
BC Law Group, P.C.

Robert A. Auchter (Reg. No. 38,069)
robert@auchterlaw.com
Auchter PLLC

Spencer Hosie (pro hac vice)
shosie@hosielaw.com
Diane S. Rice (pro hac vice)
drice@hosielaw.com
Darrell Atkinson (pro hac vice)
datkinson@hosielaw.com
Hosie Rice LLP

BAKER BOTTS L.L.P.

/ Eliot D. Williams /
Eliot D. Williams (Reg. No. 50,822)
Lead Attorney for Petitioner

Date: September 20, 2024

Baker Botts L.L.P.
700 K Street, N.W.
Washington, D.C. 20001
Telephone: (202) 639-1334
eliot.williams@bakerbotts.com

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME
LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE
REQUIREMENTS**

1. This Reply complies with the type-volume limitation of 5,600 words, comprising 5,583 words, excluding the parts exempted by 37 C.F.R. §42.24(c).
2. This Reply complies with the general format requirements of 37 C.F.R. §42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman.

Respectfully submitted,

BAKER BOTTS L.L.P.

/ Eliot D. Williams /

Eliot D. Williams (Reg. No. 50,822)

Lead Attorney for Petitioner

Date: September 20, 2024

Baker Botts L.L.P.
700 K Street, N.W.
Washington, D.C. 20001
Telephone: (202) 639-1334
eliot.williams@bakerbotts.com