

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

IPR2023-01290
U.S. Patent No. 10,032,171

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,032,171**

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.	Claim Listing	4
II.	Mandatory Notices Under 37 C.F.R. § 42.8(a)(1).....	13
	A. Real Party-in-Interest under 37 C.F.R. § 42.8(b)(1)	13
	B. Related Matters under 37 C.F.R. § 42.8(b)(2)	13
	C. Lead and Back-Up Counsel under 37 C.F.R. § 42.8(b)(3)	13
	D. Service Information under 37 C.F.R. § 42.8(b)(4).....	14
III.	Introduction.....	15
IV.	Requirements Under 37 C.F.R. § 42.104	15
	A. Grounds for Standing	15
	B. Priority Date	15
	C. Prior Art.....	15
	D. Identification of Challenge and Statement of Precise Relief Requested	17
	E. Discretionary Denial Is Not Appropriate	17
V.	Overview of the '171 Patent.....	20
	A. Description of the '171 Patent.....	20
	B. Relevant Prosecution History.....	20
VI.	Level of Ordinary Skill in the Art	20
VII.	Claim Construction.....	21
VIII.	Summary of the Prior Art	22
	A. Background of Payment Systems.....	22
	B. White (Ex[1013])	23
	C. Mellqvist (Ex[1014]).....	24
	D. EMV (Ex[1019] to Ex[1029])	25
	1. Overview	25
	2. Transaction Flow.....	28
	3. Session Key and Application Cryptogram Generation.....	29
	4. Subsequent Processing.....	30

IX.	Asserted Grounds of Invalidity.....	30
A.	Motivation to Combine Common to Both Grounds.....	30
B.	Ground 1: Claims 1-33 Are Obvious Over <i>White</i> in View of EMV...31	
1.	Claim 1	31
2.	Claim 17	49
3.	Claims 2 and 18.....	54
4.	Claims 3 and 19.....	54
5.	Claims 4 and 20.....	55
6.	Claims 5 and 21.....	55
7.	Claims 6 and 22.....	56
8.	Claims 7 and 23.....	57
9.	Claim 8.....	57
10.	Claims 9 and 26.....	59
11.	Claims 10 and 27.....	59
12.	Claims 11 and 28.....	63
13.	Claims 12 and 29.....	65
14.	Claims 13 and 30.....	66
15.	Claims 14 and 31.....	66
16.	Claims 15 and 32.....	67
17.	Claims 16 and 33.....	68
18.	Claim 24	68
19.	Claim 25	68
C.	Ground 2: Claims 1-33 Are Obvious Over <i>Mellqvist</i> in View of EMV	69
1.	Obviousness Over Mellqvist in General	69
2.	Claim 1	73
3.	Claim 17	79
4.	Claims 2 and 18.....	80
5.	Claims 3 and 19.....	81

6.	Claims 4 and 20.....	81
7.	Claims 5 and 21.....	81
8.	Claims 6 and 22.....	81
9.	Claims 7 and 23.....	82
10.	Claim 8.....	82
11.	Claims 9 and 26.....	83
12.	Claims 10 and 27.....	83
13.	Claims 11 and 28.....	84
14.	Claims 12 and 29.....	85
15.	Claims 13 and 30.....	85
16.	Claims 14 and 31.....	85
17.	Claims 15 and 32.....	85
18.	Claims 16 and 33.....	86
19.	Claim 24.....	86
20.	Claim 25.....	86
X.	Secondary Considerations	87
XI.	Conclusion	88

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....	19
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (<i>Fintiv-I</i>)	17
<i>Apple, Inc. v. SEVEN Networks, LLC</i> , IPR2020-00156, Paper 10 (P.T.A.B. June 15, 2020)	19
<i>Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017).....	17
<i>Godbersen-Smith Constr. Co., D/B/A/ Gomaco Corp., v. Guntert & Zimmerman</i> <i>Const. Div., Inc.</i> IPR2021-00050, Paper 24 at 19-21 (P.T.A.B. May 7, 2021)..	19
<i>Healthcare Inc. v. Daiichi Sankyo Co., Ltd.</i> , No. IPR2015–00865, 2016 WL 5224324 (P.T.A.B. Sept. 12, 2016).....	87
<i>In re Hiniker Co.</i> , 150 F.3d 1362 (Fed. Cir. 1998)	88
<i>Molo Design, Ltd. v. Chanel, Inc.</i> , No. 21-cv-01578 (VEC), 2022 WL 2135628 (S.D.N.Y. May 2, 2022).....	18
<i>NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018).....	17
<i>Resideo Techs., Inc. v. Innovation Scis., LLC</i> , IPR2019-01306, Paper 19 (P.T.A.B. Jan. 27, 2020)	18
<i>Trs. of Columbia Univ. in City of N.Y. v. Illumina, Inc.</i> , 620 F. App’x 916 (Fed. Cir. 2015)	87

STATUTES

35 U.S.C. § 112	21
-----------------------	----

OTHER AUTHORITIES

37 C.F.R. 42.100(b)	21
MPEP § 2128	16
MPEP § 2136	15, 16
MPEP § 2141	69

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	Reserved
1007	Reserved
1008	Expert Declaration and CV of Matthew Calman
1009	Reserved
1010	Reserved
1011	Reserved
1012	U.S. Patent No. 11,080,693 to Fiske (“Fiske”)
1013	U.S. Patent No. 8,374,916 to White (“White”)
1014	U.S. Patent Publication No. 2010/153721 to Mellqvist (“Mellqvist”)
1015	U.S. Patent Publication No. 2010/0252624
1016	Reserved
1017	U.S. Patent No. 7,415,439 B2 to Kontio et al.
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)

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.

Exhibit No.¹	Description
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)
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	EMVCo Newsletter, July 2008 (Attachment L to Byrne Declaration)
1031	EMVCo Newsletter, May 2011 (Attachment M to Byrne Declaration)
1032	Expert Declaration of Dr. Sylvia Hall-Ellis dated August 10, 2023 (“Hall-Ellis Declaration”) and Attachments
1033	Curriculum Vitae of Dr. Sylvia Hall-Ellis

Exhibit No. ¹	Description
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	U.S. Congress, Technology Assessment Board of the 103d Congress: <i>Protecting Privacy in Computerized Medical Information</i>
1036	U.S. PTO: <i>Technical Reference Model</i> , Version 2.0 (Nov. 1, 1996)
1037	Cristian Radu, <i>Implementing Electronic Card Payment Systems</i> (2003)
1038	Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, <i>An Introduction to Mathematical Cryptography</i> (2008)
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 ofr Merchants and Financial Institutions</i> , A First Data White Paper (2011)
1042	EMVCo FAQ webpage (accessed 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>SimplyTap Wins Best Contactless Payments Solution as Future Digital Awards</i> (Aug. 13, 2015), https://www.prweb.com/releases/2015/08/prweb12903489.htm
1048	Reserved

I. CLAIM LISTING

Claim 1

[1.PRE]	A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:
[1.A-1]	at a mobile device, executing an application in an operating system of the mobile device,
[1.A-2a]	the application interrogable by an electronic reader, over a first communications channel,
[1.A-2b]	for digital credential data corresponding to an account
[1.A-2c]	having a corresponding digital credential and
[1.A-3]	configured to [1] request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and
[1.A-4]	[2] generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations
[1.B]	requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;
[1.C]	receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;
[1.D]	locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;
[1.E]	participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:
[1.E-1]	receiving at least one POS command communication sent by the POS terminal over the first communications channel, wherein the at least one POS command communication comprises a request

	for digital credential data to authorize a transaction against the account, the request for digital credential data including a cryptogram request;
[1.E-2]	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; and
[1.E-3]	responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;
[1.F]	subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account;
[1.G]	receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account; and
[1.H]	storing the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between at least two interrogations.

Claim 2

[2]	The method of claim 1, wherein the mobile device is an NFC emulating device, wherein the first communications channel is an NFC communications channel and the first set of data associated with the account and the second set of data associated with the account are received via a data connection over the internet.
-----	---

Claim 3

[3]	The method of claim 1, wherein the response cryptogram is a hash.
-----	---

Claim 4

[4]	The method of claim 1, 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 5

[5]	The method of claim 4, 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 6

[6]	The method of claim 1, wherein 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.
-----	--

Claim 7

[7]	The method of claim 1, wherein the mobile device does not have connectivity to the wireless network during the interrogation.
-----	---

Claim 8

[8.PRE]	The method of claim 1, further comprising, at the remote computer system:
[8.A]	prior to the interrogation, generating the first non-permanent cryptographic key at the remote computer system, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the

	account identifier to the mobile device over the wireless network; and
[8.B]	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.

Claim 9

[9]	The method of claim 8, wherein the digital credential comprises a secure element representation maintained at the remote computer system.
-----	---

Claim 10

[10.PRE]	The method of claim 1, further comprising, at the remote computer system, performing an authorization process comprising:
[10.A]	receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;
[10.B]	determining a current non-permanent cryptographic key associated with the account using the account identifier;
[10.C]	calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account; verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and
[10.D]	sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

Claim 11

[11]	The method of claim 10, wherein: 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 12

[12]	The method of claim 11, wherein the POS command communications comprise the unpredictable data.
------	---

Claim 13

[13]	The method of claim 12, wherein the authorization data further comprises values from the transaction.
------	---

Claim 14

[14]	The method of claim 1, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.
------	---

Claim 15

[15]	The method of claim 1, wherein the application is configured to generate the response cryptogram according to a card specification.
------	---

Claim 16

[16]	The method of claim 1, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.
------	---

Claim 17

[17.PRE]	A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:
[17.A]	a mobile device comprising:
[17.B]	a controller configured to route communications received over a communication channel from an electronic reader;

[17.C]	a wireless interface to connect to a wireless network that is separate from the communications channel;
[17.D]	a processor;
[17.E]	a computer readable storage medium accessible by the processor storing an application executable in an operating system of the mobile device, the application, when executed, interrogable over the communications channel for digital credential data to authorize transactions against an account having a corresponding digital credential hosted at a remote computer system, wherein the application does not have access to a permanent cryptographic key issued for the digital credential and the application is executable to:
[17.E-1]	request from the remote computer system, over the wireless network, a first set of data associated with the account;
[17.E-2]	receive by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;
[17.E-3]	store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;
[17.E-4]	during an interrogation:
[17.E-4a]	receive at least one point-of-sale (POS) command communication sent by a POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data, the request for digital credential data including a cryptogram request;
[17.E-4b]	access the local cryptographic key associated with the account;
[17.E-4c]	generate 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; and
[17.E-4d]	respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the

	at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;
[17.F]	subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;
[17.G]	receive by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data associated with the account comprising a second non-permanent cryptographic key associated with the account; and
[17.H]	store the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between at least two interrogations.

Claim 18

[18]	The system of claim 17, wherein the mobile device is an NFC emulating device, the first communication channel is an NFC channel, and the application is further executable to request and receive the first set of data associated with the account and the second set of data associated with the account via a data connection over the internet to the remote computer system.
------	---

Claim 19

[19]	The system of claim 17, wherein the response cryptogram is a hash.
------	--

Claim 20

[20]	The system of claim 17, wherein the interrogations conform 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 21

[21]	The system of claim 20, wherein the request for digital credential data requests digital credential data comprising a first cryptogram and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.
------	--

Claim 22

[22]	The system of claim 17, wherein 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.
------	---

Claim 23

[23]	The system of claim 17, wherein the mobile device does not have connectivity to the wireless network during the interrogation.
------	--

Claim 24

[24]	The system of claim 17, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.
------	---

Claim 25

[25]	The system of claim 17, further comprising the remote computer system, the remote computer system configured to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.
------	--

Claim 26

[26]	The system of claim 25, wherein the remote computer system is configured to maintain a secure element representation for the
------	--

	account, wherein the digital credential comprises the secure element representation.
--	--

Claim 27

[27.PRE]	The system of claim 17, further comprising, a remote computer system programmed to:
[27.A]	receive an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;
[27.B]	determine a current non-permanent cryptographic key associated with the account using the account identifier;
[27.C]	calculate a calculated cryptogram using the current non-permanent cryptographic key associated with the account; verify a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and
[27.D]	send an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

Claim 28

[28]	The system of claim 27, wherein: 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 29

[29]	The system of claim 28, wherein the POS command communications comprise the unpredictable data.
------	---

Claim 30

[30]	The system of claim 28, wherein the authorization data further comprises values from the transaction.
------	---

Claim 31

[31]	The system of claim 17, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.
------	--

Claim 32

[32]	The system of claim 17, wherein the application is executable to generate the responsive cryptogram according to a card specification.
------	--

Claim 33

[33]	The system of claim 17, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.
------	--

II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(a)(1)

A. Real Party-in-Interest under 37 C.F.R. § 42.8(b)(1)

Mastercard Incorporated and Mastercard International Incorporated are the real parties-in-interest and the Petitioner(s). No other parties exercised or could have exercised control over this Petition and no other parties funded or directed this Petition.

B. Related Matters under 37 C.F.R. § 42.8(b)(2)

The '171 Patent is asserted against Petitioner in Case No. 7-23-cv-01773 (S.D.N.Y. Mar. 1, 2023).

C. Lead and Back-Up Counsel under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel:

LEAD COUNSEL	BACK-UP COUNSEL
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

D. Service Information under 37 C.F.R. § 42.8(b)(4)

A copy of this entire Petition, including all Exhibits and a Power of Attorney, is also being served by Priority Mail Express or by means at least as fast and reliable as Priority Mail Express, costs prepaid, to the address of the attorney or agent of record for Patent Owner at the USPTO regarding the '171 Patent:

26191 - Fish & Richardson P.C. (TC)
PO Box 1022
Minneapolis, MN 55440-1022
United States

A courtesy copy of this entire Petition, including all Exhibits and a Power of Attorney, is being served by Electronic Mail to the address of the attorney or agent of record for Patent Owner in the district court proceedings regarding the '171 Patent:

Spencer Hosie
Diane S. Rice
Darrell R. Atkinson
HOSIE RICE LLP
505 Sansome Street, Suite 1575
San Francisco, CA 94111
Tel: (415) 247-6000
Fax: (415) 247-6001

III. INTRODUCTION

Petitioner challenges claims 1-33 of U.S. Patent No. 10,032,171 (“’171 Patent”), assigned to OV Loop, Inc. (“Patent Owner”).

IV. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Grounds for Standing

Petitioner certifies that the ’171 Patent is eligible for IPR and that Petitioner is not barred or otherwise estopped.

B. Priority Date

Solely for purposes of this Petition, Petitioner assumes the ’171 Patent is entitled to a priority date of August 30, 2011 based on U.S. Provisional Patent Application 61/575,846 (“’846 Provisional”).²

C. Prior Art

U.S. Patent No. 8,374,916 (“White”) claims priority to non-provisional U.S. Patent Application No. 12/606,243 filed October 27, 2009 and is prior art under pre-AIA 35 U.S.C. § 102(e). MPEP § 2136.

² As explained in Petitioner’s separate petition (IPR2023-01289), the ’846 Provisional and other provisionals on which the ’171 Patent claims priority do not support the August 30, 2011 priority date.

U.S. Patent Publication No. US 2010/0153721 (“Mellqvist”) was filed June 18, 2009 and published on June 17, 2010 and is therefore prior art under pre-AIA 35 U.S.C. § 102(e). MPEP § 2136.

“EMV® Contactless Specifications for Payment Systems” version 4.2, Books A to D (“Contactless Specification”), Exs[1023]-[1029], which incorporates by reference and refers to “EMV Integrated Circuit Card Specifications for Payment Systems” version 2.1, Books 1 to 4 (“ICC Specification”), Exs[1019]-[1022], (collectively “EMV Specifications,” hereinafter “EMV”) are industry specification documents published as of April 6, 2011, and June 27, 2008, respectively. Ex[1018] ¶ 13. The EMV Specifications are published and posted on EMVCo LLC (“EMVCo”)’s website (<https://www.emvco.com/>) free of charge, a source regularly monitored and consulted by persons of ordinary skill in the art or anyone working with payment systems. Ex[1008] ¶ 36; Ex[1018] ¶ 13. EMVCo also sends notifications to the industry about publication of EMV. Ex[1018] ¶¶ 10, 14; Ex[1030]; Ex[1031]. Thus, a person of ordinary skill in the art (“POSA”), exercising reasonable diligence, can locate them, and EMV is “printed publication” prior art under pre-AIA 35 U.S.C. § 102(b). MPEP § 2128.

D. Identification of Challenge and Statement of Precise Relief Requested

Ground	Patent Claims	Basis for Challenge
1	1-33	<i>White</i> renders the challenged claims obvious under § 103 in view of <i>EMV</i> and knowledge of a POSA
2	1-33	<i>Mellqvist</i> renders the challenged claims obvious under § 103 in view of <i>EMV</i> and knowledge of a POSA

Submitted with this Petition is the declaration of Matthew Calman, a qualified technical expert, Ex[1008].

E. Discretionary Denial Is Not Appropriate

§ 314(a): This and a contemporaneously filed petition are the only petitions challenging the '171 Patent filed by Petitioner. The factors identified in *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017), therefore, do not provide a basis for denying institution.

Discretionary denial is also not warranted under *NHK Spring Co., Ltd. v. Intriplex Techs., Inc.*, IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018). The six-factor test addressed in *Fintiv* favors institution. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential) (*Fintiv-I*); *cf. id.*, Paper 15 (P.T.A.B. May 13, 2020) (informative) (*Fintiv-II*).

Factor one (stay) weighs in favor of institution. The district court case is in its infancy. The district court permitted Mastercard to file a stay motion in view of

its planned IPRs prior to requiring Mastercard to respond to the Complaint (which motion was filed on the same day this petition was filed), and discovery has not yet opened. *Fintiv-II*, at 12. The district court has in the past granted motions to stay, even before IPR institution. *See, e.g., Molo Design, Ltd. v. Chanel, Inc.*, No. 21-cv-01578 (VEC), 2022 WL 2135628 (S.D.N.Y. May 2, 2022).

Factors two (trial dates) and three (investment in parallel proceedings) weigh in favor of institution. The district court has not entered a scheduling order, Mastercard has not answered the Complaint, and discovery is not open. No trial date has been set. *See Resideo Techs., Inc. v. Innovation Scis., LLC*, IPR2019-01306, Paper 19 at 11 (P.T.A.B. Jan. 27, 2020).

Factor four (overlap) does not weigh against institution. The claims and defenses are still being developed in the district court action and it would be speculative to conclude that there would be any overlap with this proceeding.

Factor five (parties): Petitioner and Patent Owner are the same parties as in district court. However, because this is “far from an unusual circumstance,” panels routinely grant institution even when the parties are the same as in a parallel district court proceeding.

Factor six (other circumstances) weighs in favor of institution given the similarity between Petitioner’s primary references and the ’171 Patent. This Petition shows that the claims involve a combination of familiar elements, according to

known methods, yielding predictable results, and provides several good reasons for combining the routine teachings of the cited references. *See Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10 at 20 (P.T.A.B. June 15, 2020). Moreover, under the Patent Owner’s asserted scope, this Petition shows that the claims are invalid.

§ 325(d): In considering its discretion under §325(d), the Board uses the two-part *Advanced Bionics* framework. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8 (P.T.A.B. Feb. 13, 2020) (precedential).

Where “neither [the combination references] nor similar prior art was before the examiner ... the prosecution history does not include any overlapping arguments directed to this prior art[]” the first part of the test is not met and the Board need not address the second. *Godbersen-Smith Constr. Co., D/B/A/ Gomaco Corp. v. Guntert & Zimmerman Const. Div., Inc.*, IPR2021-00050, Paper 24 at 19-21 (P.T.A.B. May 7, 2021). The EMV Specifications were not presented to the USPTO during prosecution. *See* Ex[1001], Field (56). White and Mellqvist were cited on the face of the patent, but do not appear to have been considered substantively by the examiner. Ex[1002]. If the Board looks to part two of *Advanced Bionics*, Petitioner shows below how the claims are invalid in view of the art, which arguments were not addressed during prosecution.

V. OVERVIEW OF THE '171 PATENT

A. Description of the '171 Patent

The '171 Patent describes “using a mobile computing device in combination with a remotely hosted Secure Element representation to make payments....” Ex[1001], 1:26-30. This involves verification of a “cryptogram,” often generated by a “microchip referred to as a ‘Secure Element’ (SE) ... embedded into a payment card, ... , a cell phone, or other mobile devices.” *Id.* 1:34-38. Generation of the “cryptogram” requires cryptographic keys, and the '171 Patent claims require use of a non-permanent cryptographic key obtained from a remote server to generate such cryptograms, instead of using a permanent cryptographic key. *Id.*, cl. 1.

B. Relevant Prosecution History

The '171 Patent was filed on August 30, 2012. Ex[1002], 126. During prosecution, the applicant focused on the non-permanent key as purportedly inventive. *Id.* 285-290, 519-544, 576, 694-703, 824, 875. However, as explained below, non-permanent payment card keys were conventional, and were described in the pre-existing EMV standards.

VI. LEVEL OF ORDINARY SKILL IN THE ART

As of August 30, 2011, a POSA would be a person with a Bachelor’s degree in Electrical Engineering or Computer Engineering, or equivalent knowledge, with sufficient mathematical background to understand basic cryptographic techniques,

and with two to four years of academic or industry experience in payment systems. Additional education could compensate for less practical experience and vice versa.

VII. CLAIM CONSTRUCTION

Petitioner gives the terms their ordinary and customary meaning, as understood by a POSA at the time of the invention and in the context of the patent disclosure.

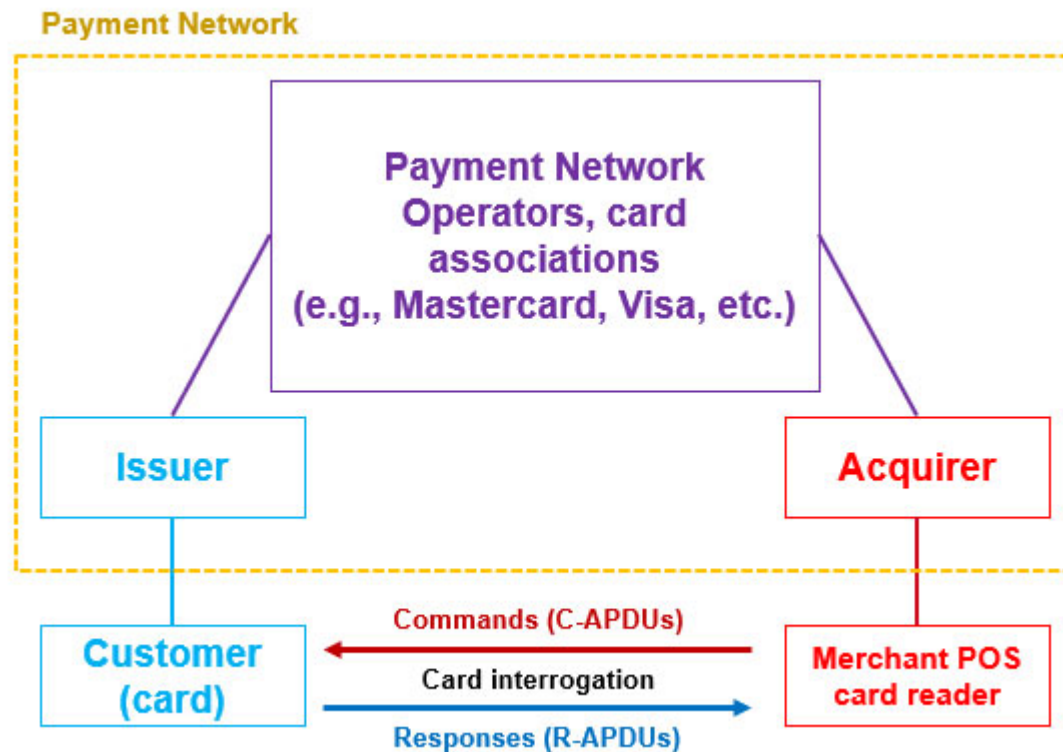
Claims 1 and 17 of the '171 Patent recite, “at least one response application data protocol unit containing the response cryptogram and an account identifier for the account” (hereinafter, the “**R-APDU Term**”). The term is potentially subject to at least two alternative constructions: “one or more response application data protocol unit, collectively containing the response cryptogram and an account identifier for the account” (“**Construction 1**”) or “one or more response application data protocol unit, each of which contains both the response cryptogram and an account identifier for the account” (“**Construction 2**”). Construction 2 is likely correct, but as detailed below, *see* Part IX.B.1.i(3); *see* [1.E-3] of Grounds 1 and 2, the challenged claims are rendered obvious under either construction.

Petitioner does not concede that the '171 Patent's claims are supported under 35 U.S.C. § 112.

VIII. SUMMARY OF THE PRIOR ART

A. Background of Payment Systems

Card payment systems have worked generally as follows since prior to the '171 Patent's priority date. One financial institution ("issuer") would issue a card to a consumer, who uses the card to pay a merchant receiving payments at another financial institution ("acquirer"). Ex[1037], 18. Other players such as payment system operators like Mastercard or Visa facilitate the transaction by operating a payment interchange network.

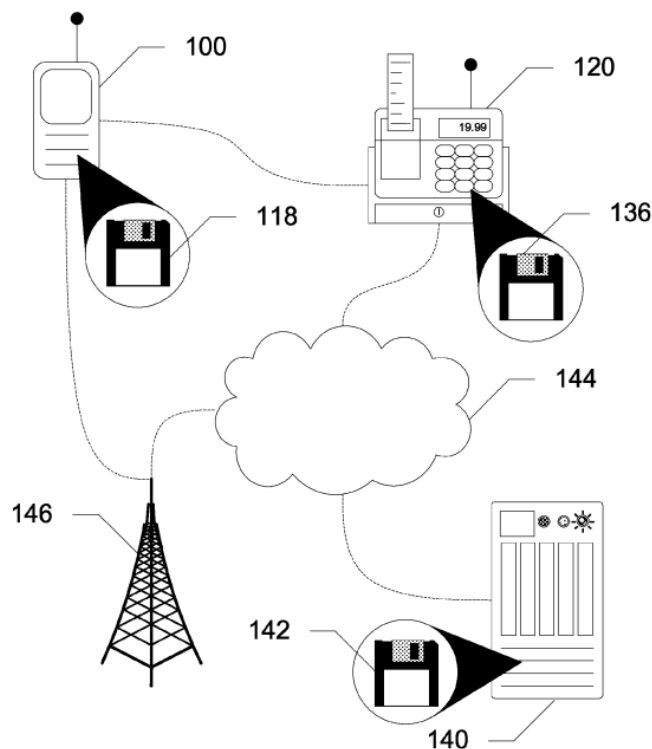


Ex[1008] ¶ 27.

In a typical transaction, a merchant point-of-sale (POS) terminal reader reads information (e.g. card number, expiration date, and authentication information) from the card or a payment mobile device. This is known in the art as “interrogation.” *E.g.* Ex[1015], [0062], [0070]. After interrogation, the POS terminal sends such information, together with other information provided by the merchant to the payment network for authorization. Ex[1008] ¶ 28.

B. White (Ex[1013])

White is prior art at least under pre-AIA 35 U.S.C. § 102(e). *Supra* Part IV.C. White discloses payments made by a mobile device 100 at a POS terminal 120. Ex[1013], Abstract, 4:41-46; Ex[1008] ¶ 30.



Id., Fig. 1.

Mobile communication device 100 may also communicate with a remote server over network 144. *Id.* 4:58-60. For each payment transaction, the mobile device 100 receives a “one-time digital key” from payment server 140, and “combines” that one-time digital key with a “random number” by e.g. “***mixing*** the numbers.” *Id.* 4:49-55. The output is a “payment number,” which may be sent through POS device 120 to the payment server. *Id.* 4:49-55, 5:6-8, 10-12. Under White, “a one-time digital key limits a hacker to a single transaction,” thus improving security of the transaction. *Id.* 2:6-7; Ex[1008] ¶ 31.

C. Mellqvist (Ex[1014])

Mellqvist is prior art at least under pre-AIA 35 U.S.C. § 102(e). *Supra* Part IV.C. Mellqvist discloses an NFC-enabled portable electronic device (“portable device”) and remote secure element servers for payment and ticketing applications. Ex[1014] Abstract, [0036], [0040].

Like the provisional applications from which the ’171 Patent purportedly claims priority (e.g. Ex[1003], [0070]-[0071]; Ex[1004], [0051]-[0052]; Ex[1005], [0045]-[0046]), Mellqvist discloses that portable device communicates, over wireless network 150, with a remote secure element server that hosts one or more secure elements. *Id.* [0036], Fig. 1. These secure elements may store “payment ...

applications,” and may be securely accessed by a virtual secure element module of the portable device. *Id.*

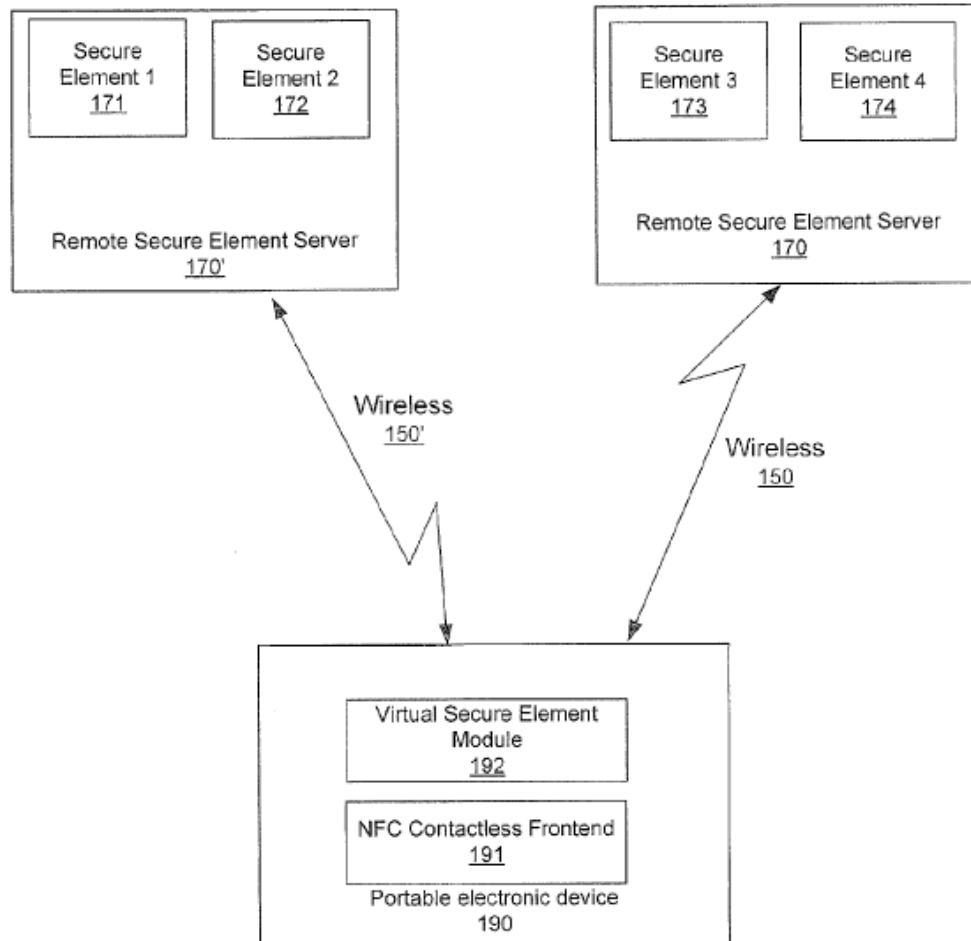


Figure 1

D. EMV (Ex[1019] to Ex[1029])

1. Overview

As of the '171 Patent's priority date, magnetic stripe payment cards were being replaced by “chip cards,” where a tamper-resistant microchip containing processing and memory circuitry that can store account credentials. Ex[1037], 13-

14, 34-47; Ex[1041], 6. These chip cards were designed and configured to conform to industry standards and best practices known as the EMV Specifications of EMVCo, a technical body formed in February 1999 by three major payment brands—*Europay*, *MasterCard* and *Visa*. Ex[1042]. Such payments are known as the “EMV transactions.” Global migration to EMV was well under way as of 2011. Ex[1041], 6.

Some of these chip cards had contactless or Near Field Communication (“NFC”) communication capabilities, allowing transactions by simply waving or tapping the card at the POS reader. Ex[1040] § 2.3.3. Some mobile phones in 2011 also had NFC capability and could also function as a payment card in “card emulation” mode, i.e., the mobile device emulates a contactless NFC payment card, enabling transactions with an NFC contactless POS. Ex[1008] ¶ 37.

Traditional magnetic stripe cards were prone to fraud because data on these cards, such as primary account number (PAN), expiration date, and CVV verification code, do not change, and thus the card could be easily duplicated. *Id.* ¶ 39. To combat fraud, EMV transactions conduct “card authentication” (where card issuer verifies whether the card is authentic) by requiring the card or mobile contactless payment device to generate an “Application Cryptogram” (AC), an encrypted message that differs for each transaction because it is generated by encrypting unique information about *that* transaction using a previously stored

cryptographic key. Ex[1020] §§ 8.1.1-8.1.2, and thus an unauthorized person cannot re-generate an AC intercepted from the POS. Ex[1008] ¶ 38.. The POS terminal receives only the AC but not the cryptographic key used to generate the AC, and thus an unauthorized person cannot replicate the card or device to give the same response AC for another transaction. *Id.*

The POS reader sends an authorization request including the transaction information and AC to the payment network. The issuer server verifies the AC in the authorization request by generating an AC with the same transaction data and comparing the two, because the issuer knows (or can derive) the secret cryptographic key and knows, from the authorization request, the data used to calculate the AC. Ex[1008] ¶ 39. The issuer may approve the transaction, if it generates an AC matching the one in the authorization request and agrees the transaction is determined to be valid. Ex[1037], 57-58.

EMV (Exs[1019]-[1029]) describes in detail the transaction process, including messages exchanged between devices. It was well known in the art and disclosed in EMV that communications between the “Card” and the POS terminal during the interrogation are carried out using application protocol data unit (APDU) messages. Ex[1037], 46-48; Ex[1021] §§ 6.1-6.2; Ex[1008] ¶ 41.

2. Transaction Flow

In Mastercard and Visa transactions, during the interrogation, the “Card” (user device) provides account information such as a Primary Account Number (PAN) in response to a READ RECORD or GET PROCESSING OPTIONS (GPO) command. Ex[1026] § 3.4.3; Ex[1027] § 2.4.1. Here, if the “Card” does not either approve (with a “TC” Application Cryptogram) or decline (with an “AAC” cryptogram) the transaction locally, the POS machine will send an “online” authorization request (requesting authorization from the card issuer); under such scenarios, the “Card” provides an Authorization ReQuest Cryptogram (“ARQC”) Application Cryptogram to the POS to be forwarded to the issuer. Ex[1021] § 9.3.1; Ex[1026] § 5.3.1; Ex[1027] § 5.4.3.2; Ex[1008] ¶ 42.

In an EMV contactless Mastercard transaction, the POS terminal reader reads data record(s) from the “Card” through a READ RECORD command, including, among other things, a PAN, Ex[1026] §§ 3.4.3, 5.7.3; Ex[1021] Part III, § 7.2; then, in response to a subsequent GENERATE AC command, the “Card” returns an Application Cryptogram, which may be TC, AAC, or ARQC. Ex[1021] § 9.3.1; Ex[1026] § 5.3.1; Ex[1008] ¶ 43.

In an analogous EMV contactless Visa transaction, the POS issues a GPO command, and the “Card” may return a cryptogram together with Track 2 Equivalent Data, which contains, among other things, a PAN (Application PAN) and expiration

date. Ex[1027] § 2.4.1, Table E-6. The cryptogram returned is an Application Cryptogram (TC, AAC, or ARQC). Ex[1027] §§ 2.4.1, 5.4.3.2; Ex[1008] ¶ 44.

3. Session Key and Application Cryptogram Generation

Under the EMV, the “Card” generates the Application Cryptogram (TC, AAC, or ARQC), which is also a “Message Authentication Code” (MAC), by applying a one-time cryptographic key known as a “Session Key” (SK) to a set of “input data.” Ex[1020] §§ 8.1, A1.2-1.3. The input data consists of transaction information such as transaction amount, an Unpredictable Number for the transaction, and the value of an Application Transaction Counter (ATC). *Id.* § 8.1.1. In particular, the “Unpredictable Number,” is a random number supplied by the POS terminal that ensures that the input data is unique to the transaction and not predictable before the transaction occurs. *Id.*; Ex[1008] ¶ 45.

The “Session Key” used for generation of the Application Cryptogram, is generated for *each transaction* using an ICC Master Key (the master key for each “Card”) and an Application Transaction Counter (ATC) that increments with each transaction. Ex[1020] § A1.3.1; Ex[1008] ¶ 46.

Generation of the Application Cryptogram (TC, AAC, or ARQC) (which is a MAC) involves applying the Session Key to the set of input data (explained above) using a “block cipher algorithm” such as Triple DES (3DES), which are well known cryptographic operations, and taking the *s* most significant bytes (here, *s*=8).

Ex[1020] §§ 8.1.2.2, A1.2, B1.1. The result is a fixed length (8-byte) value, which becomes the MAC. *Id.*; Ex[1008] ¶ 47.

4. Subsequent Processing

In an online authorization, the POS terminal sends an online authorization request including the Application Cryptogram (here, an ARQC) to the payment network to be verified by the issuer. Ex[1026] Table 2.1; Ex[1027] § 2.4.7; Ex[1021] § 10.9. The issuer knows or can derive the same Session Key used by the “Card” (including mobile device acting as a payment card) to generate the ARQC and thus verify the ARQC received in the authorization request, authenticating the card. Ex[1021] § 10.9 n.17; Ex[1037], 58; Ex[1008] ¶ 48.

IX. ASSERTED GROUNDS OF INVALIDITY

A. Motivation to Combine Common to Both Grounds

A POSA would have been motivated to implement either White or Mellqvist to conduct transactions in accordance with the EMV specifications. Ex[1008] ¶ 49. A POSA would understand both White and Mellqvist disclose conducting payment transactions with merchant POS terminals. *Id.*; *see e.g.*, Ex[1013] Fig. 1; Ex[1014] Figs. 1-2. Therefore, White’s and Mellqvist’s inventions depend on compatible infrastructure to work. Ex[1008] ¶ 49.

POS terminals worldwide were in the process of becoming EMV-compliant as of September 2010. Ex[1041], 6. A POSA would not view replacement of POS

terminals globally with an alternative standard as practical. Ex[1008] ¶ 50. A POSA would therefore be motivated to make the payment device compliant with standardized payment specifications, particularly EMV. *Id.* ¶ 51. A POSA would recognize that EMV transactions offer technical and economic advantages, including the ability to reduce fraud with techniques such as card authentication using dynamic data e.g. ARQC cryptogram. *Id.*; Ex[1040] §§ 1, 1.2, 2.1.1.1, 2.3.1, 3.

Thus, a POSA would be highly motivated to implement White or Mellqvist according to EMV to achieve compliance with payment-industry security expectations, and to improve marketability of resulting devices by allowing its use with the large and growing majority of merchant POS terminals that communicate using the standardized EMV transaction approach. Ex[1040] § 3; Ex[1008] ¶ 52.

B. Ground 1: Claims 1-33 Are Obvious Over *White* in View of EMV

1. Claim 1

a. [1.PRE]

To the extent the preamble is limiting, White in view of EMV discloses such a method. Both disclose a “mobile device.” Ex[1013] 4:2-8; Ex[1023] § 4.1. Both disclose a “secure application” for “payment card transaction.” *E.g.*, Ex[1013] 7:14-16, Fig. 6; Ex[1037] 38-41; *see generally* Exs[1021], [1023].

b. [1.A-1]

White discloses a “mobile communication device” (“mobile device”) 100, which a POSA would understand to contain applications including a “client payment logic” 118. 4:2-8, 15-18, 41-47, Fig. 1; Ex[1008] ¶ 54. A POSA would have understood this to mean software application executed on an operating system. Ex[1013] 4:15-18; Ex[1008] ¶ 54.

Further, a POSA implementing White would have found it obvious to refer to EMV, under which a “Card” can be “any consumer token supporting contactless payment transactions, whether ... payment chip card ... *a mobile phone*, or another form factor.”³ Ex[1023] § 4.1. Thus, a POSA would understand “Card” for contactless payment transactions to include not only payment cards but also a mobile device containing its processor and memory, which may be the processor and memory of the mobile device in White. Ex[1008] ¶ 55; Ex[1037] 38-41. In particular, EMV is directed to financial “applications” that run on the operating system of the card or equivalently on mobile device with an NFC controller operating in card emulation mode, Ex[1013], 2:14-17, and the POS terminal’s application “sends commands as a client to the card application, which responds as a server.” Ex[1037] 40, 47-48; Ex[1008] ¶ 55.

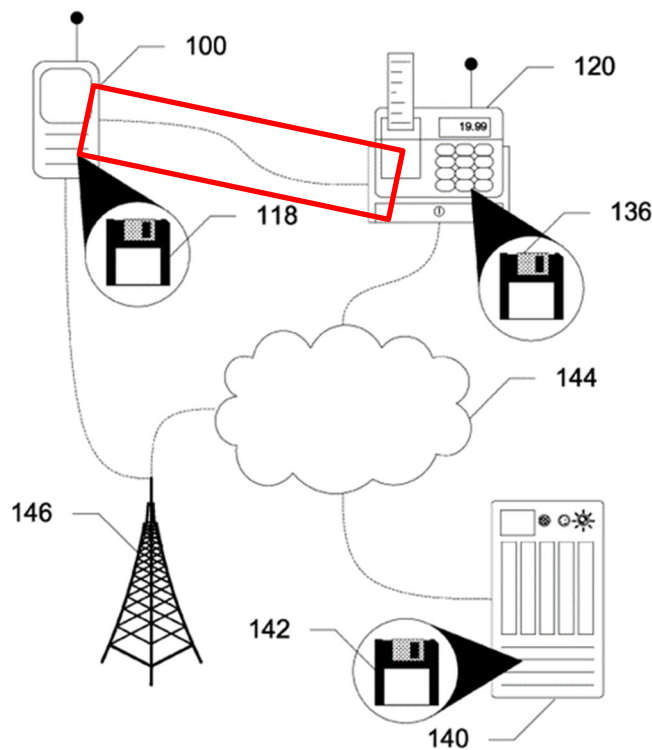
³ All emphases added except otherwise noted.

c. [1.A-2]

(1) [1.A-2a]

The '171 Patent suggests that interrogation refers to querying or extraction of information, *e.g.*, Ex[1001], 6:3-5, 6:50-53, a well-understood process in the art, Ex[1015], [0062], [0070]; Ex[1008] ¶ 56.

White discloses that the mobile device containing the payment logic can “us[e] near field communication (NFC) to communicate with the point-of-sale device” in conducting a financial transaction. Ex[1013], 2:14-17. Further, “[m]obile communications device 100 may communicate wirelessly with point-of-sale (“POS”) device 120,” and POS 120 may also communicate with mobile device 100 with information such as a sales amount “directly.” Ex[1013], 4:55-57, 5:2-4. Such communications may occur over a “first communication channel” (shown below in red) and are known in the art as “interrogation.” *e.g.*, Ex[1015], [0062], [0070]; Ex[1008] ¶ 57.



Ex[1013] Fig. 1. Moreover, when implemented in compliance with EMV, the device application would be interrogable by the POS to comply with that standard. Ex[1026] § 3.5.3; Ex[1027] §§ 2.4.1, 5.4.3.2; Ex[1023] §§ 4.1-4.3, 10.1-10.2; Ex[1008] ¶ 58.

(2) [1.A-2b]

The '171 Patent states that “[t]he term ‘digital credential data’ as used herein refers to at least a portion of all data ... necessary to authorize approval of a transaction at a POS terminal.” Ex[1001], 7:3-7.

White discloses that the application is interrogable “for digital credential data corresponding to an account”—specifically, that “[m]obile communications device 100 ... communicates a payment number” that “may be routed “through

point-of-sale device 120.” Ex[1013] 5:4-6, 10-12. Server 140 then authorizes the transaction after verifying the payment number. *Id.* 5:16-26. Thus, the payment number is the claimed “digital credential data” because it is a portion of the data that are “necessary to authorize approval of a transaction at a POS terminal.” Ex[1001], 7:3-7. Further, a POSA would have considered it obvious that the mobile communication device 100 will communicate to the payment server 140 an account identifier such as an account number (e.g. PAN), because such information is typically used to determine from which or whose account the transaction amount should be deducted. Ex[1008] ¶ 60.

EMV similarly discloses an application interrogable by a reader over a communication channel. It is well known in the art that, an EMV transaction begins with, among other things, selection of an “application,” which responds to POS commands. Ex[1037] 40, 47-48; Ex[1023] § 5.8.2 (“Application Selection”); Ex[1026] § 2.3.3-2.3.4; Ex[1027] § 2.4.1; Ex[1008] ¶ 61. The application on the “Card” will return certain “digital credential data”—data necessary for approval of a transaction, Ex[1001], 7:3-7, including account information (e.g., PAN) and Application Cryptogram. Ex[1021] § 7.2, 9.3.1; Ex[1026] §§ 3.4.3, 5.3.1, 5.7.3; Ex[1027] §§ 2.4.1, 5.4.3.2; Ex[1037], 57-58; Ex[1008] ¶ 61.

Accordingly, because a POSA would have been motivated to implement White to carry out EMV transactions, the POSA would understand the mobile device

containing logic, as disclosed in White, to be emulating the “Card” by utilizing the mobile device’s onboard NFC controller in “card-emulation” mode, and made White’s mobile device capable of being interrogated by a POS terminal for data necessary for approval of transaction (“digital credential data”) under EMV, by programming payment logic 142 or mobile application to give responses in the manner specified under EMV. Ex[1008] ¶ 62.

(3) [1.A-2c]

According to the ’171 Patent, “digital credential,” is an “SE representation.” Ex[1001] 26:34-35. An SE or “Secure Element” is a “microchip ... embedded into a payment card, a payment fob (medallion), a cell phone, or other mobile devices that may be *used for making payments.*” *Id.* 1:35-38. Further, a “secure element representation” may be “(a) actual SE hardware ... , ... (b) virtual hardware secure element representations such as a computer model that simulates the operation of a hardware SE element ... , or ... (c) data in a database (typically a secure database) such as static Track Data or data dynamically or statically generated by an HSM (Hardware Security Module).” *Id.* 9:44-58. The ’171 Patent further explains that “Track Data” refers to “Track1/Track2 data” during interrogation for authorization, and HSM would generate “credential data.” *Id.* 8:47-49, 9:6-8, 23:30-33.

Based on these descriptions, a POSA would have understood “digital credential” or “SE representation” to contain as at least a portion of data necessary

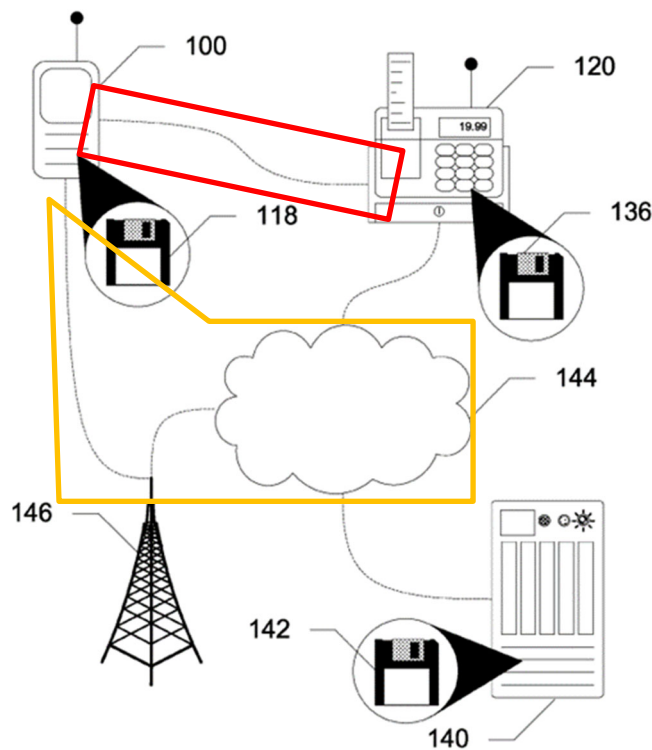
to authorize approval of a POS payment transaction—that is, of the “digital credential data.” *Id.* 7:3-7; Ex[1008] ¶ 64. As discussed above for [1.A-2b], White and EMV disclose using digital credential data for approval of a transaction for an account, and thus imply or render it obvious that the account must have a “corresponding digital credential,” to perform authentication and approval of the requested payment transaction.

d. [1.A-3]

White discloses payment server 140, Ex[1013] Fig. 1, which is “a remote computer system” because it is accessed through a network 144. Ex[1013] 4:53-55. A POSA would have understood payment server 140 as “hosting the corresponding digital credential” of an account ([1.A-2c]) because payment server 140 represents the payment server network and is responsible for both supplying one-time digital key used to calculate the payment number and approving a transaction associated with an account. Ex[1013], 5:23-26. Thus, the server must necessarily host “digital credential,” which contains “digital credential data” i.e., “data necessary to authorize approval” including “any data that are required to calculate [such] data” like White’s one-time digital key. Ex[1001], 7:3-7; Ex[1008] ¶ 65. It was well known in the art that, in an EMV transaction, such data include account information and authentication data associated with the account (such as an ARQC cryptogram and data necessary to authenticate that cryptogram). Ex[1037], 57-58; Ex[1008] ¶ 65.

White further discloses that “[m]obile communications device 100 receives the one-time digital key from payment server 140 through network 144.” Ex[1013], 4:53-55. The “one-time digital key” is data associated with the account because it is used to generate payment number for authorizing a transaction associated with the account. *Id.* 5:6-8, 22-26. Further, a POSA implementing White in accordance with EMV would use an EMV “Session Key” as the “one-time digital key” from the payment server 140. Ex[1008] ¶ 66. An EMV Session Key is unique to each transaction (“one-time”) and is data associated with the account because it is derived from an ICC Master Key generated from the account number, and thus directly corresponds with White’s described one-time key. *Id.*; Ex[1020] §§ A1.3.1-A1.4.

White also discloses that “[m]obile communications device 100 may ... communicate wirelessly with payment server 140 over network 144 through cellular tower 146,” Ex[1013] 4:48-60, which is separate from the first communications channel between the mobile device and the POS terminal over which interrogation of mobile device occurs, *id.* Fig. 1.



Even if White does not explicitly describe a “request” to the remote server, a POSA would have understood White as implying, or otherwise deem it obvious, that the mobile device may be configured to receive the one-time digital key after making a *request* to the server because it would be an efficient use of computation and communication resources for the server to deliver data (e.g., the one-time digital key) to the mobile device in response to a request for it, rather than providing such data regardless of whether the mobile device needs the data or is powered and connected to the network. Ex[1008] ¶¶ 68-69. A POSA in 2011 would further recognize that a mobile device may often be out of range from a network, such as in

large buildings, or underground, including in public transit. *Id.*; Ex[1044] ¶¶ 4.41-4.43.

e. [1.A-4]

White discloses a “payment number,” which is a cryptogram generated using data associated with an account. Ex[1013] Fig. 6, 7:14-19. For each payment transaction, mobile device 100 would receive a “one-time digital key” from payment server 140 through network 144, and “combines” that one-time digital key with a “random number” by e.g. “*mixing* the numbers.” Ex[1013] 4:49-55. The “payment number” may be communicated to the POS device 120, which will pass it on to the payment server. *Id.* 4:49-55, 5:6-8, 10-12.

A POSA would have understood that “*mix/ing* the data and key together in a prescribed manner” is how well-known cryptographic operations, such as DES (or its advanced version, Triple DES or 3DES/DES3), operate to encrypt data, and would therefore understand that, by referring to a “mixing” operation, White discloses and renders obvious performing an encryption operation with the one-time digital key to generate the “payment number.”⁴ Ex[1035], 11; Ex[1036], 9; Ex[1038], 7-8;

⁴ This distinguishes “mixing” from other operations also described in White, such as addition, multiplication, subtraction, and concatenation (appending). Ex[1013] 4:49-53; Ex[1008] ¶ 72 n.7.

Ex[1043], 3; Ex[1008] ¶ 72. Thus, the resulting “payment number” is encrypted data or message, or a “cryptogram.”⁵ Ex[1008] ¶ 72. Indeed, the ’171 Patent itself refers to a “*number* sequence” so calculated as a “cryptogram.” Ex[1001] 7:42-43.

Further, White’s “one-time digital key,” as explained for [1.A-3], is “data associated with the account” and is “received from the remote computer system,” namely, payment server 140. The “one-time digital key,” as its name suggests, is valid for only one transaction. Ex[1013] 6:40-42. By contrast, a “permanent cryptographic key,” according to the ’171 Patent, “refers to a cryptographic key that is unchanging (or static) throughout the life of a card, SE, mobile device, or digital credential.” Ex[1001], 27:30-32. White does not disclose receiving from the server or using any other cryptographic key besides the one-time digital key in generating the cryptogram (payment number), Ex[1013] 4:49-55, 5:6-10, and thus application including the payment logic does not “access a permanent cryptographic key issued for the digital credential during the interrogations.”

In addition, because the cryptogram (“payment number”) may be communicated to the POS terminal, which will communicate the cryptogram to the payment server, Ex[1013] 5:10-12, the cryptogram is information extracted by POS

⁵ The ’171 Patent itself defines “cryptogram” as “encrypted data that may or may not be able to be un-encrypted.” Ex[1001] 25:37-38.

terminal from the mobile device, Ex[1001], 6:3-5, and is therefore cryptogram “requested during interrogations over the first communications channel.”

Accordingly, a POSA would have recognized that a straightforward way to implement White to conduct EMV transactions would be to implement White’s “one-time digital key” as an EMV Session Key, and to implement White’s “payment number” as an EMV Application Cryptogram. Ex[1008] ¶ 75. Specifically, an EMV-compliant terminal requests an Application Cryptogram via a GENERATE AC or GPO command during interrogation. Ex[1021] § 9.3.1; Ex[1026] § 5.3.1; Ex[1027] § 5.4.3.2. The Session Key is not a permanent cryptographic key because it is generated using an application transaction counter (ATC) that increments for each transaction and is therefore unique for each transaction. Ex[1020] § A1.3. Thus, the “Card” or mobile device does not access a permanent cryptographic key for generation of cryptogram requested during interrogation but accesses only a temporary Session Key. This would have been well within the level of skill in the art and would entail nothing more than implementing the known EMV techniques in the payment system of White. Ex[1008] ¶ 75.

f. [1.B]

As explained in connection with [1.A-3], White and EMV disclose and render obvious requesting account/payment data from the remote system over a wireless network.

g. [1.C]

As explained for [1.A-3], White discloses that the application of the mobile device receives, from the payment server (remote computer system) over the wireless network, a “one-time digital key,” and this key is “data associated with the account.” Further, as explained in connection with [1.A-4], a POSA would have understood or consider it obvious that the “one-time digital key” is a cryptographic key for generation of a cryptogram using well-known encryption methods. In addition, because the “one-time digital key” is valid for one transaction only, it is not a permanent cryptographic key but a non-permanent cryptographic key. Ex[1008] ¶ 78.

Also as explained in [1.A-4], a POSA implementing White to carry out EMV transactions would understand that a Session Key, which is unique to each transaction hence a non-permanent cryptographic key, would be an obvious way to implement White’s “one-time digital key.” The mobile device application would generate an Application Cryptogram in response to a GENERATE AC or GPO command. It was also well understood in the art and required by EMV that responses from the “Card” (or mobile device here) during interrogations are response application protocol data units (R-APDU), and the AC would be passed back to POS terminal in a R-APDU. Ex[1037], 46-48; Ex[1021] §§ 6.1-6.2, 6.5.5; Ex[1008] ¶ 79.

h. [1.D]

White discloses that “[t]he one-time digital key is stored on mobile device ... until it is used ... [or] replaced by a new one-time digital key.” Ex[1013] 6:25-28. As explained above for [1.A-4], the one-time digital key is a non-permanent cryptographic key because it is replaced at least after each transaction. Further, a POSA implementing White to carry out EMV transactions would have found it obvious to follow EMV and use the Session Key, which is a non-permanent cryptographic key associated with the account, as the “one-time digital key” in White. Ex[1008] ¶ 80. Accordingly, the one-time digital key or Session Key is the claimed locally stored local cryptographic key.

i. [1.E]

As explained for [1.A-1] and [1.A-2a], White discloses the application participating in an interrogation between a POS terminal and the mobile device. Further, a POSA implementing White to carry out EMV transactions would have found it obvious to follow EMV for such interrogations, as explained below. Ex[1008] ¶ 81.

(1) [1.E-1]

Under EMV, a POS terminal issues at least one READ RECORD command and one GENERATE AC command (for Mastercard transactions), or a GPO command (for Visa transactions) over the contactless communication channel.

Ex[1026] §§ 3.4.3, 5.3, 5.7; Ex[1027] §§ 2.4.1, 5.4.3.2. These commands are “request[s] for digital credential data to authorize a transaction against the account” that “include[es] a cryptogram request,” because the “Card” responds to these commands with at least account information and an Application Cryptogram. Ex[1008] ¶ 82. Thus, the GENERATE AC or GPO commands are each a “cryptogram request.” *Id.*

As explained above for [1.A-2], White discloses a mobile device with application interrogable by a POS terminal over a first communications channel for digital credential data used to authorize transactions against an account. Accordingly, a POSA implementing White to carry out EMV transactions would have found it obvious to program the mobile device application to respond to READ RECORD, GENERATE AC, and/or GPO commands received from the POS requesting credential data in the manner specified by EMV, satisfying this claim element. Ex[1008] ¶ 83.

(2) [1.E-2]

White discloses generation of the “payment number” by mixing input data (a random number) with the one-time digital key. Ex[1013] 4:49-50, 5:6-8. As explained for [1.A-4], this is a cryptogram. Likewise, EMV prescribes the generation of an Application Cryptogram (AC), which would be the “payment number” in White and be returned in a response message, based on a set of inputs and a Session

Key. Ex[1020] §§ 8.1.1 (minimum set of data elements for AC generation); 8.1.2 (generation of AC with Session Key). The Session Key, which would be the “one-time digital key” in White, is stored locally, as explained for [1.D].

Further, it was well understood in the art that a cryptogram, or cipher text, is generated by “mixing” the input data with a cryptographic key. Ex[1035], 11; Ex[1036], 9; Ex[1038], 7-8; Ex[1008] ¶ 85. As a result of such “mixing,” the resulting response AC does not include the cryptographic key but only the encrypted text or cryptogram. Ex[1008] ¶ 85. Specifically, EMV specifies that an AC may be generated using 3DES (Triple DES) algorithm with a 128-bit Session Key and the key is “mixed” into the data to be encrypted—data cannot be called “encrypted” if the ciphertext includes the key, allowing an interceptor to decrypt. Ex[1020] §§ 8.1.2, A1.2, A1.3.1, B1.1; Ex[1008] ¶ 85, n.10; Ex[1039]. Hence, a POSA implementing White to carry out EMV transactions would have found it obvious to configure the mobile application (“Card”) to generate, using a Session Key, an AC to be included in a response APDU message, where the AC does not include the Session Key. Ex[1008] ¶ 85.

(3) [1.E-3]

A POSA implementing White to carry out EMV transactions would have found it obvious to configure the mobile device to communicate with the POS terminal using application protocol data unit (APDU) messages, in accordance with

EMV, which were also well known in the art—in particular, a command issued by the terminal is a command APDU (C-APDU) while a response from the “Card” responding to C-APDU is a response APDU (R-APDU). Ex[1037] 46-48; Ex[1021] §§ 6.1-6.2; Ex[1008] ¶ 86.

As explained above, the R-APDU Term here is potentially subject to two alternative constructions. *Supra* Part VII. Under Construction 1, the Term could mean one or more APDUs collectively containing the response cryptogram and an account identifier for the account. *Id.* Under this construction, a Mastercard EMV transaction would render this element obvious because, as explained above, a response message to the READ RECORD command contains, among other things, a payment account number (Ex[1026] §§ 3.4.3, 5.7.3; Ex[1021] § 7.2), while another response message in response to the GENERATE AC command returns an Application Cryptogram (AC), Ex[1026] § 3.5.3. In addition, the Term is satisfied by EMV’s disclosure of a contactless EMV mode Visa transaction, in which there is at least one response ADPU to the GPO command containing both “Track 2 Equivalent” data (which includes *inter alia* a primary account number (PAN), hence

the “account identifier”)⁶ and a response cryptogram (an AC). *Supra* Part VIII.D.2; Ex[1027] §§ 2.4.1, 5.4.3.2; Ex[1008] ¶ 87.

Alternatively, under Construction 2, the Term could refer to one or more APDUs, each of which contains both the response cryptogram and an account identifier for the account. *Supra* Part VII. An EMV mode Visa transaction would meet this limitation with the response APDU to the GPO command containing both account identifier and AC, as explained above. Therefore, under either construction, EMV discloses this R-APDU Term. Hence, White in view of EMV render this element obvious.

j. [1.F]-[1.G]

After a payment transaction, White explains, “[w]ith the payment completed, payment server 440 issues a new one-time digital key S455 to mobile device 400.” Ex[1013] 6:40-42. Thus, White’s mobile application would receive, from payment server over the wireless network, a new one-time digital key, which, as explained above in connection with [1.A-3] and [1.C], is also data associated with the account and thus “a second set of data associated with the account.”

⁶ The term “account identifier” did not appear in ’171 Patent’s specification, but a POSA would have understood that in the very least, an account number, such as a PAN, is an account identifier. Ex[1008] ¶ 87 n.11.

Also as explained above for [1.A-3] and [1.C], a POSA would have understood White as implying (or otherwise deem it obvious) to program the application on the mobile device to request a new one-time digital key, which would be a new Session Key. Ex[1008] ¶ 90. Hence, White discloses or renders obvious that, after a transaction, the mobile application *requests and receives* a new one-time digital key, which is a second set of data associated with the account that satisfies this element. *Id.* ¶¶ 90-91.

k. [1.H]

White explicitly discloses that each “one-time digital key is stored on mobile device ... until it is used, until it is replaced by a new one-time digital key, for a period of time, etc.” Ex[1013] 6:25-29, 2:6-11. As explained above for [1.A-3], [1.A-4], and [1.D], the one-time digital key is a local, non-permanent cryptographic key. Ex[1008] ¶ 92.

2. Claim 17

a. [17.PRE]

To the extent the preamble is limiting, As discussed for [1.PRE] and [1.E], White, alone or in view of EMV disclose this limitation.

b. [17.A]

For reasons discussed for [1.A-1], White, alone or in view of EMV Specification disclose a “mobile device.”

c. [17.B]

As discussed for [1.A-1], White discloses a mobile device with a central processing unit and transceiver allowing communication with a POS device over NFC or otherwise wirelessly. Ex[1013] 2:13-16, 4:55-57. This implies or makes it obvious to a POSA that the mobile device includes a controller configured to route the communications received from a POS device. Ex[1008] ¶ 95.

d. [17.C]

White discloses that “[m]obile communications device 100 may ... communicate wirelessly with payment server 140 over network 144 through cellular tower 146,” Ex[1013] 4:48-60; Fig. 1, which is separate from the first communications channel between the mobile device and the POS terminal over which interrogation of mobile device occurs, *id.* Fig. 1, and implies or makes it obvious to a POSA that the device includes a wireless interface. Ex[1008] ¶ 96.

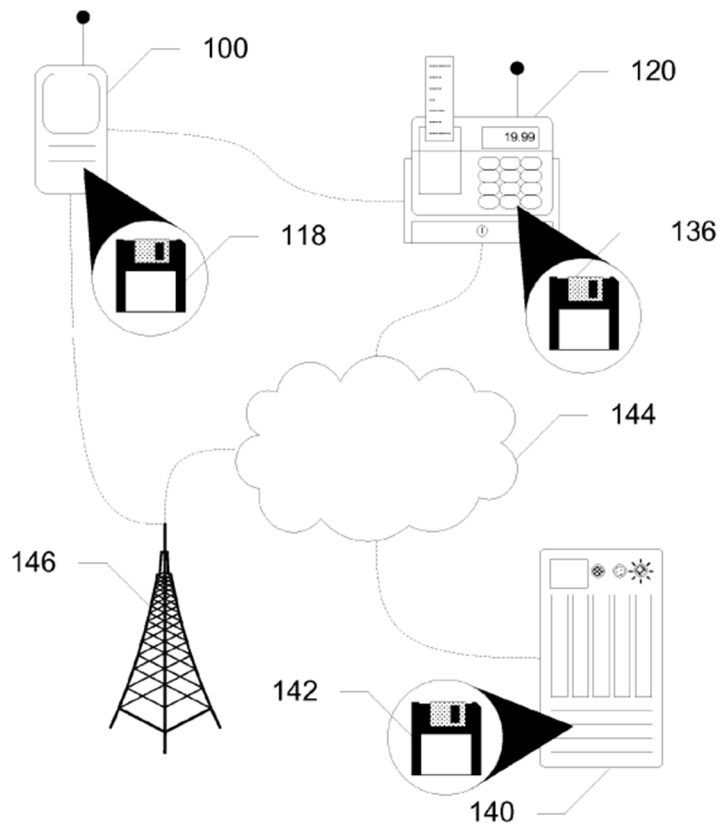


Figure 1

e. [17.D]

White discloses a central processing unit 314, which is a processor. Ex[1013] 5:65, Fig. 3A-3B. Moreover, it was well known in the art that a “Card” in EMV transactions also contains a processor. Ex[1037] 38-41; Ex[1008] ¶ 97.

f. [17.E]

White discloses that the mobile device has a memory 316, which is the “storage medium” claimed in this element. Ex[1013] 5:64. “Memory 316 stores logic, data, digital keys, etc. Client payment logic 318 includes a random number

generating algorithm, instructions for combining a random number with a one-time digital key, instructions for transmission, etc.” *Id.* 6:16-20. Further, the memory is accessible by the processor because “CPU 314 commands components of mobile device 300 according to a client payment logic 318 on memory 316.” *Id.* 6:14-16. For reasons discussed for [1.A-2] and [1.A-4], White discloses an application interrogable by POS terminal to authorize transactions without accessing a permanent cryptographic key. An EMV “Card” similarly has such an application stored in the memory and accessible to the processor and, as previously explained a POSA would have been motivated to have White’s payment functionality perform the functions of an EMV Card to be compatible with EMV infrastructure. Ex[1037] 38-41; Ex[1008] ¶ 98. Accordingly, White discloses or renders obvious this element.

(1) [17.E-1]

For reasons discussed for [1.A-3] and [1.B], White discloses or renders obvious this claim element.

(2) [17.E-2]

As discussed for [1.C], White discloses this limitation.

(3) [17.E-3]

As discussed for [1.D], White discloses this limitation.

(4) [17.E-4]

As discussed for [1.E], White discloses this limitation.

(a) [17E-4a]

As discussed for [1.E-1], White, in view of EMV, EMV discloses or renders obvious this limitation.

(b) [17.E-4b]

As discussed for [1.D] and [1.E-2], White in view of EMV discloses or renders obvious this limitation because the payment number or cryptogram is generated using the locally stored cryptographic key.

(c) [17.E-4c]

As discussed for [1.E-2], White, in view of EMV, discloses or renders obvious this limitation.

(d) [17.E-4d]

As discussed for [1.E-3], White, in view of EMV, discloses or renders obvious this limitation.

g. [17.F]

As discussed for [1.F], White discloses this limitation.

h. [17.G]

As discussed for [1.G], White discloses this limitation.

i. [17.H]

As discussed for [1.H], White discloses this limitation.

3. Claims 2 and 18

White explicitly discloses that the mobile device may communicate with a POS terminal using NFC communications—hence “an NFC emulating device” communicating over a first communications channel.⁷ Ex[1013] 2:14-17; Ex[1008] ¶ 110. It would also have been obvious to a POSA to carry out EMV contactless transactions with NFC. Ex[1040] § 2.3.3; Ex[1008] ¶ 110. Further, for reasons stated for [1.A-3], [1.B], [1.C], [1.F], and [1.G], the mobile device in White is programmed to request and receive data associated with the account over the internet.

4. Claims 3 and 19

For reasons discussed for [1.A-4] and [1.E-2], the “payment number” in White, when generated by “mixing” input data and key, *i.e.* by encryption using a key as disclosed in White, is a response cryptogram, and a POSA implementing White to conduct EMV transaction would have found it obvious that the cryptogram is an Application Cryptogram (AC) which is a Message Authentication Code (MAC) under EMV.

⁷ According to the '171 Patent, “NFC emulating device” may refer to a “mobile device ... set to NFC mode in which it is emulating or pretending to be a card.” Ex[1001] 8:35-37.

An AC/MAC is a hash. '171 Patent describes “hash” as “[e]ncrypted data that cannot be un-encrypted.” Ex[1001] 25:39-40. EMV provides that a MAC is generated by (1) padding the input data with extra data, (2) encrypting the padded data, and (3) taking only the $s=8$ most significant bytes. Ex[1020] §§ 8.1.2, A1.2, B1.1. As a result, the input data is scrambled when encrypted by DES using CBC mode block cipher, *id.* A1.2, B1.1, Ex[1039], and the encrypted data is truncated in step (3), making it impossible to de-crypt and recover the input data. Ex[1034], 17-18; Ex[1008] ¶ 112. Thus, White, in view of EMV, discloses or renders obvious this element.

5. Claims 4 and 20

For reasons stated in Part IX.A, a POSA would have found it obvious and been motivated to implement White to carry out transactions in accordance with EMV.

6. Claims 5 and 21

For reasons stated in Part IX.A, a POSA would have found it obvious and been motivated to implement White to carry out transactions in accordance with EMV. It would not be clear to a POSA what this claim element means by reciting responding to a request for a first cryptogram with a second cryptogram. Ex[1008] ¶ 114. To the extent it means responding to a request for a second cryptogram after a request for a first cryptogram, EMV discloses that in addition to requesting, with

a GPO or GENERATE AC command, and generating a first ARQC cryptogram in response, for [1.E-2] and [17.E-4c], there may be a second command for generating a second cryptogram e.g. the second GENERATE AC command. Ex[1021] § 9.3.2. This is an optional step for “complet[ing] the transaction.” *Id.*; Ex[1008] ¶ 114.

On the other hand, to the extent this claim element means responding to the same (first) request for cryptogram with a cryptogram not requested, EMV also discloses this. For example, in response to a first request for cryptogram (GENRATE AC or GPO) from the POS terminal requesting for an approval (TC) cryptogram, a “Card” may respond with a decline (AAC) cryptogram if it decides that the transaction should be declined, or with an ARQC if it decides that online approval from issuer would be required. Ex[1021] § 9.3.1.

Accordingly, this element is obvious in view of White, in view of EMV.

7. Claims 6 and 22

As explained for Claims 3 and 19 *supra*, EMV provides that an Application Cryptogram (response cryptogram) is generated by encrypting the input data with the 3DES algorithm (DES algorithm executed three times), Ex[1043], 3, and taking only the $s=8$ most significant bytes (hence a portion of the output). Ex[1020] §§ 8.1.2, A1.2, B1.1. Accordingly, this element is disclosed or rendered obvious by White, in view of EMV.

8. Claims 7 and 23

White explicitly contemplates that the mobile device may not have connectivity to wireless network during the interrogation, by disclosing that “[a] customer using embodiments of the present invention can also conduct a transaction *outside of network coverage* by using near field communication (NFC) to communicate with the point-of-sale device.” Ex[1013] 2:13-17. Further, White discloses that a one-time digital key, or Session Key under EMV, is stored locally on the mobile device and thus there is no need to access wireless network during the interrogation, as stated for [1.H] and [17.H]. Ex[1008] ¶ 118. Accordingly, White discloses or renders obvious this element.

9. Claim 8

a. [8.PRE]

As discussed for [1.A-3], White discloses a remote computer system.

b. [8.A]

As discussed for [1.A-3], [1.B]-[1.C], White discloses or renders obvious that the mobile device requests and receives “a one-time digital key from payment server 140 through network 144,” which is a wireless network, prior to interrogation. Ex[1013] 4:53-55. Therefore, it would have been obvious that the one-time digital key is generated by the payment server. Ex[1008] ¶ 120. Further, because that key is used to generate a payment number, and the payment server would use the same

digital key to verify the payment number before approving a transaction, Ex[1013] 5:4-6, 19-25, it would therefore also be obvious that the payment server, in generating the one-time digital key, would associate the key with an account so that, when the payment server receives the payment number for verification, the server would know with which account the transaction is associated.

In addition, White discloses that the mobile application may host multiple accounts at the same time. *Id.* Fig. 6, 7:18-19.

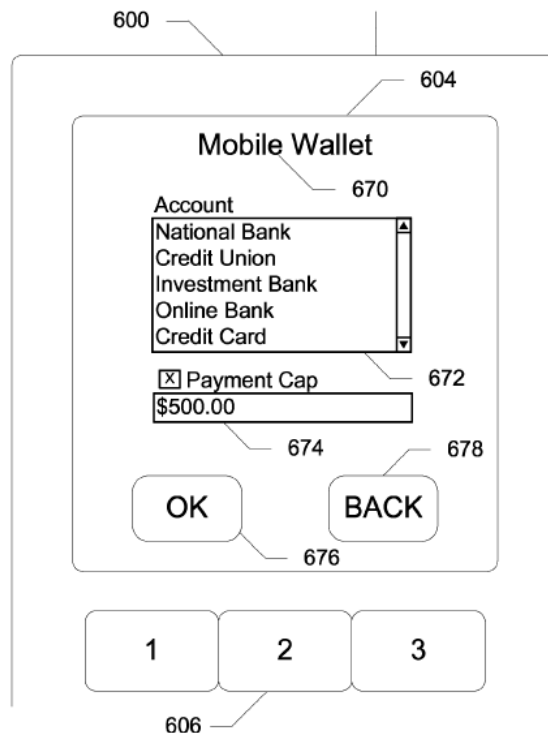


Figure 6

Accordingly, a POSA would have deemed it obvious to have the payment server (remote computer system) send the account identifier together with the digital key

so that the application knows with which account each key corresponds. Ex[1008] ¶ 123.

c. [8.B]

As discussed for [1.A-3], [1.F], and [1.G], White discloses or renders obvious that the mobile device requests and receives “a one-time digital key from payment server 140 through network 144,” which is a wireless network, after interrogation (hence a “second” key). Ex[1013] 4:53-55. Further, for the same reason as stated for [8.A], a POSA would have deemed it obvious to have the payment server (remote computer system) send the account identifier together with the digital key. Ex[1008] ¶ 124.

10. Claims 9 and 26

As discussed for [1.A-2c] and [1.A-3], White, alone or further in view of EMV, discloses a “digital credential” or “secure element representation” maintained at the remote computer system, rendering these claims obvious. Ex[1008] ¶ 125.

11. Claims 10 and 27

a. [10.PRE]/[27.PRE]

To the extent that the preamble is limiting, White discloses authorization by a server, which is a remote computer system. Ex[1013] 5:23-26. EMV further specifies that online authorization is performed by, inter alia, verification of an ARQC Application Cryptogram by a remote computer. Ex[1021] § 10.9.

b. [10.A]/[27.A]

White discloses that, under one embodiment, the payment server receives a payment number and amount through the POS terminal, and uses the information therein to approve a transaction. Ex[1013] 5:8-12, 19-25. A POSA would understand this as a request for authorization for transaction transmitted from the POS terminal, and deem it obvious that this request would also include an account identifier, for the reason that without such information, the payment server would not know from which or whose account the transaction amount should be deducted. Ex[1008] ¶ 127.

Further, a POSA implementing White to carry out EMV transactions would have found it obvious that an EMV transaction involves transmission of an authorization request to the issuer for verification. Ex[1021] § 10.9; Ex[1008] ¶ 128. Specifically, it was well understood in the art that an authorization request in EMV transactions would include, inter alia, the ARQC cryptogram, account identification data (including PAN), and an unpredictable number. Ex[1037], 57-58; Ex[1008] ¶ 128.

c. [10.B]/[27.B]

White discloses that the payment server “knows the one-time digital key in use” and would use it for verification of the payment number for approving a transaction from an account. Ex[1013] 5:19-26. Further, the authorization request

received by the server contains an account identifier such as a PAN. Ex[1037], 56-57; Ex[1008] ¶ 129. Moreover, as discussed for [10.C]/[27.C] below, in an EMV transaction, the authorization would involve determining and using the non-permanent session key to calculate an ARQC cryptogram for authentication.

d. [10.C]/[27.C]

While White does not explicitly disclose that the payment server would calculate a cryptogram, White discloses that the payment server would verify information in the “payment number,” Ex[1013] 5:19-26, which may be a cryptogram, and a POSA implementing White to carry out EMV transactions would have found it obvious to use an Application Cryptogram—specifically, an ARQC cryptogram as the cryptogram or payment number, as explained for [1.A-4]. Ex[1008] ¶ 130.

Further, a POSA would find it obvious to configure or modify White to conform to EMV, which provides that the server would generate the ARQC (which is also a Message Authentication Code or MAC) with the same key and the same input information, and compare that with the ARQC received in authorization request. Ex[1021] § 10.9 n.17; Ex[1037], 58; Ex[1008] ¶ 131.

As a specific method for verification, White would have the server decrypt the cryptogram and compare the input data with what is known to the server, Ex[1013] 5:19-21. EMV would have the server conduct an encryption calculation

using the one-time digital key and random number, and compare the resulting cryptogram with the cryptogram received. Ex[1021] § 10.9 n.17; Ex[1037], 58. A POSA would have been motivated to comply with the EMV approach in the combination as it was the standard approach already used by card issuers to verify transactions, and would have made White’s system more marketable to entities using the existing EMV infrastructure. Ex[1008] ¶ 132. Moreover, a POSA would have recognized that both the White and EMV approach to card and message authenticity were obvious implementation choices. *Id.*

Both approaches serve the same functions of “card authentication,” i.e., verifying that the transaction request does not originate from a fake card (or device), and of ensuring that the message was not modified in transit. Ex[1021] 10.9 n.17; Ex[1013] 1:48-53 (problem of fraudulent transaction from a “hacked device”); Ex[1034] 17-18; Ex[1008] ¶ 132. The two approaches are conceptually the same because, with either encryption or decryption, they use the same set of information to accomplish the same objective, where the server uses a secret—a one-time key—known to both the server and an authentic device to verify whether the input data and cryptogram correspond to each other given that key. Ex[1008] ¶ 132.

A POSA would expect success in making this modification because it was within the POSA’s level of skill to program a computer system to do either an encryption or a decryption operation. Ex[1008] ¶ 133. Further, as explained for

Claims 3 and 19, because the ARQC under EMV is a “hash”—that is, encrypted data that cannot be decrypted, a POSA seeking to use the device for EMV transaction would have no other choice but to use encryption, rather than decryption, to verify the cryptogram. *Id.* Therefore, a POSA would have found it obvious to make this modification of White to comply with EMV, rendering this element obvious. *Id.*

e. [10.D]/[27.D]

White explicitly discloses sending an authorization response to the POS terminal if the verification in [10.C]/[27.C] above is successful. Ex[1013] 5:23-26. It is understood in the art that, in EMV transactions, this would involve sending an authorization response, such as an ARC (Authorization Response Code) reflecting the issuer’s decision back to the POS terminal. Ex[1027] § A.2 at 101; Ex[1037], 59; Ex[1008] ¶ 134.

12. Claims 11 and 28

These claims are dependent on Claim 10 and 27, which further depend on Claims 1 and 17, and “set of inputs” here means inputs for generation of a response cryptogram. Ex[1001] Claims 1, 17. White explicitly discloses that the response cryptogram is generated by mixing a “random number” with a “one time-digital key,” Ex[1013] 5:6-8; 4:49-52, as explained in [1.A-4] and [1.E-2]. Further, EMV explicitly requires that input data for generation of the response cryptogram to include an “Unpredictable Number,” supplied by “[POS]Terminal.” Ex[1020]

§ 8.1.1. A POSA would understand the “Unpredictable Number” to be the random number in this context because it cannot be predicted by an attempted fraudster or attacker. Ex[1008] ¶ 135.

The “authorization data” refers to such data contained in the authorization request (Claims 10 and 27). It is well understood in the art that, in EMV transactions, the authorization request would include the unpredictable number. Ex[1037], 57; Ex[1008] ¶ 136. White discloses that the “[s]erver payment logic 142 includes a random number generating algorithm that is identical to that included in client payment logic 118 of mobile device 100.” Ex[1013] 5:13-16, and a POSA would have deemed it obvious to modify White to provide the unpredictable number to the server, to carry out EMV transactions. Ex[1008] ¶ 136.

Indeed, there are obvious efficiency reasons to make such a modification as well: it is not necessary to generate a supplemental random number at the server since under EMV, the POS is already providing an Unpredictable Number (random number), both to the payment device (“Card”) as input data for Application Cryptogram (e.g. ARQC) generation and also in the authorization request to the server; it is easier to simply have the server use that random (or unpredictable) number received in the authorization request to regenerate the ARQC for verification. Ex[1008] ¶ 137; Ex[1020] § 8.1.1; Ex[1037], 57-58.

Further, as explained above for [10.C]/[27,C], in an EMV transaction, the server also calculates the same ARQC cryptogram using the same key and the same input data as the “Card” did, to verify the ARQC cryptogram in the authorization request.

Accordingly, White in view of EMV renders these claims obvious.

13. Claims 12 and 29

The “POS command communication[]” has antecedent basis in Claims 1 and 17, which recite that it is “sent by the POS terminal” and “comprises a request for digital credential data to authorize a transaction.” As explained above for [1.A-4], [1.E-1], [1.E-2], in an EMV transaction, the “Card” generates an Application Cryptogram, such as an ARQC, in response to commands from the POS terminal. It is also well known in the art that communications from the POS terminal are commands and the “Card” responds to such commands. Ex[1037], 48; Ex[1008] ¶ 140. EMV further provides that the input data for generating the Application Cryptogram includes “Unpredictable Number” that is provided by “Terminal.” Ex[1020] § 8.1.1. Therefore, a POSA would have understood or found it obvious that a POS command communication would comprise unpredictable data for the Card or mobile device to generate the response cryptogram. Ex[1008] ¶ 140.

14. Claims 13 and 30

White explicitly discloses that the authorization request received by payment server includes “the amount” for a sale of goods, which is a “value from the transaction,” Ex[1013], 4:61-63, 5:2-4, 8-12, as also explained for [10.A]/[27.A]. Further, it is understood in the art that, in an EMV transaction, the authorization request would include values from the transaction including “[a]ll the data objects necessary to reproduce the transaction claim,” Ex[1037], 58, which usually include information such as amount and currency code. Ex[1008] ¶ 141. Accordingly, White alone or in view of EMV discloses or renders obvious these claims.

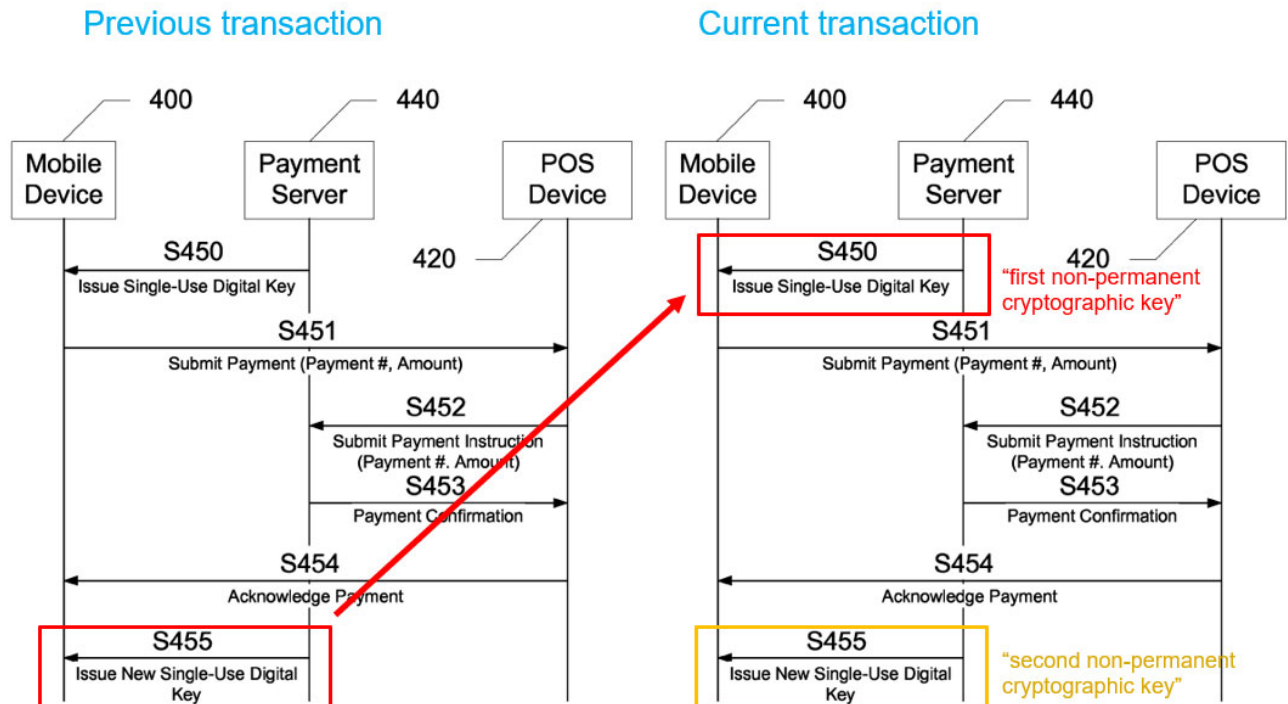
15. Claims 14 and 31

As explained for [1.A-3]-[1.A-4], [1.B]-[1.C], [1.F]-[1.G], White discloses a “one-time digital key” (a Session Key in an EMV transaction), which is a “non-permanent cryptographic key” White explicitly discloses that, “[w]ith the payment *completed*, payment server 440 issues a new one-time digital key S455 to mobile device 400.” Ex[1013], 6:40-42. Accordingly, the “second non-permanent cryptographic key” is shared by a remote payment authorization process.

Further, it is obvious that this new one-time digital key may be used for the next transaction, because otherwise it would be wasteful and pointless to deliver a key with no intention to use it, and thus the “first non-permanent cryptographic key” in a transaction is usually the “second non-permanent cryptographic key” from the

previous transaction, as demonstrated below. Ex[1013] Fig. 4 (annotated); Ex[1008]

¶ 143.



Accordingly, White discloses or renders obvious these claims.

16. Claims 15 and 32

For reasons stated in Part IX.A, a POSA would have found it obvious and be positively motivated to implement White to carry out EMV transactions, for many economic, security, and efficiency reasons. Further, as explained for [1.A-4] and [17.E-4c], a POSA would have followed EMV's specifications to generate the response cryptogram, which would be an Application Cryptogram. Accordingly, White in view of EMV renders these claims obvious.

17. Claims 16 and 33

As explained above for [1.A-3], [1.C], [1.G], [17.E-2], [17.G], White discloses one-time digital keys as the “first and second non-permanent cryptographic keys,” and a POSA would find it obvious to use a Session Key under EMV as such one-time digital key to implement White to carry out EMV transactions.

As further explained in *supra* Part VIII.D.3, the “Session Key” is generated using an ICC Master Key (MK), which is further generated using an Issuer Master Key IMK, and is therefore associated with an issuer master key. Ex[1020] §§ A1.3.1-A1.4. Accordingly, White in view of EMV renders these claims obvious.

18. Claim 24

For the same reason as stated in [17.F]-[17.G], White renders this Claim obvious.

19. Claim 25

For the same reason discussed for [8.A]-[8.B], White renders this element obvious.

In conclusion, all claims of the '171 Patent are obvious either over White alone or in view of EMV.

C. Ground 2: Claims 1-33 Are Obvious Over *Mellqvist* in View of EMV

1. Obviousness Over *Mellqvist* in General

Mellqvist discloses an NFC-enabled portable device and explicitly teaches that its invention is suitable for NFC credit card transactions at a POS reader. Ex[1014] [0033]. A POSA would be motivated to implement Mellqvist to carry out standardized credit card payment transactions under EMV. Ex[1008] ¶ 150; *supra* Part IX.A. Further, a POSA implementing Mellqvist to carry out EMV transactions would arrive at the solution described in '171 Patent by choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success. MPEP § 2141.

Specifically, Mellqvist discloses secure elements hosted in remote servers and storing payment applications. Ex[1014] [0036]. As explained above in [1.A-1] and [1.A-2] of Ground 1, it is well understood in the art payment applications would respond to POS commands with digital credential data necessary to authorize payment transactions. It is also well understood that data necessary for such authorization are data provided by either the “Card” or the POS terminal during the interrogation. Ex[1037], 57-58; Ex[1008] ¶ 152. All of these necessary (“[a]lways” included) data as listed in EMV (*e.g.* Ex[1027] § B.1.1) can be categorized into three categories:

- (a) **Data to be provided by the Terminal.** This includes, inter alia, transaction Amount, Currency Code, Transaction Date, Transaction Type, and Unpredictable Number (Reader-Terminal);
- (b) **Data to be provided by the “Card” and knowable prior to initiation of a transaction at a POS terminal.** This includes, inter alia, Application Transaction Counter (ATC), and Track 2 Equivalent Data.⁸
- (c) **Data to be provided by the “Card” and but not knowable prior to initiation of a transaction.** The Application Cryptogram (AC) belongs to this category, because AC is calculated using transaction-specific data and Unpredictable Number provided by POS terminal during interrogation. Ex[1020] § 8.1.1.

Ex[1008] ¶ 152.

Because the portable device of Mellqvist is a user device equivalent to the “Card,” Ex[1014] [0033], a POSA would understand the secure elements in Mellqvist as providing data to be provided by “Card,” that is, categories (b) and (c) above. Ex[1008] ¶ 153.

⁸ As explained above, this includes basic card information such as PAN and expiration date. *Supra* Part VIII.D.2.

A POSA would therefore have only a finite number of potential solutions to implement Mellqvist to carry out EMV credit card transactions. First, one could have remote secure elements 171-174 provide all items in (b) and (c), and the user device merely relays interrogation messages between the remote secure element and the POS terminal. Ex[1008] ¶ 154. However, because there are multiple messages being exchanged in an EMV transaction, Ex[1026] §§ 2.3.3, 3.4.3, the latency caused by roundtrip between the user device and the remote secure elements will be significant, in particular over cellular wireless network, a well-known problem in the art as of the priority date of the '171 Patent. Ex[1008] ¶ 154; *see also* Ex[1017] 48:30-35. This would be undesirable because the user needs to hold the device next to the reader during this whole time. Ex[1029] §§ 2.4, A.1; Ex[1014] [0032]; Ex[1008] ¶ 155. Further, the user must have wireless network connection (e.g. cellular coverage) throughout the interrogation, which is not guaranteed, and was particularly a problem in in-door environments as of 2011, such as public transit, as was well known in the art. Ex[1008] ¶ 155; Ex[1044] ¶¶ 4.41-43.

A second solution would utilize the optional hardware secure element or memory of the portable device and store information in category (b) in advance. Ex[1008] ¶ 156. Because information in this category is knowable in advance, they may be provisioned to the device at any time. *Id.* The remote secure elements would be responsible for generating AC (category (c)). *Id.* This solution reduces latency,

but still requires that the user have network connection (e.g. cellular coverage) during the interrogation to request and receive the AC. *Id.*

The final solution, then, would be to use processor or hardware secure element of the portable device to generate the AC, with only minimal information requested from the remotely hosted SE. *Id.* ¶ 157. The device has a processor but also needs the Session Key to compute an AC. *Id.*; *supra* Part VIII.D.3. Thus, a POSA would have found it obvious to configure the virtual secure element module 192 in Mellqvist to access remote secure element server 170 and obtain the Session Key, which can be conducted at any time between two transactions so long as the device has network coverage. Ex[1008] ¶ 158.

This is also consistent with Mellqvist's disclosure that the remotely hosted secure elements are to provide a "predetermined level of security" for transactions to eliminate the need to maintain such level of security at the mobile device. Ex[1014] [0004], [0035]. If the Session Key is to be generated locally at the mobile device, this would require having the ICC Master Key in the device. Ex[1020] § A1.3.1; Ex[1008] ¶ 159. Because the ICC Master Key is tied to the card and is usually kept in a hardware secure element or microchip in a chip card, Ex[1037], 65-66, this would require maintaining the "predetermined level of security" in the mobile device and would be contrary to Mellqvist's teaching. Ex[1008] ¶ 159. Instead, because AC calculation requires only the Session Key, Ex[1020] § A1.2, it

makes sense to request and store only the Session Key on the mobile device. Ex[1008] ¶ 160. The Session Key is useful for only a single transaction, limiting fraud exposure compared to storing the ICC Master Key on the mobile device. *Id.*

In sum, given the well-known practical constraints from network latency and coverage, and in light of the finite number of categories of standardized digital credential data, a POSA implementing Mellqvist to conduct EMV credit card transactions had a finite number of solutions and would have found it obvious to configure Mellqvist to request only a Session Key from the remotely hosted secure elements. Ex[1008] ¶ 161.

All claim elements below are obvious over Mellqvist in view of EMV.

2. Claim 1

a. [1.PRE]

To the extent the preamble is limiting, both Mellqvist and EMV disclose such a method. Both disclose a “mobile” or “portable” device. Ex[1014] [0046], Fig. 2; Ex[1023] § 4.1. Both disclose a “secure application” for “payment card transaction.” *E.g.*, Ex[1014] [0046]; Ex[1037] 38-41; *see generally* Exs[1021], [1023].

b. [1.A-1]

Both Mellqvist and EMV disclose such a “mobile device.” Mellqvist discloses a “portable electronic device” (“portable device”) which includes a

processor which may be, among other things, a “cellular radio telephone,” including a “processor” and an “application” for payment. Ex[1014] [0033]-[0034] [0040]. A POSA would understand that an obvious way to operate a processor is to execute an application on an operating system of the mobile device. Ex[1008] ¶ 163.

Further, a POSA implementing Mellqvist would have found it obvious to refer to EMV, and understood “Card” for contactless payment transactions using a mobile device containing its processor and memory and capable of emulating a contactless or NFC card. Ex[1037], 57-60. For the same reason as stated above in Ground 1, [1-A.1], EMV discloses or renders obvious this element, because it is well understood in the art that a card application would run on a card or equivalently in a mobile device processor because such applications require only basic arithmetic operations that a mobile phone processor is perfectly capable of handling. Ex[1008] ¶ 164.

c. [1.A-2]

(1) [1.A-2a]

The '171 Patent suggests that interrogation refers to querying or extraction of information. *E.g.*, Ex[1001], 6:3-5; 6:50-53. Mellqvist discloses that the portable device can use NFC for short-range communications and user “can pay by simply waving their portable device at a point-of-sale reader,” Ex[1014], [0033], [0035], which a POSA would understand as disclosing this element. Ex[1008] ¶ 165; Ex[1015], [0062], [0070].

(2) [1.A-2b]

The '171 Patent defines “digital credential data” as data necessary to authorize approval of a transaction at a POS terminal. Ex[1001], 7:3-7. Because Mellqvist discloses a system for “payment” applications, Ex[1014] [0033], [0036], a POSA would have understood this as disclosing that the applications are interrogable for data required to authorize payment from a user’s account. Ex[1008] ¶ 166.

(3) [1.A-2c]

As explained in [1.A-2c] for Ground 1, a “digital credential” may be actual SE hardware, virtual hardware secure elements, or data hosted on a server. Ex[1001] 9:44-58, 26:34-35. Mellqvist discloses or renders obvious this element by disclosing “secure elements” remotely hosted on a server containing payment applications. Ex[1014] [0036].

d. [1.A-3]

Mellqvist discloses that portable device 190 connects wirelessly with servers which hosts the remote secure elements. Ex[1014], [0031], [0036]. This connection cannot be made using NFC (“first communication channel” for interrogation by POS terminal) because NFC can communicate over only a short range of a few centimeters. *Id.* [0003]. Further, for similar reasons as explained for [1.A-3] of Ground 1 and in Part IX.C.1 *supra*, a POSA implementing Mellqvist to conduct

“credit card” payment transactions, Ex[1014], [0033], would also have found it obvious to configure application of portable device 190 to request, from remotely hosted secure elements, a Session Key, which is data associated with the account because it is derived from an ICC Master Key generated from the account number, *supra* Part VIII.D.3.

e. [1.A-4]

Under EMV, the Session Key is data associated with the account and is not a “permanent” cryptographic key because it is unique to each transaction. Ex[1020] § A1.3.1. As explained for [1.E-1] and [1.E-2] in Ground 1 above, the “Card” generates and returns an AC at the request of terminal commands GENERATE AC or GPO during the interrogation.

As explained above, a POSA implementing Mellqvist to conduct “credit card” payment transactions, Ex[1014] [0033], would have found it obvious to configure application of device 190 to request only a Session Key from the remote server and generate an Application Cryptogram (AC) with that key, rendering this element obvious. *Supra* Part IX.C.1.

f. [1.B]

For the same reason as explained for [1.A-3], this element is obvious over Mellqvist in view of EMV.

g. [1.C]

It was well known in the art and required by EMV that responses from the “Card” (or portable device here) during interrogations are response APDUs (R-APDU), and the AC would be passed back to POS terminal in a R-APDU. Ex[1037], 46-48; Ex[1021] §§ 6.1-6.2, 6.5.5; Ex[1008] ¶ 172. Accordingly, for the same reason as explained for [1.A-3] and [1.A-4], this element is obvious over Mellqvist in view of EMV.

h. [1.D]

As explained above, a POSA would have found it obvious to configure Mellqvist’s portable device to request a Session Key before a transaction, because the device is not guaranteed to have network connectivity during a transaction. *Supra* Part IX.C.1. Thus, the Session Key must obviously be stored on the device until used in a transaction. Ex[1008] ¶ 173.

i. [1.E]

As explained above for [1.A-1] and [1.A-2a], payment application on Mellqvist’s portable device participates in an interrogation with a POS terminal.

j. [1.E-1], [1.E-2], [1.E-3]

For the same reason stated for [1.E-1] to [1.E-3] in Ground 1, EMV prescribes these elements, where the Application Cryptogram is a response cryptogram that does not include the Session Key and is the local cryptographic key as explained in

[1.D] of this Ground. Therefore, these elements are obvious over Mellqvist in view of EMV.

k. [1.F]

As explained above, because the Session Key is unique to each transaction, Ex[1020] § A1.3.1, a POSA would have found it obvious to program the application to request a new Session Key from the remotely hosted secure elements between two transactions, i.e., after a transaction. *Supra* Part IX.C.1. In particular, because it is uncertain that the user will have wireless network connection during the next transaction, *id.*, it is imperative that the application requests the new Session Key (“second non-permanent cryptographic key”) soon after authorization of a transaction (hence consumption of the last Session Key) if the device has wireless connection. Ex[1008] ¶ 178.

l. [1.G]

As explained above for [1.A-3] and [1.A-4], the Session Key is a non-permanent cryptographic key associated with the account. Thus, for the reasons explained in [1.F] above, this element is obvious over Mellqvist in view of EMV.

m. [1.H]

As explained for [1.D] and [1.F], a POSA would have found it obvious to configure the application to request a new Session Key after a completed transaction as soon as the device has wireless connection and to store the key. Ex[1008] ¶ 180.

3. Claim 17

a. [17.PRE]-[17.A]

To the extent the preamble is limiting, as discussed for [1.PRE], [1.A-1] and [1.E], Mellqvist alone or in view of EMV discloses these limitations.

b. [17.B]

Mellqvist discloses a portable device that has a “NFC frontend” and may be used for NFC payment transactions involving a POS reader. Ex[1014] [0033], [0040]. The “NFC frontend” is in communication with a processor of the device.” *Id.* [0040]. Therefore, a POSA would understand or find it obvious that the NFC frontend 250, alone or under control of processor 295, serves as a controller routing communications received over an NFC communication channel. Ex[1008] ¶ 183.

c. [17.C]

Mellqvist discloses that the portable device has a “transceiver” 212 that may communicate with a base station 260. *Id.* [0041], Fig. 2. For reasons stated for [1.A-4], this is a communications channel separate from the NFC communications. *Id.*

d. [17.D]

Mellqvist discloses that the portable device has a processor. Ex[1014] [0040]-[0041]. Moreover, it was well known in the art that a “Card” in EMV transactions also contains a processor. Ex[1037] 38-41; Ex[1008] ¶ 185.

e. [17.E]

For reasons discussed for [1.A-1], [1.A-2], and [1.A-4], Mellqvist discloses such an application. Further, Mellqvist discloses the claimed computer “storage medium” having “program code.” Ex[1014] [0023]. An EMV “Card” similarly has such an application stored in the memory and accessible to the processor. Ex[1037], 38-41. Therefore, this element is obvious over Mellqvist in view of EMV.

(1) [17.E-1] to [17.E-4]

For reasons discussed for [1.B] to [1.E], these elements are obvious over Mellqvist in view of EMV.

(2) [17.E-4a] to [17.E-4d]

As discussed for [1.E-1] to [1.E-3], these elements are disclosed by EMV and thus obvious over Mellqvist in view of EMV, with Application Cryptogram generated using the previously stored local Session Key.

f. [17.F] to [17.H]

As discussed for [1.F] to [1.H], these elements are obvious over Mellqvist in view of EMV.

4. Claims 2 and 18

Both Mellqvist and EMV explicitly disclose that the mobile device may communicate with a POS terminal using NFC communications—hence “an NFC emulating device” communicating over a first communications channel. Ex[1001]

8:35-37; Ex[1014], [0033], [0040]; Ex[1040] § 2.3.3. Further, for reasons stated for [1.A-3], [1.B], [1.C], [1.F], and [1.G], the portable device in Mellqvist is programmed to request and receive data associated with the account over the internet.

5. Claims 3 and 19

As discussed for [1.E-2] and Claims 3 and 19 in Ground 1, under EMV, the Application Cryptogram is a response cryptogram, and is a hash.

6. Claims 4 and 20

For reasons stated in Parts IX.A and IX.C.1, a POSA would have found it obvious and be positively motivated to implement Mellqvist to carry out EMV transactions, for many economic, security, and efficiency reasons, and in light of Mellqvist's explicit disclosure that the invention is suitable for NFC credit card transactions, Ex[1014] [0033].

7. Claims 5 and 21

For reasons stated for Claims 5 and 21 in Ground 1, these claims are disclosed by EMV and thus are obvious over Mellqvist in view of EMV.

8. Claims 6 and 22

For reasons stated for Claims 6 and 22 in Ground 1, these claims are disclosed by EMV and thus are obvious over Mellqvist in view of EMV.

9. Claims 7 and 23

As discussed in Part IX.C.1 above, a POSA would have understood that the user possibly does not have connectivity to wireless network during an interrogation for a transaction and thus would provide for acquisition of a Session Key prior to a transaction. Accordingly, these claims are obvious over Mellqvist in view of EMV.

10. Claim 8

a. [8.PRE]

Mellqvist's "remote secure element servers" satisfy this element. Ex[1014] [0035]-[0036].

b. [8.A]

As discussed for [1.A-3], [1.B]-[1.C], Mellqvist in view of EMV renders it obvious that the mobile device requests and receives a first Session Key from the remotely hosted secure elements. Therefore, it would have been obvious to have such remote secure elements generate the Session Key. Ex[1008] ¶ 205. Further, Mellqvist discloses that each remote secure element server may host multiple secure elements at a time, which a POSA may understand to allow hosting secure elements for multiple accounts or cardholders/customers. Ex[1014], [0036]. Accordingly, a POSA would have deemed it obvious to have the server send the account identifier together with the Session Key so that the application knows with which account the key corresponds. Ex[1008] ¶ 205.

c. [8.B]

As discussed for [1.A-3], [1.F], and [1.G], Mellqvist in view of EMV renders it obvious that the requests and receives a second Session Key associated with the account, over the wireless network from the remotely hosted secure elements. Therefore, it would have been obvious to have such secure elements generate the Session Key. Ex[1008] ¶ 206. Further, for the same reason as stated for [8.A], a POSA would have deemed it obvious to have the remote server send the account identifier together with the Session Key. *Id.*

11. Claims 9 and 26

As explained above for [1.A-2c], Mellqvist explicitly discloses remotely hosted secure elements, Ex[1014] [0036], and thus disclose these claims.

12. Claims 10 and 27

Each claim element below is obvious over Mellqvist in view of EMV:

a. [10.PRE]/[27.PRE]

To the extent the preamble is limiting, EMV specifies that such online authorization is performed by verification of ARQC, an Application Cryptogram, by a remote computer. Ex[1021] § 10.9. A POSA would understand this to be carried out on a remote server or server network. Ex[1008] ¶ 208.

b. [10.A]/[27.A]

A transaction under EMV satisfies this element because it was well known in the art that the server receives an authorization request from the POS terminal including, inter alia, the Application Cryptogram (ARQC) (response cryptogram), account identification data (including PAN) (account identifier), and the unpredictable number. Ex[1037], 57-58; Ex[1008] ¶ 209.

c. [10.B]/[27.B]

A transaction under EMV satisfies this element because it was well known in the art that the server would verify the ARQC by calculating the same cryptogram, which necessarily involves deriving the same cryptographic key associated with the account. Ex[1037], 58; Ex[1008] ¶ 210.

d. [10.C]/[27.C]

As discussed for [10.C]/[27.C] in Ground 1, a transaction under EMV satisfies this element. Accordingly, this element is obvious over Mellqvist in view of EMV.

e. [10.D]/[27.D]

As discussed for [10.D]/[27.D] in Ground 1, a transaction under EMV satisfies this element.

13. Claims 11 and 28

As discussed for Claims 11 and 28 in Ground 1, these claims are satisfied by a transaction under EMV and are thus obvious over Mellqvist in view of EMV.

14. Claims 12 and 29

As discussed for Claims 12 and 29 in Ground 1, these claims are satisfied by a transaction under EMV and are thus obvious over Mellqvist in view of EMV.

15. Claims 13 and 30

As discussed for Claims 13 and 30 in Ground 1, these claims are satisfied by a transaction under EMV and are thus obvious over Mellqvist in view of EMV.

16. Claims 14 and 31

As discussed for [1.F] of this Ground, a POSA would have found it obvious to configure the application to request the new Session Key as soon as possible *upon authorization of a transaction* which consumes the last Session Key, so that a new, unused Session Key can be ready for the next transaction, and thus the key is shared as part of the “authorization process.” Ex[1008] ¶ 216. Further, for reasons similar to those stated for Claims 14 and 31 in Ground 1, a POSA would have understood that the “second non-permanent cryptographic key” in reference to one transaction will be the “first non-permanent cryptographic key” of the next transaction to avoid unused keys.

17. Claims 15 and 32

For reasons stated in Parts IX.A and IX.C.1, a POSA would have found it obvious and been positively motivated to implement Mellqvist to carry out mainstream payment card transactions, in particular EMV transactions, and in light

of Mellqvist's explicit disclosure that the invention is suitable for NFC credit card transactions. Ex[1014] [0033]. EMV prescribes generation of an Application Cryptogram, which is a response cryptogram, rendering it obvious to implement these claims with Mellqvist in accordance with EMV. Ex[1020] § 8.1.2.

18. Claims 16 and 33

As explained above for [1.A-3], [1.C], [1.G], [17.E-2], [17.G], a POSA would have found it obvious to use the Session Key under EMV as the “first and second non-permanent cryptographic keys.” As further explained *supra* Part VIII.D.3, the “Session Key” is generated using an ICC Master Key (MK), which is further generated using an Issuer Master Key IMK, and is therefore associated with an issuer master key. Ex[1020] §§ A1.3.1-A1.4. Accordingly, these claims are obvious over Mellqvist in view of EMV.

19. Claim 24

For the same reason as stated in [17.F] and Claims 14 and 31, this claim is obvious over Mellqvist in view of EMV.

20. Claim 25

For the same reason discussed for [8.A] and [8.B], White renders this element obvious.

Thus, all claims of the '171 Patent are obvious in view of Mellqvist in view of EMV.

X. SECONDARY CONSIDERATIONS

As explained in IPR2023-01289, Paper No. 1, two references, *Collinge* and *Fiske*, both with the priority date April 2, 2012, anticipate or render obvious all claims of the '171 Patent. While they are not relied upon as prior art in this Petition because this Petition assumes an August 30, 2011 priority date for the '171 Patent, they are persuasive evidence of obviousness because the inventors of *Collinge* and *Fiske* independently invented the solution claimed in the '171 Patent around the same time (2011 to early 2012). Indeed, *Fiske* originates from a U.K. patent application filed April 5, 2011, more than four months before the earliest priority date of the '171 Patent assumed in this Petition. Ex[1012] (Field (30)). While the UK application might not be prior art under pre-AIA 35 U.S.C. § 102(e), it is positive proof that *Fiske* invented the claimed application even before the inventor of the '171 Patent. Thus, near-simultaneous invention weighs in favor of obviousness. *See Trs. of Columbia Univ. in City of N.Y. v. Illumina, Inc.*, 620 F. App'x 916, 929 (Fed. Cir. 2015); *Accord Healthcare Inc. v. Daiichi Sankyo Co., Ltd.*, No. IPR2015–00865, 2016 WL 5224324 (P.T.A.B. Sept. 12, 2016).

Patent Owner may argue that '171 Patent's claimed invention is not obvious based on secondary considerations of praise and awards from the industry, where the inventor's company, SimplyTapp, was “awarded Best Contactless Payments Solution of the Year at the 2015 Future Digital Awards.” Ex[1045], 2-3 (citing

webpage in Ex[1046]). However, a closer examination reveals that the award was directed at having the POS terminal accessing “a secure payment *application in the cloud*” to complete the transaction, without any reference to “executing an application” “at a mobile device” that would, *inter alia*, “generat[e] a response cryptogram” (Ex[1001] cl. 1), Ex[1047], as claimed by the ’171 Patent. Thus, such evidence of secondary considerations of nonobviousness “are not commensurate with the claim scope and are therefore unpersuasive.” *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998). *See also* Ex[1014], [0035]-[0036] (disclosing by 2009, the use of “remote secure element server” storing “payment...applications” to perform “NFC transactions”).

XI. CONCLUSION

Petitioner respectfully request institution of IPR and cancelation of Claims 1-33 of the ’171 Patent as unpatentable.

Date: September 6, 2023

Respectfully submitted,

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

CERTIFICATE OF SERVICE

The undersigned hereby certifies on this September 6, 2023, that true and correct copies of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 10,032,171, Exhibits 1001-1048, and Power of Attorney were served in their entirety on the following parties via Priority Mail Express:

26191 - Fish & Richardson P.C. (TC)
PO Box 1022
Minneapolis, MN 55440-1022
United States

With courtesy copy to litigation counsel via email:

Spencer Hosie (shosie@hosielaw.com)
Diane S. Rice (drice@hosielaw.com)
Darrell R. Atkinson (datkinson@hosielaw.com)
HOSIE RICE LLP
505 Sansome Street, Suite 1575
San Francisco, CA 94111
Tel: (415) 247-6000
Fax: (415) 247-6001

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

Date: September 6, 2023

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 Petition complies with the type-volume limitation of 14,000 words, comprising 13,985 words, excluding the parts exempted by 37 C.F.R. § 42.24(a).

2. This Petition 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 6, 2023

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