

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INCORPORATED AND MASTERCARD INTERNATIONAL
INCORPORATED
Petitioner

v.

OV LOOP, INC.
Patent Owner

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

IPR2023-01290

DECLARATION OF MATTHEW CALMAN
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,032,171

TABLE OF CONTENTS

I.	INTRODUCTION	4
II.	Background and Qualifications	5
	A. Educational Background	5
	B. Career History	5
	C. Materials and Other Information Considered	8
III.	Understanding of the Law	8
	A. Legal Standard for Obviousness	8
	B. Legal Standard for Claim Construction	11
IV.	The '171 Patent.....	12
V.	Level of Ordinary Skill in the Art	12
VI.	Claim Construction.....	13
VII.	Summary of the Prior Art.....	14
	A. Technical Background on Payment Systems	14
	B. White (Ex[1013])	16
	C. Mellqvist (Ex[1014]).....	19
	D. EMV (Ex[1019] to Ex[1029]).....	21
	1. EMV Generally	21
	2. Transaction Flow.....	24
	3. Session Key and Application Cryptogram Generation.....	26
	4. Subsequent Processing.....	27
VIII.	Grounds of Invalidity.....	28
	A. Motivation to Combine	28
	B. Ground 1: Claims 1-33 Are Obvious Over <i>White</i> Further in View of EMV	30
	1. Claim 1	30
	2. Claim 17	54
	3. Claims 2 and 18: “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”; “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.” 59

4. Claims 3 and 19: “wherein the response cryptogram is a hash” 60
5. Claims 4 and 20: “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” 61
6. Claims 5 and 21: “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” 61
7. Claims 6 and 22: “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” 62
8. Claims 7 and 23: “wherein the mobile device does not have connectivity to the wireless network during the interrogation” 63
9. Claim 8 63
10. Claims 9 and 26: “wherein the digital credential comprises a secure element representation maintained at the remote computer system”; “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” 66
11. Claims 10 and 27 66

12.	Claims 11 and 28: “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”	71
13.	Claims 12 and 29: “wherein the POS command communications comprise the unpredictable data”	72
14.	Claims 13 and 30: “wherein the authorization data further comprises values from the transaction”	73
15.	Claims 14 and 31: “wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process”....	74
16.	Claims 15 and 32: “wherein the application is [configured/executable] to generate the response cryptogram according to a card specification”	75
17.	Claims 16 and 33: “wherein the first and second non-permanent cryptographic key are associated with an issuer master key”...76	
18.	Claim 24: “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation”	76
19.	Claim 25: “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”	76
C.	Ground 2: Claims 1-33 Are Obvious Over <i>Mellqvist</i> Further in View of EMV	77
1.	Obviousness Over <i>Mellqvist</i> in General	77
2.	Claim 1	83
3.	Claim 17	91
4.	Claims 2 and 18: “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”; “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.” 96
5.	Claims 3 and 19: “wherein the response cryptogram is a hash” 97
6.	Claims 4 and 20: “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” 97
7.	Claims 5 and 21: “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” 97
8.	Claims 6 and 22: “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” 98
9.	Claims 7 and 23: “wherein the mobile device does not have connectivity to the wireless network during the interrogation”98
10.	Claim 8 98
11.	Claims 9 and 26: “wherein the digital credential comprises a secure element representation maintained at the remote computer system”; “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” 100
12.	Claims 10 and 27.....100
13.	Claims 11 and 28: “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” 102

14.	Claims 12 and 29: “wherein the POS command communications comprise the unpredictable data”	102
15.	Claims 13 and 30: “wherein the authorization data further comprises values from the transaction”	102
16.	Claims 14 and 31: “wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process”..	103
17.	Claims 15 and 32: “wherein the application is [configured/executable] to generate the response cryptogram according to a card specification”	103
18.	Claims 16 and 33: “wherein the first and second non-permanent cryptographic key are associated with an issuer master key”.104	
19.	Claim 24: “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation”	104
20.	Claim 25: “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”	105
IX.	Reservation of Rights	105
X.	DECLARATION	106

LIST OF EXHIBITS

Exhibit No. ¹	Description
1001	U.S. Patent No. 10,032,171 (the “’171 Patent”)
1002	File History of the ’171 Patent
1003	Reserved
1004	Reserved
1005	Reserved
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.

Expert Declaration for *Inter Partes* Review
U.S. Patent No. 10,032,171

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

I. INTRODUCTION

I, Matthew Calman, declare as follows:

1. My name is Matthew Calman. I submit this declaration in support of a Mastercard Incorporated and Mastercard International Incorporated (“Petitioner”) petition for *Inter Partes* Review of U.S. Patent No. 10,032,171 (“the ’171 Patent”).

This declaration contains my opinions regarding how a hypothetical person of ordinary skill in the art (“POSA”) would understand the ’171 Patent, and whether certain claims that patent are invalid.

2. This declaration contains my opinions as of today, and the bases and reasons for those opinions. After further review of materials in this case, including opinions and/or testimony of other expert witnesses, I reserve the right to offer additional opinions. This declaration is based upon my personal knowledge and, if asked to testify, I would testify competently to the matters contained herein. For my efforts in connection with the preparation of this declaration I have been compensated at my standard rate for consulting, which is \$750 per hour for all activities. My compensation is not contingent on the results any proceedings relating to the above-captioned patent.

II. BACKGROUND AND QUALIFICATIONS

3. In rendering my opinions, I relied upon my education, training, knowledge, and experience, which is summarized below. My curriculum vitae is attached as Appendix A to this declaration.

A. Educational Background

4. I received my Master of Business Administration degree from Georgia State University's Executive MBA program in 1999 and was awarded the *George J. Malonos Award for Academic Excellence*. As an undergraduate, I attended Carnegie Mellon University as an engineering and mathematics student from 1982-1984.

B. Career History

5. I am currently employed as an Adjunct Professor of statistics in the Business Administration department of Coe College, a liberal-arts college in Cedar Rapids, Iowa, USA, where I reside. I am also an innovation consultant and expert witness for U.S. and Canadian banks, financial and technology firms supplying deposit, payment, mobile and related financial services and technology solutions.

6. I was employed by Bank of America and its predecessor banks for 27 years, from 1986 – 2013. In the 1980's and 1990's, I was Vice President of Corporate Trust Automation, responsible for capital market systems servicing over one million stock and bond holders. From 1996-2003, I managed more than twenty technical

platform integrations and deposit operations consolidation projects during Bank of America's growth by merger. From 2003-2006 I was the Business Champion for a \$135 million digital transformation of check image processing, leading the core team responsible for business requirements, process design and transformation leadership.

7. From 2006-2013, I was R&D Executive of the Gateway Innovation Lab and additionally, from 2009-2011, was appointed Research Affiliate at the MIT Media Lab, where I led the *Center for Future Banking*. My lab team created over 500 prototypes including Bank of America's tests and trials of NFC contactless payments with Blackberry and Apple devices in controlled tests 2011-2012 in Charlotte, NC and New York, NY. (<https://www.atmmarketplace.com/articles/bank-of-america-to-pilot-payments-with-mobile-phones-in-new-york/>)

8. Later, in 2013, I led the Bank of America "eSAFE" team responsible for e-Commerce Security, Authentication, Fraud, and Enrollment. My team developed Bank of America's five-year roadmap of technologies and policies to improve the customer experience and enhance the Bank's security defenses. Capabilities on the plan included reliable device fingerprinting, location-based authentication, mobile network integration, collaborative authentication (e.g., the FIDO alliance), biometrics, behavioral metrics, machine learning, cryptography, credential tokenization, secure elements ("SE"), and multi-band authentication.

9. From 2015-2018, I was Principal Program Manager at Microsoft in their Commercial Software Engineering division. Our *Innovation Outreach Program* delivered cutting edge cryptography, cloud, artificial intelligence, and credential management technologies in targeted solutions for select Fortune-100 clients.

10. I was a founding member of the Federal Reserve's Mobile Payments Industry Workgroup, a board member of the Smart Card Alliance, an individual contributor to the Federal Reserve's Faster Payments Taskforce, and a board member of the Electronic Check Clearinghouse Organization.

11. I have been an invited speaker at dozens of industry conferences, Universities, and government agencies to share my expertise with financial services emerging technology and innovation. Specific to mobile payments, in 2010 I spoke at the Federal Reserve Board in Washington, D.C. on protecting customers in a mobile finance world and in 2011 was invited by the Center for the Study of Intelligence in Langley, VA to deliver a talk to 400 Agency analysts on "The Coming Mobile-Centric World." I was a judge for the BAI-Finacle Global Banking Innovation Awards from 2011-2014 where I judged a wide range of mobile payments innovations.

12. During my work at Bank of America, I developed intellectual property and filed more than 250 patent applications, and was subsequently named as inventor on ninety-six (96) issued United States Patents in the fields of transaction processing,

mobile commerce, communications, security, and image processing, more fully described in my C.V. attached as Appendix A For these accomplishments in intellectual property, Bank of America twice awarded me *Inventor of the Year*.

C. Materials and Other Information Considered

13. I considered information from several sources in forming my opinions. I have reviewed the documents cited in this declaration in forming my opinions.

III. UNDERSTANDING OF THE LAW

14. I am not an attorney. I have a general understanding of the applicable legal standards pertaining to the patentability issues presented in this proceeding based on my experience with patents and my discussion with counsel. I have applied the following legal principles provided to me by counsel in arriving at the opinions set forth in this declaration.

A. Legal Standard for Obviousness

15. I have been asked to consider and provide my opinions on the claims of the '171 Patent, including the technical subject matter and the application of various references that predate the filing of the '171 Patent. In particular, I have been asked to consider what one of ordinary skill in the art would have understood from the '171 Patent, whether certain references disclose or suggest the features recited in the

claims of the '171 Patent, and whether one of ordinary skill in the art would have had reason to combine certain references to arrive at the claimed subject matter.

16. My opinions concerning the application of the references to the claimed subject matter and the state of the art are provided based on what a person of ordinary skill in the art (i.e., the technical field of the invention) would have understood at the time of the alleged invention of the '171 Patent, which I have been asked to initially assume is August 30, 2011 ("the priority date").

17. In evaluating the content of the prior art references and their application to the claims of the '171 Patent, I understand that one must put himself in the position of a person of ordinary skill in the art. In my opinion, the person of ordinary skill is a hypothetical concept referring to one who thinks along the lines of conventional wisdom at the time.

18. I have been informed that subject matter claimed in a patent is obvious if a person of ordinary skill in the art at the time the alleged invention was made would have had reason (whether, for instance, commonsense, explicit statements in the references, suggestions in the references, or the state of the art at the time) to combine or modify the disclosures of one or more references to arrive at the claimed subject matter.

19. To assess obviousness, I understand that I am to consider the scope and content of the prior art, the differences between the prior art and the claim, the level

of ordinary skill in the art, and any secondary considerations to the extent they exist.

I understand that any evidence of secondary indicia of non-obviousness should be considered when evaluating whether a claimed invention would have been obvious to one of ordinary skill at the time of invention. These secondary indicia of non-obviousness may include, for example: a long felt but unmet need in the prior art that was satisfied by the claimed invention; commercial success of processes claimed by the patent; unexpected results achieved by the invention; praise of the invention by others skilled in the art; the taking of licenses under the patent by others; and deliberate copying of the invention. I understand that there must be a nexus between any such secondary indicia and the claimed invention.

20. It is also my understanding that there are additional considerations that may be used as further guidance as to when the above factors will result in a finding that a claim is obvious, including the following:

- the claimed subject matter is simply a combination of prior art elements according to known methods to yield predictable results;
- the claimed subject matter is a simple substitution of one known element for another to obtain predictable results; the claimed subject matter uses known techniques to improve similar devices or methods in the same way;
- the claimed subject matter applies a known technique to a known device or method that is ready for improvement to yield predictable results;

- the claimed subject matter would have been “obvious to try” choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- there is known work in one field of endeavor that may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to a POSA;
- there is some teaching, suggestion, or motivation in the prior art that would have led a POSA to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed subject matter.

B. Legal Standard for Claim Construction

21. I understand that “claim construction” is the process of determining a patent claim’s meaning. I also understand that, during an *inter partes* review, a claim construction analysis begins with the plain meaning of the claim term, which is the ordinary and customary meaning given to the term by those of ordinary skill in the art at the time of the invention. I also understand that the claims of a patent must be interpreted in light of the specification—that is, the claim language itself, the written description, and the figures in the patent—as well as the patent’s prosecution history.

IV. THE '171 PATENT

22. The '171 Patent relates to authorization and payment methods “using a mobile computing device in combination with a remotely hosted Secure Element representation to make payments, authorizations or exchange information with other devices.” Ex[1001] at 1:26-30. Authorization of payments involved 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.* at 1:34-38. Generation of the “cryptogram” required cryptographic keys for encryption of input message, and the '171 Patent describes, as its invention, using a non-permanent cryptographic key obtained from a remote server and stored on a mobile device to generate such cryptograms, instead of storing a permanent cryptographic key on the mobile device. *Id.*, cl. 1.

V. LEVEL OF ORDINARY SKILL IN THE ART

23. In considering a hypothetical person of ordinary skill in the art (“POSA”) of the '171 Patent at the time of the claimed invention, I considered many issues, including prior art relating to payment systems, the type of problems that such techniques gave rise to, and the rapidity with which innovations were made. I also considered sophistication of the technologies involved, and the educational background and experience of those actively working in the field. I also considered the level of education needed to understand the '171 Patent. I placed myself back in

the relevant period of time, and considered the individuals that I had worked with in the field.

24. I concluded that as of August 30, 2011, a person of ordinary skill in the art of the '171 Patent would have been a person with Bachelor's degree, in Electrical 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. A person with less education but more relevant practical experience, or more relevant education but less practical experience, may also meet this standard. I was at least a person of ordinary skill in the art at the time of the alleged invention of the '171 Patent.

VI. CLAIM CONSTRUCTION

25. For purposes of this *Inter Partes* Review, I have considered the claim language, specification, and relevant portions of the prosecution history, to determine the ordinary and customary meaning of the claim language as it would have been understood by a person of ordinary skill in the art at the time of the invention.

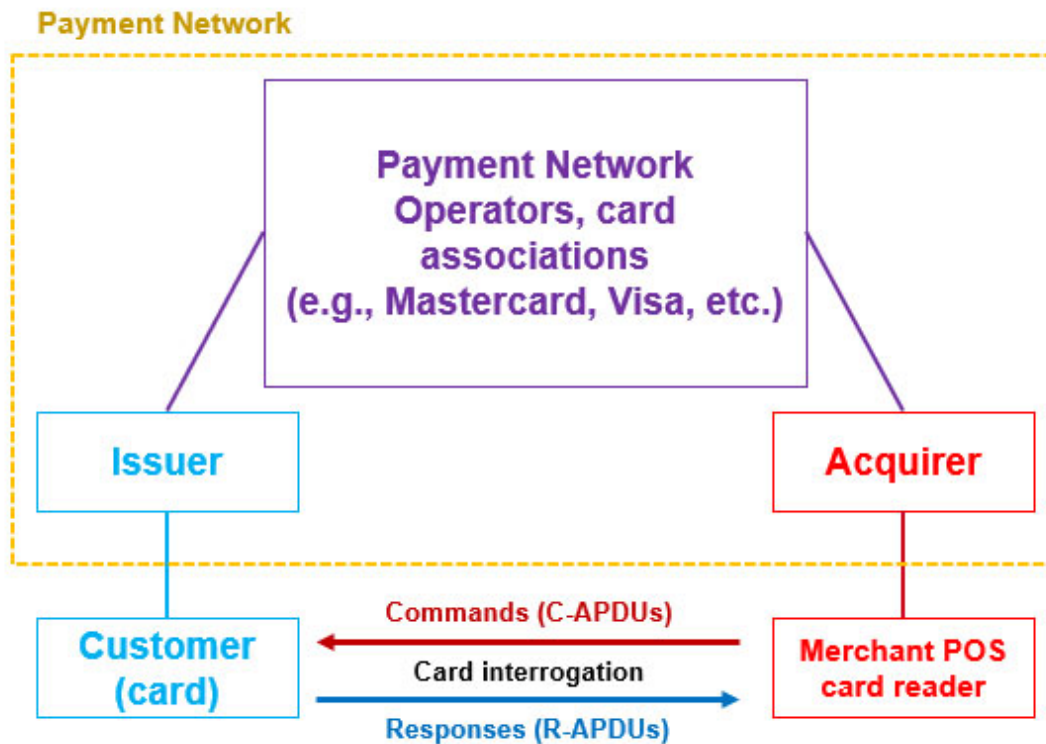
26. Claims 1 and 17 of the '171 Patent recite, among other things, "at least one response application data protocol unit containing the response cryptogram and an account identifier for the account" (hereinafter, the "**R-APDU Term**"). The term is potentially subject to at least two alternative constructions: "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**”).

VII. SUMMARY OF THE PRIOR ART

A. Technical Background on Payment Systems

27. While card payment systems have continuously evolved over the years, the basic players and their roles have been generally as follows since prior to the '171 Patent's priority date. In a typical card transaction, 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 (the “acquirer”). Ex[1037] at 18. Other players such as payment system operators like Mastercard or Visa play the role of facilitating the transaction by operating a payment interchange network. The general relationship of the players can be depicted as follows.



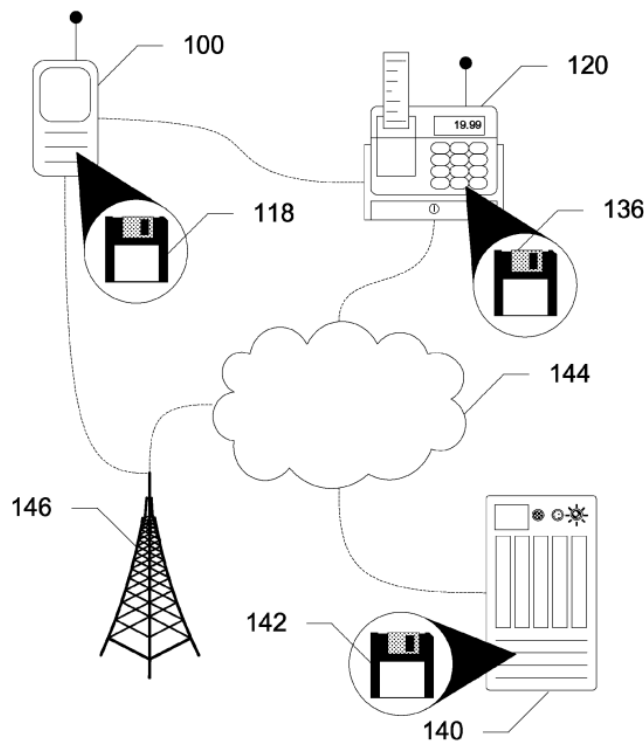
28. In a typical transaction, the merchant would use a point-of-sale (POS) terminal to read information (e.g. card number, expiration date, and authentication information) from the card or a payment mobile device. It is commonly known in the art that messages between the POS terminal and the card or payment device are application protocol data unit (APDU) messages, with those from POS terminal asking for information referred to as command APDUs (C-APDUs) and those from the card or payment device responding with information as response APDUs (R-APDUs). Ex[1037] at 46-48. 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.

29. It should be noted that it is common to refer to the payment infrastructure beyond the cardholder and card acceptor as the “payment network” or “server(s)” in general, with the understanding that these “remote” parts of the payment infrastructure consist of numerous components associated with different players, but functions as a whole to approve transactions.

B. White (Ex[1013])

30. White relates to devices, systems and methods for securing payments from a mobile communications device, including mobile device 100, POS terminal 120, and a payment server 140, all connected by network 144. Ex[1013], Abstract, 4:41-46. It is commonly understood in the art that such a remote payment server may be implemented as a collection of servers or server networks, each serving a different function, but collectively perform functions such as approving transactions and maintaining credentials.

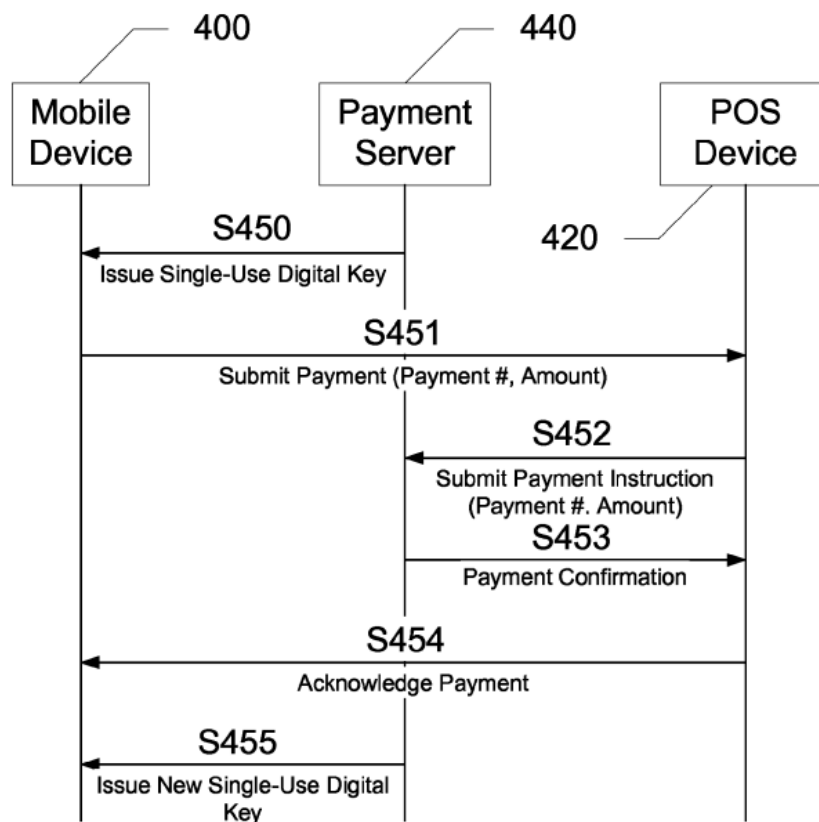


Id. Fig. 1.

31. The mobile communication device 100, such as a mobile phone or “smart phone,” *id.* 4:3-7, may communicate with a point-of-sale (POS) device 120 wirelessly, including by near-field-communication (“NFC”) technologies. *Id.* 4:55-56, 2:13-16. Mobile communication device 100 may also communicate with a remote server over network 144 through cellular tower 146. *Id.* 4:58-60. White further discloses that, for each payment transaction, the mobile communications 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 “multiplying the numbers, appending one number to the other, *mixing* the numbers,

adding the numbers, subtracting the numbers, etc.” *Id.* 4:49-55.² 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. As White has explained, “[a] one-time digital key limits a hacker to a single transaction,” thus improving security of the transaction. *Id.* 2:6-7.

32. In addition, White discloses a transaction process involving communications between a mobile device, POS device, and payment server that is highly similar to standard payment processes in the industry.



² All emphases added, unless otherwise noted.

Ex[1013], Fig. 4. The server issues a single-use digital key to the mobile device before a transaction (S450), and then after payment is completed, the server issues a new single-use digital key to the mobile device (S455). *Id.*

C. Mellqvist (Ex[1014])

33. Mellqvist discloses portable electronic devices and remote secure element servers for payment and ticketing applications, with the portable device capable of NFC transactions. Ex[1014] Abstract, [0036]. Mellqvist provides for a portable electronic device that contains a processor, memory, as well as virtual and hardware secure elements. *Id.* [0040], Fig. 2. The device also includes NFC contactless front-end to enable NFC transactions. *Id.*

34. Mellqvist further discloses that the device's virtual secure element module may communicate, over wireless network 150, with at least one 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 the virtual secure element module of the portable electronic device. *Id.*

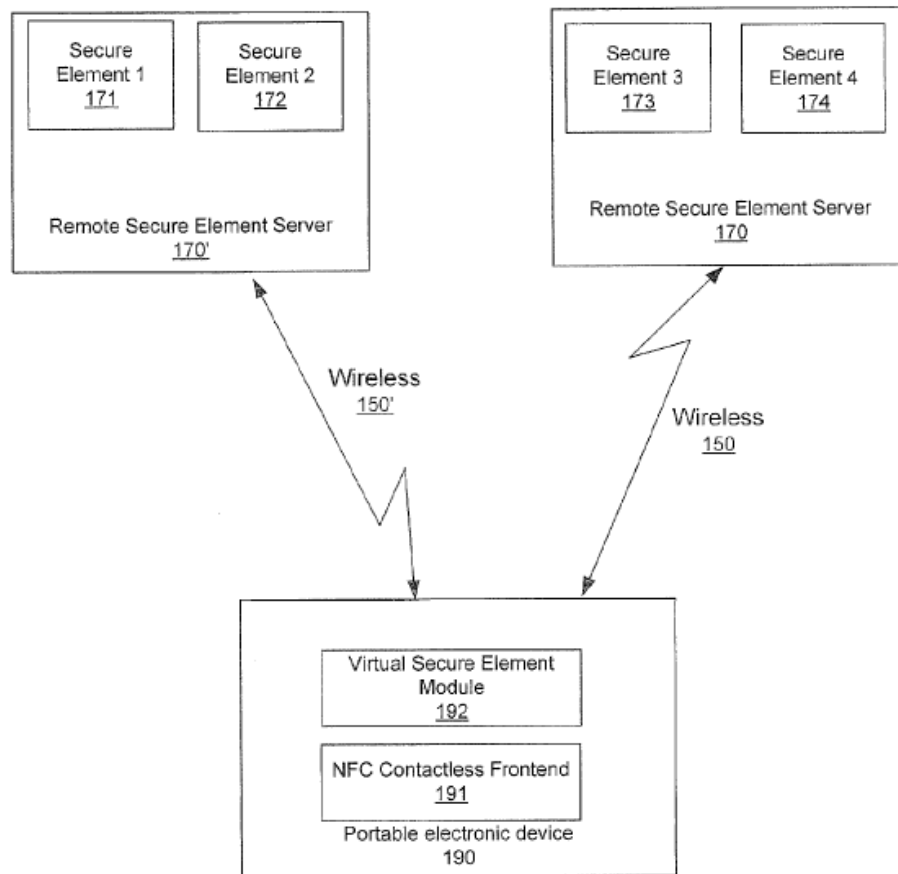


Figure 1

35. In particular, Mellqvist discloses that the system may enable NFC credit card transactions: “NFC may provide for contactless tickets and cards to be held in a portable electronic device,” and that “[o]nce an application, for example, a credit card, has been securely provisioned to the NFC enabled portable electronic device, customers can pay by simply waving their portable electronic device at a point-of-sale reader.” *Id.* [0033].

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

1. EMV Generally

36. As of the '171 Patent's priority date, traditional magnetic stripe payment cards, where a magnetic stripe stores static account information such as account number and expiration date, were being replaced by "chip cards," where a tamper-resistant microchip containing processing and memory circuitry that can store account credentials (including securely storing cryptographic keys associated with the account). Ex[1037] at 13-14, 34-47; Ex[1041] at 6. These chip cards, issued by banks and compatible with major card networks, such as Mastercard and Visa, and merchant POS terminals were designed and configured to conform to industry standards and best practices known as the EMV Specifications, which are developed and maintained by a technical body known as 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." The migration to EMV was well under way as of 2011. Ex[1041] at 6. The EMV Specifications are published and posted on EMVCo LLC's website (<https://www.emvco.com/>) free of charge, a website regularly monitored and consulted by POSAs or anyone working with payment systems.

37. Further, some of these chip cards became equipped with contactless or Near Field Communication ("NFC") communication capabilities, allowing the user to

conduct “contactless” chip card transactions by simply waving or tapping the card at the POS reader rather than inserting the card into a reader (a “contact” transaction). Ex[1040] § 2.3.3. A mobile phone may function as a payment card if it has NFC capacities and is enabled to operate its NFC controller in “card emulation” mode, i.e. the mobile device emulates a contactless NFC payment card to enable transactions with an NFC contactless POS.

38. 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. To combat fraud, EMV transactions conduct card authentication (where card issuer verifies whether the card is authentic) by having the card or mobile contactless payment device generate an “Application Cryptogram” (AC), an encrypted message that differs for each transaction because it is generated by encrypting unique information about *that* transaction with a previously stored cryptographic key. Ex[1020] §§ 8.1.1-8.1.2. In cases where the POS terminal would go online to ask the issuer to authorize the transaction, the AC is called an Authorization Request Cryptogram (“ARQC”). *Id.*; Ex[1040] § 2.1.1.1. Since the POS terminal receives only the AC but not the cryptographic keys used to generate the AC, an unauthorized person cannot re-use an AC intercepted from the POS, or replicate the card or device to give the same response AC. This drastically reduces card fraud.

39. The POS reader sends an authorization request including the transaction information and AC to the payment network. The payment network requests the issuer server to verify the AC in the authorization request by generating an AC with the same transaction data and comparing the two. The issuer knows (or can derive) the secret cryptographic keys and knows, from the authorization request, the data used to calculate the AC in the authorization request. 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] at 57-58.

40. The EMV ICC Specification (version 4.2), Exs[1019] to [1022], and Contactless Specification (version 2.1), Exs[1023] to [1029], collectively referred to herein as “EMV,” published by EMVCo, LLC (“EMVCo”), are pertinent to my analysis. They were well known, and freely accessible to professionals, engineers, and technicians in the payment industry. EMV describes in detail the transaction process, routine, as well as messages exchanged between devices in mainstream payment systems. In particular, EMV defines communications between the POS terminal and the “Card,” which can be “any consumer token supporting contactless payment transactions, whether in the form of a payment chip card, a key fob, *a mobile phone*, or another form factor.” Ex[1023] § 4.1.

41. 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, where 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] at 46-47, 48; Ex[1021] §§ 6.1-6.2.

2. Transaction Flow

42. Below, I discuss general Mastercard and Visa transaction flows.³ During the interrogation, the “Card” (user device) would provide 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. The “Card” would then first make its own decision about the transaction, and if the “Card” does not either approve (with a TC Application Cryptogram) or decline (with an AAC Application Cryptogram) the transaction locally, the POS machine will need to make an online authorization request (requesting authorization from the server); under such scenarios, the “Card” would return an ARQC Application Cryptogram to be sent to the issuer. Ex[1021] § 9.3.1; Ex[1026] § 5.3.1; Ex[1027] § 5.4.3.2.

³ Mastercard transactions kernel (Kernel 2) is defined by, inter alia, EMV Contactless Specification Book C-2, while Visa kernel (mostly Kernel 3) by Book C-3. *See* Ex[1023] §5.8.2; Exs[1026], [1027].

43. Specifically, in a Mastercard transaction, the POS Kernel reads data record(s) from the “Card” through a READ RECORD commands, Ex[1026] § 3.4.3, and the “Card” responds with a data file with the tag “70,” *id.* § 5.7.3. For Debit and Credit financial transactions, it is mandatory that the file read in response to the READ RECORD commands contains, among other things, a PAN. 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.

44. By contrast, in an EMV mode contactless Visa transaction, the POS issues a GPO command, and the “Card” may return a cryptogram as well as 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 “Card” may return an Application Cryptogram (TC, AAC, or ARQC) in the same message in response to the GPO command.⁴ Ex[1027] §§ 2.4.1, 5.4.3.2.

⁴ Specifically, in EMV mode transactions, an Application File Locator (AFL) is returned in response to the GPO message if the transaction is approved offline. Ex[1027] §2.4.1. This will cause the Kernel to issue a READ RECORD command and perform Read Application Data. *Id.* §5.3. Otherwise, the Card would provide

3. Session Key and Application Cryptogram Generation

45. The “Card” generates the Application Cryptogram (TC, AAC, or ARQC) 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, currency type, date, an Unpredictable Number for the transaction, and the value of an Application Transaction Counter (ATC), delivered to the “Card” in the form of a message (MSG). *Id.* § 8.1.1. In particular, the “Unpredictable Number,” as its name suggests, is random number supplied by the POS terminal that further ensures that the input data is unique to the transaction and not predictable before the transaction occurs. *Id.* Under EMV, Application Cryptogram is also a “Message Authentication Code” (MAC) because it authenticates the message containing the transaction information. *Id.*

46. On the other hand, the “Session Key” used for generation of the cryptogram, as its name suggests, is generated “for each transaction performed by the application” using an ICC Master Key—specifically, by “enciphering an *n*-byte ***diversification value*** with the *k*-bit ICC Master Key (MK) (essentially the master key for each “Card”) to produce a *k*-bit ICC Session Key (SK).” Ex[1020] § A1.3.1.

Track 2 Equivalent information in the same R-APDU and the Kernel proceeds to “Card Read Complete” processing. *Id.* §§5.3.2.1, 5.4.

The ICC Master Key is generated using, among other things, the account number (PAN), using an Issuer Master Key IMK, and is therefore a master key associated with the account. *Id.* § A1.4. The “diversification value” is the Application Transaction Counter (ATC) followed by padding of n minus 2 bytes of zeros. *Id.* § A1.3.1. The ATC “is a two byte (16 bit) counter that is incremented during each transaction from a nominal starting value of '0000' to a maximum of 'FFFF'.” *Id.* § D3. Hence, “[w]ith one increment per card session it gives an expected card life of 65,535 transactions” and thus “[t]he counter results in uniqueness to the cryptograms and provides tracking values for the host verification services, allowing replayed transactions and cloned cards to be identified.” *Id.* Accordingly, the “Session Key” is unique to each transaction and is thus a one-time key, because the ATC value used for creating the Session Key is incremented during each transaction.

47. Generation of the MAC or Application Cryptogram (TC, AAC, or ARQC) involves applying the Session Key to the set of input data (explained above) using “block cipher algorithm” such as Triple DES (3DES) in CBC mode, which are well known cryptographic operations, and taking the s most significant bytes (here, $s=8$). *Id.* §§ 8.1.2.2, A1.2, B1.1. The result is a fixed length (8-byte) value, which becomes the MAC. *Id.*

4. Subsequent Processing

48. The “Card” may approve the transaction locally with a “TC” Application Cryptogram or decline with an “AAC” Application Cryptogram, or, alternatively, may generate an ARQC for online authorization, Ex[1021] § 9.3.1; the POS terminal may send an online authorization request including an ARQC generated by the “Card” 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 will conduct online processing, including validation of the ARQC. Ex[1021] § 10.9. Specifically, because the issuer has both the ICC Master Key, Ex[1020] § A1.4, and the “diversification value” (consisting essentially of the ATC i.e. how many transactions a particular card has conducted), the issuer knows the same Session Key used by the “Card” to generate the ARQC. *Id.* § 10.9 n.17. Thus, issuer can verify the ARQC received in the authorization request and authenticate the card. *Id.*; Ex[1037] at 58.

VIII. GROUNDS OF INVALIDITY

A. Motivation to Combine

49. A POSA would be motivated to implement either White or Mellqvist to conduct EMV transactions by combining either reference with EMV, with the benefit of well-understood knowledge in the art about EMV transactions. Specifically, a POSA would understand both White and Mellqvist as disclosing devices, systems, and methods for conducting payment transactions using a mobile device such as a mobile phone in connection with merchant POS terminals and

payment networks consisting of servers, through communication networks. *See e.g.* Ex[1013] Fig. 1; Ex[1014] Figs. 1-2. Therefore, White's and Mellqvist's inventions cannot work on their own but must depend on compatible infrastructure for implementation. A POSA would also understand that successful implementation also requires the solution to be commercially viable and feasible.

50. Because the replacement of POS terminals globally with an alternative standard was impractical, a POSA would be motivated to bring the mobile device into compliance with existing specifications such as EMV.

51. As of the priority date of the '171 Patent, global migration from the traditional Magstripe transactions to the next-generation EMV transactions was already well underway as POS terminals worldwide were in the process of becoming EMV-compliant as of September 2010. Ex[1041] at 6. A POSA would recognize that EMV transactions offer technical and economic advantages, in particular, ability to reduce fraud with techniques such as card authentication using dynamic data, known as an ARQC cryptogram. Ex[1040] §§ 1, 1.2, 2.1.1.1, 2.3.1, 3. Additionally, a POSA would have recognized that contactless transactions offer convenience because the user can pay by simply waving a device at the POS reader. Ex[1014] [0033]. The EMV Specifications, specifically the EMV Contactless Specifications referring and incorporating the ICC Specifications, describes EMV contactless transactions with

equivalent security compared with contact chip card transactions. Ex[1040] §§ 2.1.1.1, 2.3.1.

52. Thus, a POSA would be highly motivated to implement White or Mellqvist in a way compliant with EMV to achieve compliance with payment-industry security expectations, and to improve marketability of the device 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.

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

1. Claim 1

a) [1.PRE]: “A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:”

53. 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] at 7:14-16, Fig. 6; Ex[1037] at 38-41; *see generally* Exs[1021], [1023].

b) [1.A-1] “at a mobile device, executing an application in an operating system of the mobile device,”

54. White in view of EMV discloses a “mobile device.” White discloses a “mobile communication device” 100, which a POSA would understand to contain applications including a “client payment logic” 118. Ex[1013] 4:2-8, 15-18, 41-47,

Fig. 1. A “logic” in White refers to “any information having the form of instruction signals and/or data that may be applied to affect the operation of a processor.” *Id.* 4:15-18. A POSA would have understood this to include software application executed on an operating system.

55. 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.” Ex[1023] § 4.1. 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 communications device in White. Ex[1037] at 38-41. In particular, EMV is directed to financial “applications” on “Cards,” which may be plastic chip cards or mobile devices with an NFC controller operating in card emulation mode. Ex[1013] at 2:14-17. For example, initiation of a transaction always involves selecting a particular application by its Application Identifier (AID) on a “Card,” and the application contains a set of information and instructions. Specifically, a

“card application” runs on the native operating system of the “Card,”⁵ and the POS terminal’s application “sends commands as a client to the card application, which responds as a server.” Ex[1037] at 40, 47-48. For example, in a Mastercard transaction, the POS will select a Mastercard application on a “Card,” and for a Visa transaction, a Visa application, Ex[1023] § 5.8.2; Ex[1026] § 2.3.3-2.3.4 (“The Kernel that is activated depends on the information returned by Process S,” which, upon activation, “returns the selected application and Kernel.”); Ex[1027] § 2.4.1 (“only a successful SELECT AID response ... will be passed to Kernel 3,” and “Kernel 3 processing for a transaction starts with sending a GET PROCESSING OPTIONS (GPO) command to the card”). Accordingly, this claim element is disclosed or rendered obvious by White alone or further in view of EMV.

c) [1.A-2]

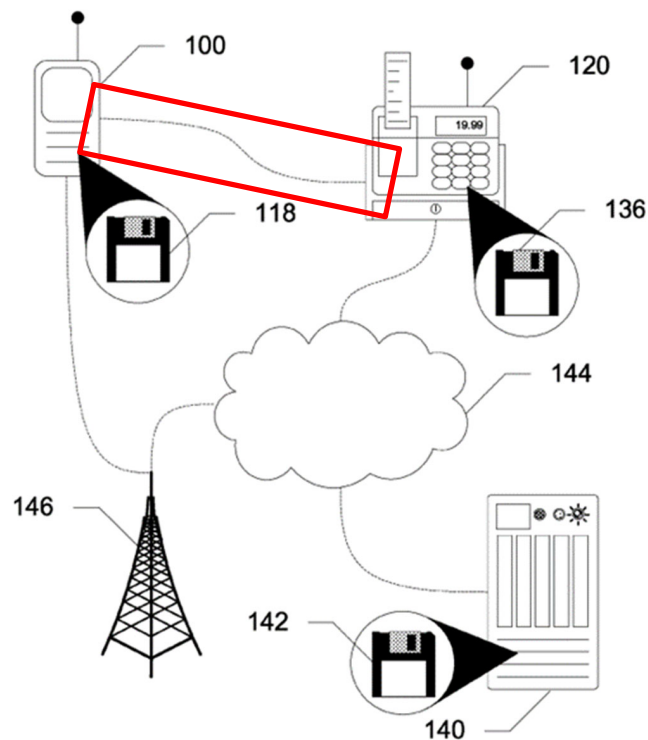
(1) [1.A-2a] “the application interrogable by an electronic reader, over a first communications channel,”

56. The ’171 Patent suggests that interrogation refers to querying or extraction of information. *E.g.* Ex[1001], 6:3-5 (“the interrogator...extracts information from the

⁵ It is possible to run the same or equivalent application on a mobile device processor because such applications require only basic arithmetic operations that a mobile device processor is perfectly capable of handling.

card”), 6:50-53 (“‘Commands’ are sometimes referred to as ‘queries’ because they originate from an ‘interrogator,’ which has a querying connotation.”), a well-understood process in the art, Ex[1015], [0062], [0070].

57. White discloses that the mobile communications 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 device 120 or may communicate in a wired fashion,” and point-of-sale device 120 may also communicate with mobile communications device 100 with information such as a sales amount “directly.” Ex[1013], 4:55-57, 5:2-4. Such communications may occur over the communication channel between the mobile communications device 100 and point-of-sale device 120, which is a “first communications channel” (shown below in red) separate from other communication channel(s), such as the network 144.



Ex[1013] Fig. 1. This is known in the art as “interrogation,” *e.g.*, Ex[1015], [0062], [0070].

58. Moreover, when implemented in compliance with EMV, the device application would be interrogable by the POS. Ex[1026] § 3.5.3; Ex[1027] §§ 2.4.1, 5.2.2.3, 5.4.3.2; Ex[1023] §§ 4.1-4.3, 10.1-10.2.

(2) [1.A-2b] “for digital credential data corresponding to an account”

59. The '171 Patent states that “[t]he term ‘digital credential data’ as used herein refers to at least a portion of all data, including any data that are required to calculate the data, that are necessary to authorize approval of a transaction at a POS terminal.”

Ex[1001], 7:3-7.

60. 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.” *Id.* 5:4-6, 10-12. Server 140 then authorizes the transaction after verifying the payment number. *Id.* 5:16-26 (“If the numbers or codes match, payment server 140 deducts the amount from an account associated with mobile communications device 100.”). Thus, the payment number is “digital credential data corresponding to an account having a corresponding digital credential” 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), for the reason that, such information is typically used to determine from which or whose account the transaction amount should be deducted.

61. EMV similarly discloses an application interrogable by a reader over a communication channel. As discussed above for [1.A-1], 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] at 40, 47-48; Ex[1023] § 5.8.2; Ex[1026] § 2.3.3-2.3.4; Ex[1027] § 2.4.1. 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. Specifically, as explained above, in a Mastercard transaction, the “Card” returns account information including a PAN in response to a READ RECORD command, Ex[1026] §§ 3.4.3, 5.7.3, Ex[1021] Part III, § 7.2, and returns an Application Cryptogram in response to a GENERATE AC command, Ex[1021] § 9.3.1; Ex[1026] § 5.3.1. In an EMV mode Visa transaction, the “Card” may return an Application Cryptogram as well as Track 2 Equivalent Data (account information) in response to a GPO command. Ex[1027] §§ 2.4.1, 5.4.3.2. Both the account information and the Application Cryptogram are data necessary for approval of a transaction. Ex[1037] at 57-58.

62. Accordingly, because a POSA would have been motivated to implement White in a manner capable of carrying out mainstream payment card transactions, the POSA would understand the mobile communications 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. A POSA would therefore have made White’s mobile communications 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. Therefore, White discloses this element or renders it obvious alone or further in view of EMV.

(3) [1.A-2c] [said account] “having a corresponding digital credential,”

63. 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), where the data in the database are elements of data that are typically stored in an SE memory” *Id.* 9:44-58. '171 Patent further explains that “Track Data” refers to “Track1/Track2 data” which is extracted from POS reader during interrogation for authorization, *id.* 8:47-49, 9:6-8, and HSM would generate “credential data,” *id.* 23:30-33. The next claim element [1.A-3] recites this credential is hosted on a remote computer.

64. 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. As discussed above for [1.A-2b], White and EMV

disclose using digital credential data from the server for approval of a transaction for an account, and thus imply or render it obvious that the account must have a “corresponding digital credential” such as on a remote server, to perform authentication and approval of the requested payment transaction. Accordingly, White discloses, or renders obvious further in view of EMV, this element.

d) [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”

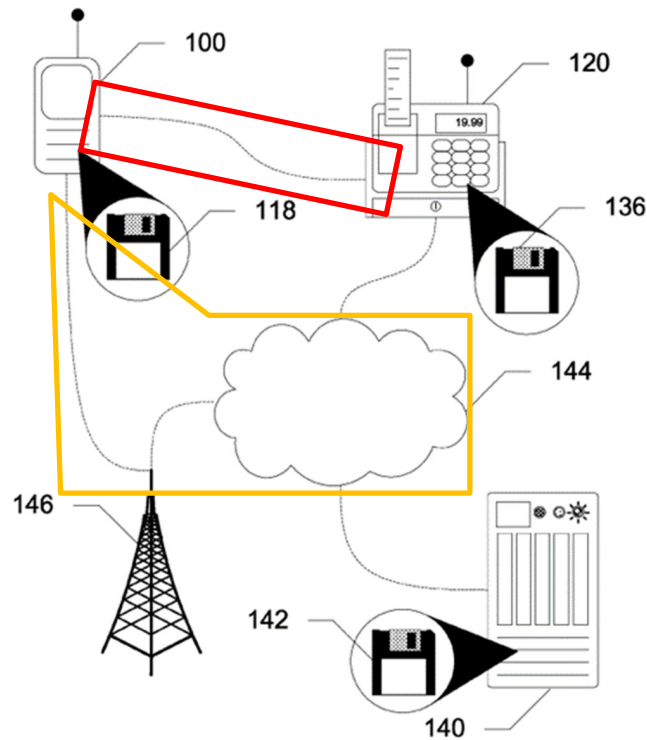
65. White discloses payment server 140, Ex[1013] Fig. 1, which is “a remote computer system” because it is accessed through a network 144. *Id.* 4:53-55. It is commonly understood in the art that such a remote payment server may be implemented as a collection of servers or server networks, each serving a different function, but collectively perform functions such as approving transactions and maintaining credentials. A POSA would understand payment server 140 as “hosting the corresponding digital credential” (which refers to digital credential of an account), because payment server 140 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], 4:53-55, 5:23-26, and thus must necessarily host “digital credential,” as explained for [1.A-2c], which contains data “necessary to authorize approval of a transaction at a POS terminal,” including “any data that

are required to calculate the data” Ex[1001], 7:3-7, like the one-time digital key in White. It was well known in the art that, in an EMV transaction, data necessary to authorize approval include both account information and authentication data (such as an ARQC cryptogram and data necessary to authenticate that cryptogram). Ex[1037] at 57-58.

66. White further discloses that “[m]obile communications device 100 receives the one-time digital key from payment server 140 [i.e. “a remote computer system hosting the corresponding digital credential”] 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. 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, Ex[1020] §§ A1.3.1, A1.4; and thus directly corresponds with White’s described one-time key.

67. White also discloses that “[m]obile communications device 100 may ... communicate wirelessly with payment server 140 over network 144 through cellular tower 146,” *id.* 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.



68. 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 communications device may be configured to receive the one-time digital key from payment server after making a *request* to the server. This is because a POSA would have understood it would be an efficient use of computation and communication resources for the server to initiate delivery of data (such as the one-time digital key) to the mobile device in response to a request for it, rather than

providing such data without regard to whether the mobile device needs the data or is powered and connected to the network such that it can receive the data.

69. A POSA in 2011 would further recognize that it would be a frequent occurrence that a mobile device would be out of communication range of a cellular network, such as when in large buildings, or when underground, including in public transit environments. Ex[1044] ¶¶ 4.41-4.43. Therefore, White discloses or renders obvious this claim element.

70. Further, a POSA implementing White in accordance with EMV would have been motivated to implement White's "one-time digital key from payment server" as an EMV "Session Key" from the payment server 140. A POSA would have recognized that the EMV Session Key, which 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, Ex[1020] § A1.3.1, and thus directly corresponds with White's described one-time key, and that using the EMV Session key for that purpose would be the most straight-forward way to make White's techniques compatible with EMV.

e) [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"

71. White discloses a “payment number,” which is a cryptogram. Specifically, White discloses that, 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 “multiplying the numbers, appending one number to the other, *mixing* the numbers, adding the numbers, subtracting the numbers, etc.” *Id.* 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.

72. 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 or consider it obvious that, by referring to a “mixing” operation, White discloses performing an encryption operation with the one-time digital key to generate the “payment number.”⁶ Ex[1035] at 11; Ex[1036] at 9; Ex[1038] at 7-8; Ex[1043] at 3. Thus, the resulting “payment number” is encrypted data or message,

⁶ This distinguishes “mixing” from other operations, such as addition, multiplication, subtraction, and concatenation (appending), that were also described in White. Ex[1013] 4:49-53.

or a “cryptogram.”⁷ Indeed, the ’171 Patent itself refers to a “**number** sequence” so calculated as a “cryptogram.” Ex[1001], 7:42-43.

73. Further, White’s “one-time digital key,” as explained above 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.”

74. In addition, because the cryptogram (“payment number”) may be communicated to the POS terminal, which will communicate the cryptogram to the payment server, the cryptogram is information extracted by POS terminal from the

⁷ 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.

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

75. Further, a POSA motivated to implement White to conduct EMV transactions would have found it obvious and straightforward to implement White’s “payment number” as an Application Cryptogram generated with a Session Key. Specifically, an EMV-compliant terminal requests and obtains an Application Cryptogram (such as an ARQC) 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 Application Cryptogram is generated using the Session Key (described above). Ex[1020] §§ 8.1.1, A1.2-1.3 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. *Id.* Thus, the “Card” or mobile communications device does not access a permanent cryptographic key for generation of cryptogram requested during interrogation but accesses only a temporary Session Key.

76. Accordingly, a POSA would have recognized that a straightforward way to make White’s technique compatible with EMV 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 such as an ARQC. 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.

f) [1.B]: “requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;”

77. 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] “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;”

78. As explained in connection with [1.A-3], White discloses that the application of the mobile communications 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 that the “one-time digital key” is a cryptographic key for generation of a cryptogram using well-known encryption methods such as 3DES. 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.

79. In addition, a POSA implementing White to carry out EMV transactions would understand that a Session Key, which is unique to each transaction and is a non-permanent cryptographic key, is to be used as the “one-time digital key” in this context as data associated with the account. As explained for [1.A-4], the mobile communications device application in White 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 APDUs (R-APDU), and the AC would be passed back to POS terminal in a R-APDU. Ex[1037] at 46-47, 48; Ex[1021] §§ 6.1-6.2, 6.5.5. Therefore, a POSA implementing White to carry out EMV transactions would arrive at this claim element by receiving a Session Key from the payment server and use the Session Key to generate an AC returned in a R-APDU during interrogation.

h) [1.D]: “locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;”

80. White discloses that “[t]he one-time digital key is stored on mobile communications device ... until it is used ... [or] replaced by a new one-time digital key.” Ex[1013] 6:25-28. As explained above in connection with [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. Accordingly, the one-time digital key or Session Key is a locally stored local cryptographic key, and White discloses this claim element.

i) [1.E]: “participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:”

81. As explained in connection with [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 further below. It was well known in the art and disclosed in EMV that, during the interrogation, commands issued by the terminal and responses from the “Card” are communicated in command- and response-application protocol data units (C-APDUs and R-APDUs), respectively. Ex[1037] at 46-47, 48; Ex[1021] §§ 6.1, 6.2.

(1) [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;”

82. 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. *Id.* Specifically, because the “Card” returns an Application Cryptogram (e.g. an ARQC) in response to a GENERATE AC command in Mastercard transactions or to a GPO command in these Visa transactions, *id.*, the GENERATE AC or GPO commands are each a “cryptogram request”.

83. As explained above for [1.A-2], White discloses a mobile communications device with application interrogable by a POS terminal over a first communications channel for digital credential data used to authorize transaction against an account. Accordingly, a POSA implementing White to carry out EMV transactions would have found it obvious to program the mobile communications 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, including responding with a cryptogram used to authorize the transaction, thereby satisfying this claim element.

(2) [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”

84. 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 (recommending a minimum set of data elements for AC generation); 8.1.2 (prescribing 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].

85. 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] at 11; Ex[1036] at 9; Ex[1038] at 7-8. As a result of such “mixing,” the resulting response AC does not include the cryptographic key but only the encrypted text or cryptogram. Specifically, EMV specifies that an AC may be generated using 3DES

(Triple DES) algorithm with a 128-bit Session Key.⁸ Ex[1020] §§ 8.1.2, A1.2, A1.3.1 (“Triple DES with $k=128[-\text{bit key}]$ ”), B1.1. This is because 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.⁹ Hence, a POSA implementing White (specifically, generation of a “payment number” using a one-time digital key) to carry out EMV transactions would have found it obvious to configure the mobile application (“Card”) to generate, using a Session Key, an AC such as an ARQC to be included in a response APDU message, where the AC does not include the Session Key.

(3) [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

⁸ Because 3DES requires two keys, the Session Key is divided into two keys when used. Ex[1021] §B1.1.

⁹ It is common knowledge in cryptography that the ciphertext does not include the key. For example, as demonstrated step-by-step in the review article by Rabah, for hexadecimal text “0123456789ABCDEF”, the resulting ciphertext (cryptogram) of DES encryption using key “133457799BBCDFF1” is “85E813540F0AB405” which does not include the cryptographic key “133457799BBCDFF1”; triple DES scrambles the ciphertext further. Ex[1037].

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;”

86. A POSA implementing White to carry out EMV transactions would have found it obvious to configure mobile communications 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] at 46-47, 48; Ex[1021] §§ 6.1-6.2.

87. As explained above, the R-APDU Term here (underlined above) is potentially subject to two alternative constructions. *Supra* Part VI. 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] § 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 APDU to the GPO command containing both "Track 2 Equivalent" data (which includes *inter alia* a primary account number (PAN), hence the "account identifier")¹⁰ and an AC. Ex[1027] §§ 2.4.1, 5.4.3.2.

88. 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. 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 further in view of EMV render this element obvious.

j) [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;"

89. 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

¹⁰ 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.

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.”

90. Also as explained above with [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 for carrying out EMV transactions. Specifically, the mobile device would communicate with the server to indicate its availability and its need to receive data, such that the server delivers such data, e.g. in issuing a new one-time digital key, upon receiving such a request from the mobile device, in order to avoid wasting computation and communication resources.

k) [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”

91. As explained previously, 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.

l) [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.”

92. White explicitly discloses that each “one-time digital key is stored on mobile communications 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. As explained above, the one-time digital key is a local, non-permanent cryptographic key.

2. Claim 17

a) [17.PRE]: “A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

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

b) [17.A] a mobile device comprising:

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

c) [17.B]: “a controller configured to route communications received over a communication channel from an electronic reader;”

95. For the reasons discussed for [1.A-1], White discloses a mobile communications 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 made it obvious to a POSA that the mobile communications device includes a controller configured to route the communications received from a POS device.

d) [17.C]: “a wireless interface to connect to a wireless network that is separate from the communications channel;”

96. 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 and implies or makes it obvious to a POSA that the device includes a wireless interface.

e) [17.D]: “a processor;”

97. 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] at 38-41.

f) [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:”

98. White discloses that the mobile communications 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 communications 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 to 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] at 38-41. Accordingly, White discloses or renders this element obvious.

(1) [17.E-1]: “request from the remote computer system, over the wireless network, a first set of data associated with the account;”

99. For reasons discussed for [1.B], White discloses or renders obvious this claim element.

(2) [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;”

100. For the reasons discussed for [1.C], White discloses this limitation.

(3) [17.E-3]: “store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;”

101. For the reasons discussed for [1.D], White discloses this limitation.

(4) [17.E-4]: “during an interrogation:”

102. For the reasons discussed for [1.E], White discloses this limitation.

(a) [17E-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;”

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

(b) [17.E-4b]: “access the local cryptographic key associated with the account;”

104. For the reasons 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]: “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”

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

(d) [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;”

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

g) [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;”

107. For the reasons discussed for [1.F], White discloses this limitation.

h) [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”

108. For the reasons discussed for [1.G], White discloses this limitation.

i) [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.”

109. For the reasons discussed for [1.H], White discloses this limitation.

3. Claims 2 and 18: “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”; “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.”

110. 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.¹¹ Ex[1013] 2:14-17.¹² It would

¹¹ 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.

¹² Even though White refers to NFC communications as a way by which a customer can “conduct a transaction outside of network coverage,” Ex[1013] 2:13-

also have been obvious to a POSA to carry out EMV contactless transactions with NFC. Ex[1040] § 2.3.3. 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: “wherein the response cryptogram is a hash”

111. For reasons discussed for [1.A-4] and [1.E-2], the “payment number” in White, if 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.

17, a POSA would not have understood the disclosure to be limiting, because White also describes more generally that “[m]obile communications device 100 may communicate wirelessly with point-of-sale device 120 ...,” *id.* 4:55-57, and a POSA implementing White to conduct EMV transactions would have understood that the mobile device in White simply has the capacity to operate as an NFC emulating device.

112. 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) encrypt 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. Thus, White, further in view of EMV, discloses or renders obvious this element.

5. Claims 4 and 20: “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”

113. For reasons discussed above, 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: “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”

114. As discussed above, a POSA would have found it obvious and been motivated to implement White to carry out transactions in accordance with EMV. It is not clear to a POSA what this claim element means by reciting responding to a request for a first cryptogram with a second cryptogram. 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, 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.*

115. On the other hand, to the extent the 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 (GENERATE 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.

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

7. Claims 6 and 22: “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”

117. As explained above, EMV provides that an Application Cryptogram (response cryptogram) is generated by encrypting the input data with 3DES algorithm (DES algorithm executed three times), Ex[1043] at 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, further in view of EMV.

8. Claims 7 and 23: “wherein the mobile device does not have connectivity to the wireless network during the interrogation”

118. 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. Accordingly, White discloses and renders obvious this element.

9. Claim 8

a) [8.PRE]: “further comprising, at the remote computer system:”

119. For the reasons discussed for [1.A-3], White discloses a remote computer system.

b) [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”

120. For the reasons discussed for [1.A-3], [1.B]-[1.C], White discloses or renders obvious that the mobile communications 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.

121. Further, White discloses that the one-time digital key is used to generate a payment number for approval of transactions against a certain account, 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 is therefore also 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 which account the transaction is associated with.

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

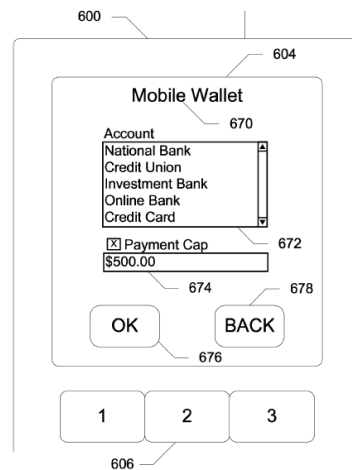


Figure 6

123. 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.

c) [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.”

124. For the reasons discussed for [1.A-3], [1.F], and [1.G], White discloses or renders obvious that the mobile communications 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.

10. Claims 9 and 26: “wherein the digital credential comprises a secure element representation maintained at the remote computer system”; “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”

125. 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.

11. Claims 10 and 27

a) [10.PRE]/[27.PRE]: “The method of claim 1, further comprising, at the remote computer system, performing an authorization process comprising:” / “further comprising, a remote computer system programmed to:”

126. 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 (“If the numbers or codes match, payment server ...sends a confirmation to point-of-sale device 120.”). EMV further specifies that online authorization is performed by, inter alia, verification of ARQC, an Application Cryptogram, by a remote computer. Ex[1021] § 10.9.

b) [10.A]/[27.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;”

127. 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.

128. 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. Specifically, it was well understood in the art that an authorization request in EMV transactions would include, inter alia, the ARQC, account identification data (including PAN), and an unpredictable number. Ex[1037] at 57-58. Accordingly, White, alone or further in view of EMV, discloses or renders obvious this element.

c) [10.B]/[27.B]: “determining a current non-permanent cryptographic key associated with the account using the account identifier;”

129. 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, as explained above, the authorization request received by the server contains an account identifier such as a

PAN. 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]: “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”

130. 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 as explained for [1.A-4]. Also as explained for [1.A-4], 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 in White.

131. To do so, 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 (“The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby

authenticate the card.”); Ex[1037] at 58 (server would: “Derive the actual session key SSK_{AC} ...”; “Use SSK_{AC} to produce a MAC on the same data objects that were considered by the card in the transaction claim”; and “Compare the computed MAC against the ARQC received in the authorization request message ...”).

132. In terms of 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] at 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. 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 (referring to the problem of fraudulent transaction from a “hacked device”). 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, that is, the server uses a secret—a one-time key—that is known to both the server and an authentic device to verify whether the input data and cryptogram correspond to each other given that key.

133. 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. Further, because the ARQC under EMV is a "hash"—that is, encrypted data that cannot be decrypted, a POSA seeking to use White's device for EMV transaction would have no other choice but to use encryption, rather than decryption, to verify the cryptogram. Therefore, a POSA would have found it obvious to make this modification of White to comply with EMV, rendering this element obvious.

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

134. 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 ("If the numbers or codes match, payment server 140 deducts the amount from an account associated with mobile communications device 100, and sends a confirmation to point-of-sale device 120."). 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] at 59.

12. Claims 11 and 28: “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”

135. These claims are dependent on Claim 10 and 27, which further depend on Claims 1 and 17. The first element here, “set of inputs,” is originally found in Claims 1 and 17, which recites generating “a response cryptogram based on a set of inputs and the local cryptographic key associated with the account.” 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. Further, EMV explicitly requires that input data for generation of the response cryptogram to include an “Unpredictable Number,” which is 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.

136. 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] at 57. 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 communications 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.

137. 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 as input data for ARQC cryptogram generation and also in the authorization request so that the server may compute the same cryptogram; it is easier for the server to simply use that random or unpredictable number in the authorization request to generate an ARQC. EMV terminals are already configured to generate unpredictable numbers during a transaction and send them to the card and to the issuer in the authorization request message. Ex[1020] § 8.1.1; Ex[1037] 218.

138. Further, as explained above for [10.C]/[27.C], in an EMV transaction, the server calculates the same response cryptogram using the same key and the same input data to verify the cryptogram in the authorization request (ARQC).

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

13. Claims 12 and 29: “wherein the POS command communications comprise the unpredictable data”

140. The “POS command communication[]” appears to refer back to 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, 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] at 48. 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 to generate the response cryptogram. Accordingly, White, further in view of EMV, renders this element obvious.

14. Claims 13 and 30: “wherein the authorization data further comprises values from the transaction”

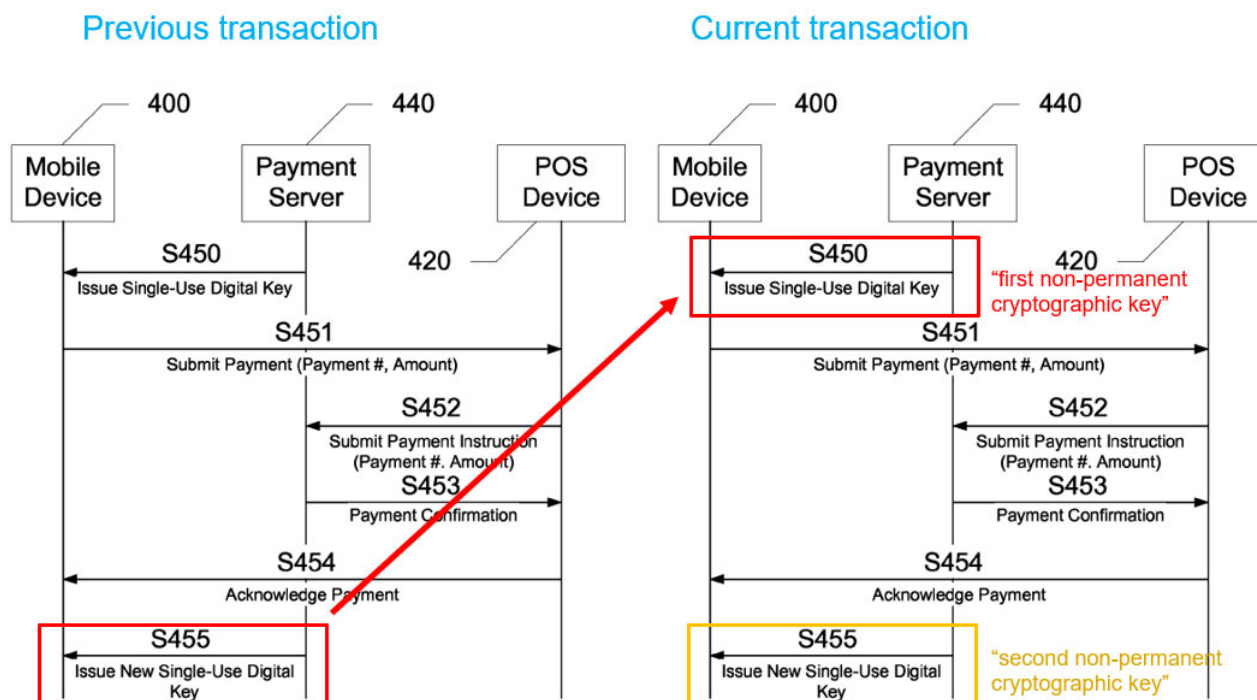
141. White explicitly discloses that the authorization request received by payment server includes “the amount” for a sale of goods, which is a “value from the transaction.” Ex[1013] at 4:61-63, 5:2-4, 8-12. Further, it was understood in the art that, in an EMV transaction, the authorization request would include values from the transaction including “[a]ll the data objects necessary to reproduce the transaction claim,” Ex[1037] at 58, which usually include information such as amount and

currency code. Accordingly, White alone or further in view of EMV discloses or renders obvious these claims.

15. Claims 14 and 31: “wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process”

142. 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] at 6:40-42. Accordingly, the “second non-permanent cryptographic key” is shared by a remote payment authorization process.

143. Further, it would have 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).



Accordingly, White discloses or renders obvious these claims.

16. Claims 15 and 32: “wherein the application is [configured/executable] to generate the response cryptogram according to a card specification”

144. For reasons stated above, a POSA would have found it obvious and be positively motivated to implement White to carry out mainstream payment card transactions, in particular 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 further in view of EMV renders these claims obvious.

17. Claims 16 and 33: “wherein the first and second non-permanent cryptographic key are associated with an issuer master key”

145. 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.

146. As further explained in above, 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 further in view of EMV renders these claims obvious.

18. Claim 24: “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation”

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

19. Claim 25: “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”

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

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

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

1. Obviousness Over *Mellqvist* in General

150. *Mellqvist* discloses an NFC-enabled portable electronic device, with secure element hosted on remote servers, 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. 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.

151. Specifically, *Mellqvist* discloses secure elements hosted in remote servers and storing payment applications. *Id.* [0036]. As explained above in [1.A-1] and [1.A-2] of Ground 1, it was well understood in the art that payment applications would respond to POS commands with digital credential data necessary to authorize payment transactions.

152. It was also well understood that data necessary for such authorization are data provided by either the "Card" or the POS terminal during the interrogation, including

both card information, transaction information such as amounts, and the Application Cryptogram (ARQC). Ex[1027] § B.1.1; Ex[1037] at 57-58. All of these necessary data (“[a]lways” included) as listed in EMV (Ex[1027] § B.1.1) can be categorized into three categories:

- (a) Data to be provided by the Terminal. This includes transaction Amount, Terminal Country Code, Terminal Entry Capability, Terminal Verification Results (TVR), Transaction 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 Application Interchange

Profile (AIP),¹³ Application Transaction Counter (ATC), Issuer Application Data (IAD),¹⁴ and Track 2 Equivalent Data.¹⁵

- (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.

153. Because the portable electronic device of Mellqvist is a user device equivalent to the “Card,” Ex[1014] [0033], not a merchant device such as a POS terminal, a POSA would understand the secure elements in Mellqvist as providing data to be provided by “Card,” that is, categories (b) and (c) above.

¹³ AIP “[i]ndicates the capabilities of the card to support specific functions in the application.” Ex[1027] § A.2 at 96.

¹⁴ IAD “[c]ontains proprietary application data for transmission to the Issuer in an online transaction” and may include “key indicator and algorithm version number” for cryptographic calculations. Ex[1027] § A.2 at 111; Ex[1037] at 58.

¹⁵ As explained above, this includes basic card information such as PAN and expiration date. Ex[1027] § A.2 at 124.

154. 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). In other words, the user device merely relays interrogation messages between the remote secure element and the POS terminal. However, because there are multiple messages being exchanged during interrogation in an EMV transaction—for example, select AID, GET PROCESSING OPTIONS, READ RECORD, GENERATE AC, 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 when carried out over cellular wireless network, which was a well-known problem in the art as of the priority date of the '171 Patent. Ex[1017] 48:30-35.

155. 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]. Further, this solution would obviously require that the user have wireless network connection (e.g. cellular coverage) throughout the interrogation, which is not guaranteed, and was particularly a problem in in-door environment as of the priority date of the '171 Patent, as was well known in the art, such as when performing a payment transaction in an underground environment, such as at a public transit facility. *See also* Ex[1044] ¶¶ 4.41-43.

156. A second solution would utilize the optional hardware secure element or memory of the portable electronic device and store information in category (b) in advance. Because information in this category is knowable in advance, they may be provisioned to the device at any time. The remote secure elements will be responsible for generating AC (category (c)). 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.

157. The final solution, then, would be to use processor or hardware secure element of the portable electronic device to generate the AC, with only minimal information requested from the remotely hosted SE. A POSA would have understood that the device has such capacity, with its hardware secure element or processor, both of which have arithmetic computation capabilities. The device also needs the Session Key to compute an AC.

158. The Session Key is generated by encrypting essentially the ATC, whose value is known before a transaction, with an ICC Master Key, which does not change with each transaction. Ex[1020] § A1.3.1. Thus, the Session Key is also information knowable before a transaction. Hence, 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.

159. This is also consistent with Mellqvist’s disclosure that the remotely hosted secure elements are to provide a “predetermined level of security” for transactions so as to eliminate the need to maintain such level of security at the mobile device. Ex[1014], [0004], [0035]. A POSA would have understood a “predetermined level of security” to be the level of security in a microchip of a chip credit card or conventional secure element. 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. Because the ICC Master Key is unique to the ICC (integrated circuit card) and is usually kept in the memory of a tamper-resistant device, such as a hardware secure element or microchip in a chip card, Ex[1037] at 65-66, this would require maintaining the “predetermined level of security” in the mobile device and would be contrary to Mellqvist’s teaching.

160. 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. Moreover, a POSA would recognize this to be the lowest risk data to maintain on the mobile device, as the Session Key is useful for only a single transaction, and therefore an attacker obtaining access to the Session Key could perform at most a single transaction—limiting fraud exposure compared to storing the ICC Master Key on the mobile device.

161. 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.

2. Claim 1

a) [1.PRE]: “A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:”

162. To the extent the preamble is limiting, both Mellqvist and EMV disclose such a method. Both disclose a “mobile device.” Ex[1014] [0046] (“portable electronic device”), Fig. 2.; Ex[1023] § 4.1. Both disclose a “secure application” for “payment card transaction.” *E.g.* Ex[1014] [0046] (“at least one hardware secure element 252 configured to provide a *secure execution environment for secure transactions*”); Ex[1037] at 38-41; *see generally* Exs[1021], [1023].

b) [1.A-1] “at a mobile device, executing an application in an operating system of the mobile device,”

163. Both Mellqvist and EMV disclose such a “mobile device.” Mellqvist discloses a “portable electronic device,” which includes a processor which may be, among other things, a “cellular radio telephone,” including a “processor.” Ex[1014] [0033]-

[0034], [0040]. A POSA would understand that an obvious way to operate a processor to is to execute an application on an operating system of the mobile device.

164. 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, which may be the processor and memory of the device in Mellqvist. Ex[1037] at 38-41. 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 an native operating system of a card and it is possible to run the same or equivalent application in a mobile device processor because such applications require only basic arithmetic operations that a mobile phone processor is perfectly capable of handling. Accordingly, this claim element is disclosed or rendered obvious by Mellqvist alone or further in view of EMV.

c) [1.A-2]

(1) [1.A-2a] “the application interrogable by an electronic reader, over a first communications channel,”

165. 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 electronic device can use NFC for short-range communications and user “can pay by simply waving their portable electronic device at a point-of-sale reader.”

Ex[1014], [0033], [0035]. A POSA would understand this as disclosing an application “interrogable by an electronic reader, over a first communications channel.” *See also* Ex[1015], [0062], [0070].

(2) [1.A-2b] [the application interrogable] “for digital credential data corresponding to an account”

166. 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 and users “waving their portable electronic device at a point-of-sale reader” to pay, 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.

(3) [1.A-2c] [said account] “having a corresponding digital credential,”

167. 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 cell phone, or other mobile devices that may be *used for making payments.*” *Id.* 1:35-38. Further, a “secure element representation” may be actual SE hardware, virtual hardware secure elements, or data hosted on a server. *Id.* 9:44-58. 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] “...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”

168. Mellqvist discloses that “the portable electronic device 190 in the system 100 is configured to establish a wireless connection ... between one or more remote secure element 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, as explained above for [1.A-3] of Ground 1, a POSA implementing Mellqvist to conduct “credit card” payment transactions, *id.* [0033], would have found it obvious to configure application of portable electronic device 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. This element is therefore obvious over Mellqvist further in view of EMV.

e) [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”

169. Under EMV, the Session Key is data associated with the account because it is derived from an ICC Master Key generated from the account number 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, under EMV, the “Card” generates and returns an AC at the request of terminal commands GENERATE AC or GPO during the interrogation.

170. As further explained above, a POSA implementing Mellqvist to conduct “credit card” payment transactions, *id.* [0033], would have found it obvious to configure application of portable electronic device to request only a Session Key from the secure elements hosted on the remote server and generate an Application Cryptogram (AC) with that key, thereby rendering this element obvious.

f) [1.B]: “requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;”

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

g) [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;”

172. It was well known in the art and required by EMV that responses from the “Card” (or portable electronic 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] at 46-47, 48; Ex[1021] §§ 6.1-6.2, 6.5.5. Accordingly, for the same reason as explained for [1.A-3] and [1.A-4], this element is obvious over Mellqvist further in view of EMV.

h) [1.D]: “locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;”

173. As explained above, a POSA would have found it obvious to configure Mellqvist’s portable electronic device to request a Session Key before a transaction, because the device is not guaranteed to have network connectivity during a transaction. Thus, it is obvious that the Session Key must be stored on the device until used in a transaction.

i) [1.E]: “participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:”

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

(1) [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;”

175. For the same reason stated for [1.E-1] in Ground 1, EMV prescribes this element. Therefore, this element is obvious over Mellqvist further in view of EMV.

(2) [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”

176. For the same reason stated in [1.E-2] in Ground 1, EMV prescribes this element, where the Application Cryptogram is a response cryptogram that does not include the Session Key, which is the local cryptographic key as explained in [1.D] of this Ground. Therefore, this element is obvious over Mellqvist further in view of EMV.

(3) [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;”

177. For the same reason stated for [1.E-3] in Ground 1, EMV prescribes this element, under either construction for the R-APDU Term of the claim. Therefore, this element is obvious over Mellqvist further in view of EMV.

j) [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;”

178. 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. In particular, because it is uncertain that the user will have wireless network connection during the next transaction, *supra* Part VIII.C.1, it is imperative that the application requests the new Session Key (“second non-permanent cryptographic key”) immediately after authorization of a transaction (hence consumption of the last Session Key) if the device has wireless connection. Further, for reasons explained in [1.A-3] of Ground 1, a POSA would have found it obvious to program the application to “request” and receive the key from the server.

k) [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”

179. 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 reason as explained in [1.F] above, this element is obvious over Mellqvist further in view of EMV.

l) [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.”

180. 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.

3. Claim 17

a) [17.PRE]: “A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

181. To the extent the preamble is limiting, for the reasons discussed for [1.PRE] and [1.E], Mellqvist alone or further in view of EMV discloses this limitation.

b) [17.A] a mobile device comprising:

182. For reasons discussed for [1.A-1], Mellqvist alone or further in view of EMV discloses a “mobile device.”

c) [17.B]: “a controller configured to route communications received over a communication channel from an electronic reader;”

183. Mellqvist discloses a portable electronic 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.

d) [17.C]: “a wireless interface to connect to a wireless network that is separate from the communications channel;”

184. Mellqvist discloses that the portable electronic device has a “transceiver” 212 that may communicate with a base station 260. *Id.* [0041], Fig. 2. For reasons stated for [1.A-3], this is a communications channel separate from the NFC communications, which are handled by NFC frontend 250. *Id.* [0041], Fig. 2. Therefore, Mellqvist discloses this element.

e) [17.D]: “a processor;”

185. Mellqvist discloses that the portable electronic device has a processor 295. Ex[Mellqvist] [0040]-[0041]. Moreover, it was well known in the art that a “Card” in EMV transactions also contains a processor. Ex[1037] at 38-41.

f) [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:”

186. For reasons discussed for [1.A-1], [1.A-2], and [1.A-4], Mellqvist discloses such an application. Further, Mellqvist discloses a memory 280 that “may communicate with processor,” and embodiments of Mellqvist may be “a computer program product on a ... storage medium having computer-usable or computer-

readable program code ... for use by or in connection with an instruction execution system.” Ex[0014], [0023]. An EMV “Card” similarly has such an application stored in the memory and accessible to the processor. Ex[1037] at 38-41. Therefore, this element is obvious over Mellqvist further in view of EMV.

(1) [17.E-1]: “request from the remote computer system, over the wireless network, a first set of data associated with the account;”

187. For reasons discussed for [1.B], this element is obvious over Mellqvist further in view of EMV.

(2) [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;”

188. For the reasons discussed for [1.C], this element is obvious over Mellqvist further in view of EMV.

(3) [17.E-3]: “store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;”

189. For the reasons discussed for [1.D], this element is obvious over Mellqvist further in view of EMV.

(4) [17.E-4]: “during an interrogation:”

190. For the reasons discussed for [1.E], this element is obvious over Mellqvist further in view of EMV.

(a) [17E-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;”

191. For the reasons discussed for [1.E-1], this element is disclosed by EMV and thus obvious over Mellqvist further in view of EMV.

(b) [17.E-4b]: “access the local cryptographic key associated with the account;”

192. For the reasons discussed for [1.D] and [1.E-2], this element is disclosed by EMV and obvious over Mellqvist further in view of EMV because the Application Cryptogram is generated using the previously stored local Session Key.

(c) [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”

193. For the reasons discussed for [1.E-2], this element is disclosed by EMV and thus obvious over Mellqvist further in view of EMV.

(d) [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;”

194. For the reasons discussed for [1.E-3], this element is disclosed by EMV and thus obvious over Mellqvist further in view of EMV.

g) [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;”

195. For the reasons discussed for [1.F], this element is obvious over Mellqvist further in view of EMV.

h) [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”

196. For the reasons discussed for [1.G], this element is obvious over Mellqvist further in view of EMV.

i) [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.”

197. For the reasons discussed for [1.H], this element is obvious over Mellqvist further in view of EMV.

4. Claims 2 and 18: “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”; “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.”

198. 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.¹⁶ 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. Therefore, these claims are obvious over Mellqvist further in view of EMV.

¹⁶ 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.

5. Claims 3 and 19: “wherein the response cryptogram is a hash”

199. 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, as further explained above. Therefore, these claims are obvious over Mellqvist further in view of EMV.

6. Claims 4 and 20: “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”

200. For reasons stated above in Part VIII.C.1, a POSA would have found it obvious and be positively motivated to implement Mellqvist to carry out mainstream payment card transactions, in particular 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]. Accordingly, these claims are obvious over Mellqvist.

7. Claims 5 and 21: “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”

201. For reasons stated for Claims 5 and 21 in Ground 1, EMV discloses these claims. Accordingly, Therefore, these claims are obvious over Mellqvist further in view of EMV.

8. Claims 6 and 22: “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”

202. For reasons stated for Claims 6 and 22 in Ground 1, EMV discloses these claims. Accordingly, these claims are obvious over Mellqvist further in view of EMV.

9. Claims 7 and 23: “wherein the mobile device does not have connectivity to the wireless network during the interrogation”

203. As discussed in above in Part VIII.C.1, 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 further in view of EMV.

10. Claim 8

a) [8.PRE]: “further comprising, at the remote computer system:”

204. Mellqvist discloses “remote secure element servers” that satisfies this element. Ex[1014] [0035]-[0036].

b) [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”

205. For the reasons discussed for [1.A-3], [1.B]-[1.C], Mellqvist in view of EMV renders it obvious that the portable device requests and receives a first Session Key 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. 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 as well as for multiple 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.

c) [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.”

206. For the reasons discussed for [1.A-3], [1.F], and [1.G], Mellqvist renders it obvious that the mobile application requests and receives a second Session Key which is a key associated with the account, over the wireless network from the remotely hosted secure elements. Therefore, it would have obvious to have such secure elements generate the Session Key. 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.

11. Claims 9 and 26: “wherein the digital credential comprises a secure element representation maintained at the remote computer system”; “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”

207. As explained above for [1.A-2c], according to the '171 Patent, a “digital credential” is a “secure element representation” that may be hosted on a remote server. Mellqvist explicitly discloses such remotely hosted secure elements, Ex[1014] [0036], and thus discloses these claims.

12. Claims 10 and 27

a) [10.PRE]/[27.PRE]: “The method of claim 1, further comprising, at the remote computer system, performing an authorization process comprising:” / “further comprising, a remote computer system programmed to:”

208. 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 have understood this to be carried out on a remote server or server network. Accordingly, this element is obvious over Mellqvist further in view of EMV.

b) [10.A]/[27.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;”

209. 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] at 57-58. Accordingly, this element is obvious over Mellqvist further in view of EMV.

c) [10.B]/[27.B]: “determining a current non-permanent cryptographic key associated with the account using the account identifier;”

210. 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] at 58 (server would: “Derive the actual session key SSK_{AC} ...”); Accordingly, this element is obvious over Mellqvist further in view of EMV.

d) [10.C]/[27.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”

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

e) [10.D]/[27.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.”

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

13. Claims 11 and 28: “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”

213. As discussed for Claims 11 and 28 in Ground 1, a transaction under EMV satisfies these claims. Accordingly, these claims are obvious over Mellqvist further in view of EMV.

14. Claims 12 and 29: “wherein the POS command communications comprise the unpredictable data”

214. As discussed for Claims 12 and 29 in Ground 1, a transaction under EMV satisfies these claims. Accordingly, these claims are obvious over Mellqvist further in view of EMV.

15. Claims 13 and 30: “wherein the authorization data further comprises values from the transaction”

215. As discussed for Claims 13 and 30 in Ground 1, a transaction under EMV satisfies these claims. Accordingly, these claims are obvious over Mellqvist further in view of EMV.

16. Claims 14 and 31: “wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process”

216. As discussed for [1.F] above, a POSA would have found it obvious to configure the application requests the new Session Key as soon as possible *upon authorization of a transaction* which consumes the last Session Key if the device has wireless connection, so that a new, unused Session Key can be ready for the next transaction. Hence, a POSA would have understood or found it obvious that the key is shared as part of the “authorization process.” 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—otherwise, it would be wasteful to have unused keys. Accordingly, these claims are obvious over Mellqvist further in view of EMV.

17. Claims 15 and 32: “wherein the application is [configured/executable] to generate the response cryptogram according to a card specification”

217. As explained, 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 Application Cryptogram, which is a response cryptogram. Ex[1020] § 8.1.2. Accordingly, these claims are obvious over Mellqvist.

18. Claims 16 and 33: “wherein the first and second non-permanent cryptographic key are associated with an issuer master key”

218. 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 above, 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 further in view of EMV.

19. Claim 24: “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation”

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

20. Claim 25: “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”

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

221. In conclusion, all claims of the '171 Patent are obvious in view of Mellqvist further in view of EMV.

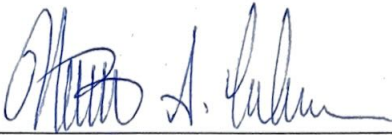
IX. RESERVATION OF RIGHTS

222. My opinions are based upon the information I considered to date. I am not aware of evidence of objective indicia of non-obviousness for the '171 Patent. I reserve the right to supplement my opinions to respond to arguments raised by the owner of the '171 Patent and to consider new information made available to me.

X. DECLARATION

223. I hereby declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true. I further understand that willful false statements and the like are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code. I declare under penalty of perjury that the foregoing is true and correct.

Executed on August 12, 2023.



A handwritten signature in blue ink, appearing to read "Mark A. Cohen", is written over a horizontal line.

Appendix A

Curriculum Vitae

Matthew A. Calman

4420 Beaver Hollow SE
Cedar Rapids, Iowa 52403

Mobile: +1 704-724-4247

matt.calman@outlook.com

Professional Summary

Mr. Calman has more than 35 years of experience as a banking leader, industry collaborator, and fintech innovator in payments and deposits, mobile financial services, online banking, and Check21 image transactions at billion scale.

As an Expert Witness, Mr. Calman has supported both Plaintiff and Defense teams in disputes and investigations before U.S. Federal District Courts, the American Arbitration Association, the USPTO Patent and Trademarks Appeals Board and the European Commission.

Mr. Calman led the process engineering for Bank of America's digital transformation to check image exchange in 2004. From 2006-2013, he led the bank's R&D function supporting innovation in payments, mobile deposits, mobile commerce, mobile wallet, augmented reality, biometrics, video banking, machine vision, AI, cryptography and other emerging technologies. He was appointed Research Affiliate at the MIT Media Lab where he led the *Center for Future Banking* from 2009-2012.

Mr. Calman is a named inventor on 96 issued U.S. patents and 244 U.S. patent applications and was twice awarded *Inventor of the Year* by Bank of America for his development of intellectual property singly and on teams.

From 2015-2018, at Microsoft, the Innovation Outreach Program connected 80 innovation executives from 35 Fortune 100 companies for prototyping and development of cloud, cryptography, augmented reality and AI technologies.

Today, Calman is a faculty member at Coe College teaching statistics and consulting.

Expertise

- | | | |
|---|--|---|
| ▪ Mobile and online financial services research & development | ▪ Mobile payments including contactless/NFC, cloud, barcode, location-based services | ▪ Billion-scale financial services payment and deposit transaction processing |
| ▪ Mobile deposit | | |
| ▪ HCI / Human Computer Interaction research | ▪ Financial services industry consortiums | ▪ Imaging and archive technologies and applications |
| ▪ Applied machine vision systems and augmented reality research | ▪ Corporate innovation labs & innovation teams | ▪ Code review and process mapping |

Education

Carnegie Mellon University, Pittsburgh, Pennsylvania, Applied Mathematics, 1982 - 1984

Georgia State University, Atlanta, Georgia, Executive MBA program 1997-1999

Degree: Masters in Business Administration (May 1999)

Honors: George J. Malanos Award for Academic Excellence

Litigation and Case Experience

	Matter	Firm	Jurisdiction	Role(s)
2023	OV Loop Inc. v. <u>MasterCard</u> International, et al	Baker Botts	PTAB / IPR	Expert declaration
	Anti-competition Investigation into <u>Apple</u> Pay	Gibson Dunn	European Commission	Expert reports
	Nantworks LLC v. <u>Bank of America</u> , Case No. 2:220-cv-07872	Bank of America Winston Strawn	Central District of Calif.	Fact witness
2021	<u>USAA</u> v. PNC Bank, N.A., Case No. 2:20-cv-00319	Irell Manella	Eastern District of Texas	Consulting expert
	Caselas LLC v. <u>First Community Bancshares, Inc., et al</u> , Case No. 2:21-cv-0030	Foley & Lardner LLP	Eastern District of Texas Western District of Texas	Consulting expert
2020	<u>NCR</u> v. Lighthouse Consulting Group, LLC, Case No. 2:19-cv-00392	King & Spaulding	Western District of Texas	Consulting expert
	<u>USAA</u> v. Wells Fargo Corporation, Case No. 2:18-cv-3656	Irell Manella	Eastern District of Texas	Consulting expert
2019	<u>USAA</u> v. Wells Fargo Corporation, Case No. 2:16-CV-245	Irell Manella	Eastern District of Texas	Expert reports, deposition, testimony
	Wells Fargo Bank v. <u>USAA</u> , Cases CBM2019-00002, 29, 28, 27	Irell Manella	PTAB	Expert declarations
	Wells Fargo Bank vs. <u>USAA</u> , IPRs 2019-01081, 1082, 1083	Irell Manella	PTAB	Expert declarations
2015-2018	<i>at Microsoft</i>			
2015	<u>Gemalto, Inc.</u> v. Merchant Customer Exchange LLC, AAA Case No. 01-14-0001-2157	Mayer Brown	AAA panel	Expert reports, testimony
	Datatresury Corporation v. <u>Jack Henry & Associates, Inc. et al</u> , Case No. 2:13-cv-00433	Polsinelli	Eastern District of Texas	Expert declarations
2014	Joao Bock Transaction Systems LLC v. <u>Jack Henry & Associates, Inc.</u> , Case No. 12-1138-SLR	Polsinelli	District of Delaware	Expert reports, deposition
	<u>Askeladden LLC</u> v. Loyalty Conversion Systems Corporation, Cases IPR2015-00122, 123, 124, 125, 133, 137	Fitzpatrick Cella	PTAB	Expert declarations
2009-2010	Datatresury Corporation v. Wells Fargo et al (<u>Bank of America</u>), Case No. 2:06-cv-72 DF	Bank of America Fish & Richardson	Eastern District of Texas	Fact witness

96 Issued U.S. Patents (named inventor)

Mobile Payments	Social Commerce / connected spending	Security / privacy / fraud	Servicing customers through video or mobile	Marketing / offers / location-based services	VR/AR and real-time video analysis
9,582,826	10,002,395	9,646,342	9,754,320	9,384,497	10,268,891
9,514,456	9,990,594	9,519,934	9,508,058	8,694,456	10,268,890
9,508,070	9,965,729	9,043,609	9,007,448	8,660,951	9,524,524
9,177,451	9,934,536	8,639,062	9,001,180	8,554,647	9,519,932
9,177,308	9,786,019	8,126,252	8,942,684	8,544,725	9,519,924
9,053,490	9,786,018		8,902,279		9,519,923
9,047,595	9,773,285	Machine learning	8,867,734	Ethical spending	9,317,860
9,026,461	9,639,893	8,444,051	8,866,878	9,530,145	9,317,835
9,026,460	9,639,892	8,161,325	8,866,877	9,519,913	9,224,166
9,026,453	9,436,965		8,490,864	9,406,031	9,105,011
9,015,070	9,390,454	Image processing		9,374,430	8,929,591
8,965,790	9,390,453	8,811,711	Transaction processing / cash processing / mail	8,356,302	8,922,657
8,925,805	9,384,514	7,971,059			8,873,807
8,925,804	9,336,548	7,630,518	8,972,292	Personal Financial Management (PFM)	8,721,337
8,805,725	9,324,115		8,903,154		8,718,612
8,744,968	9,324,114	ATM/mobile/online banking	8,447,094	9,767,503	8,668,498
8,732,077	9,323,852		8,352,383	9,600,839	8,611,601
8,571,985	9,311,685		8,184,893	9,519,928	8,582,850
		8,688,559			8,571,888
					8,438,110

Professional Experience

Currently [Coe College](#) | Cedar Rapids, IA
Faculty Lecturer in statistics for undergraduate business majors.

2018- Current [GDI Experts LLC](#) | Cedar Rapids, IA
Consultant to banks and related firms on innovation and IP development; expert witness for financial services technology and intellectual property matters.

2015 – 2018 [Microsoft Corporation](#) | Seattle, WA | Principal Program Manager
Program Manager of the “Innovation Outreach Program”, a global network of heads of R&D and innovation from 35 of the world’s largest companies. Collaborated on client solutions with Microsoft technologies including Azure cloud, AI/ML, Hololens/Mixed Reality, cryptography, data visualization, NLP, OCR, and cognitive services.

2013 – 2015 [Calman & Company LLC](#) | Charlotte, NC
Consultant to banks and related firms on innovation and IP development; expert witness for financial services technology cases.

2006 – 2013 [Bank of America](#) | Charlotte, NC | SVP, R&D Executive
R&D Executive of the Gateway Innovation Lab, responsible for research, concept development, prototypes, patent applications and customer tests of future products.

2003 – 2006 [Bank of America](#) | Charlotte, NC | SVP, Check 21 Process Executive
Process design executive for Check 21 Image Exchange, developed transaction processing infrastructure capable of clearing more than 10 billion check annually; then process design executive for Check Image Deposits Platform for teller, ATM, lockbox, online, remote check image capture and mobile check deposits.

2002 – 2003 [Bank of America](#) | Atlanta, GA | SVP, Process Design Executive
Six Sigma Black Belt for nationwide check operations, responsible for operations process quality and delivered \$10 million in annual efficiency improvements

Professional Experience (continued)

2001 – 2002	Bank of America Atlanta, GA SVP, Industry Joint Venture
1999 – 2001	Bank of America Atlanta, GA SVP, Tech & Ops Business Architecture
1996 – 1999	NationsBank Atlanta, GA VP, Merger Transition Change Manager
1986 – 1995	Commerce Union Bank Nashville, TN and C&S/Sovran Bank Atlanta, GA VP, Corporate Trust Division Operations and Automation Manager
1985 –1986	Premier Systems, Inc. Wayne, PA Systems Converter – Corporate Trust Systems

Certifications

2002	Six Sigma Black Belt	Bank of America
2001	Six Sigma Green Belt	Bank of America

Professional Organizations

2015-2017	Federal Reserve Faster Payments Task Force , individual participant
2011-2020	Association of Managers of Innovation , 501c(3) non-profit, board director '12-'14, Washington, DC
2011-2014	Mobey Forum , board of directors '13-'14,, Helsinki, Finland Lifetime Member awarded
2011-2013	Microsoft Innovation Outreach Program , founding member, advisory board, Seattle, WA,
2010-2015	Federal Reserve Mobile Payments Industry Workgroup , steering committee, Boston, MA & Atlanta, GA,
2010-2013	Marketing Science Institute , trustee, Cambridge, MA
2010-2011	Smart Card Alliance , board of directors, Princeton, NJ
2007-2008	Financial Services Technology Consortium , board of directors, Washington, DC
2005-2006	Electronic Check Clearinghouse Organization , board of directors alternate, Dallas TX
1994-1995	Securities Industry Daily , editorial advisory board
1991-1993	BondMaster Users Association , President

Civic Awards

2022	United Way, Volunteer Social Impact Award , Cedar Rapids, IA
------	---

Professional Appointments & Awards

2011-2016	BAI Global Banking Innovation Awards, Innovation Circle Judge , Chicago, IL
2011	Bank of America Inventor of the Year (Team award)
2009-2011	MIT Media Lab, Appointed Research Affiliate and Executive in Residence , Cambridge, MA
2007	Bank of America Inventor of the Year (Individual award)
1998	NationsBank Leadership Award
1995	NationsBank Technology Expert

Publications

2013	Calman M, Dinh N, Ewing D, Sarai R, Schmeltzer G, Sidhu P, Steere D, "The MPOS Breakthrough: How the Power of Mobile has Disrupted Payments," (Mobey Forum, 2013)
2013	Calman M, Dinh N, Rankin G, Sarai R, Sidhu P, Verdeschi J "The MPOS Strategy: Shifting the Balance of `Power,"

Case Study

- 2005 Gardner J, **Innovation and the Future Proof Bank**, (Wiley) ISBN-13: 978-0470714195
"Case Study: Innovation at Bank of America," pp. 85-88 *Describes my work, my team and our approach.*

Media

- March 27, 2015 **"Bank of America patents mobile banking programs and video ATM terminals,"**
Steve Brachman, IPwatchdog.com, (named inventor on 5 of 13 applications cited)
- December 29, 2014 **"Top 10 Patent Applications for 2014,"** Steve Brachman, IPwatchdog.com, (cited as #8)
- December 3, 2014 **"Bank of America Patents: From Customer Loyalty to Cybersecurity and Social Networking,"**
Steve Brachmann, (named inventor on 4 of 13 applications cited)
- October 14, 2014 **"Taking Innovation to the Next Level"** Kenneth Cline, BAI Banking Strategies
- February 16, 2014 **"Doing Better: Nonprofit AMI creating innovative NC business leaders,"** Christopher Gergen
and Stephen Martin, Raleigh News & Observer
- November 25, 2013 **"Mobile Point of Sale Projected to Reach 46% Market Share in 2017,"**
Bailey Reutzel, Payments Source
- May 3, 2013 **"Mobey Forum Tackles Mobile Payments,"** Bryan Yurcan, Bank Systems & Technology
- January 7, 2013 **"Predictions 2013,"** Electronic Payments International
- September 18, 2012 **"Bank of America's Wild Patents on Live-Video Analysis Could Reinvent Mobile Banking,
Shopping and More,"** Gus G. Sentementes, Baltimore Sun
- February 4, 2010 **"More Banks Try to Seed Innovation Through Labs,"** Karen Epper Hoffman, American Banker
- February 2010 **"Banks Incubate the Innovation Fixation,"** Karen Epper Hoffman, Bank Technology News,
- March 8, 2007 **"In Brief: Test Developed to Calibrate Imaging,"** Steve Bills, American Banker
- March 31, 2004 **"The Tech Scene: Problem of Blurry Images Clouds Check 21's Future,"**
Chris Costanzo, American Banker

Invited Speaker at Industry Conferences

Sept 2017	Microsoft Design Salon	Los Angeles, CA	<i>Fostering Idea Flow and Connections at Microsoft's Innovation Outreach Program</i>
Sept 2017	Ford Motor Global Developers	Dearborn, MI	<i>Lessons Learned on an Innovation Journey</i>
Sept 2015	payCLT	Charlotte, NC	<i>Capitalizing on the Stages of Innovation</i>
Oct 2014	BAI Retail Delivery Conference	Las Vegas, NV	<i>Partnerships for Innovation: No size fits all!</i>
Sept 2014	2014 CEO FinSvcs Roundtable	Washington, D.C.	<i>Rewarding Innovation</i>
Aug 2013	PYMNTS.COM @Harvard	Cambridge, MA	<i>The Technology of Mobile Commerce</i>
Oct 2012	Microsoft IOP	Amsterdam, NL	<i>Research Programs in HCI</i>
Oct 2012	BAI Retail Delivery Conference	Washington, DC	Mobile Payments Panelist
Feb 2012	Mobey Day 2012	Barcelona, Spain	<i>Leading innovation in mobile payments</i>
Feb 2012	Smart Card Alliance Summit	Salt Lake City, UT	<i>Can Stakeholders Find a Path to Mobile Payments Adoption</i>
Oct 2011	BEI: Back End of Innovation	Boston, MA	<i>Creating and Operating a Successful R&D Subculture</i>
Oct 2011	BAI Retail Delivery	Orlando, FL	Panelist on innovation leadership
June 2011	Mobey Forum	Helsinki, Finland	<i>Mobile Commerce at Bank of America</i>
Nov 2010	Marketing Sciences Institute	San Francisco, CA	<i>The Journey from Innovation to R&D</i>
May 2010	Mobile Monday America	Boston, MA	Panelist on mobile payments
May 2010	FEI: Front End of Innovation	Boston, MA	<i>Innovation at Bank of America</i>
April 2009	Canadian Assoc of Innovation	Toronto, ON	<i>Leading Innovation</i>
Sept 2008	PDMA Annual Conference	Orlando, FL	<i>Inside the Guru's Studio</i>
Nov 2006	McKinsey Check Forum	Atlanta, GA	<i>Leading the Industry in Evolutionary Change</i>
May 2006	BAI TransPay	Las Vegas, NV	<i>Managing Suppliers through Image Platform Change</i>
Apr 2006	KPMG FSI Perspective Forum	New York, NY	Corporate innovation panelist
Feb 2006	McKinsey Strategy Forum	Philadelphia, PA	<i>Design Choices in Image Transactions</i>
Feb 2005	EastPay Information Exchange	New York, NY	<i>Check 21 Update: Our March to Interoperability</i>
Jan 2005	McKinsey Check Forum	Atlanta, GA	<i>Leading the Industry in Evolutionary Change</i>
Oct 2004	NY Float Mgt Roundtable	New York, NY	<i>How FSTC Defines Image Quality & Usability</i>
Oct 2004	Orbograph Annual Conference	Orlando, FL	<i>The Impact of Six Sigma & the Drive for Image Quality</i>
Oct 2004	McKinsey Check Forum	Atlanta, GA	<i>Check 21 is Here</i>
Sept 2004	BAI Check Conference	Orlando, FL	<i>Making Image Exchange Happen</i>
May 2004	BAI TransPay	Las Vegas, NV	<i>Bank of America's Check 21 Strategy</i>
May 2004	McKinsey UK Cheque Forum	London, England	<i>Preparing for Check 21</i>
Oct 2003	McKinsey Check Forum	Atlanta, GA	Check 21 Briefing

Invited Speaker at Graduate Schools and Universities

Apr 2013	University of North Carolina, MBA program	Charlotte, NC	Leading Innovation at Bank of America
Mar 2012	Carnegie Mellon University E&TIM Masters Program	Pittsburgh, PA	Leading Innovation at Bank of America
Mar 2010	Carnegie Mellon University E&TIM Masters Program	Pittsburgh, PA	Leading Innovation at Bank of America
Apr 2009	Georgia State University Executive MBA Program	Atlanta, GA	Observations on Business in China
Jan 2009	Carnegie Mellon University Leadership Lecture Series	Pittsburgh, PA	Leading Innovation at Bank of America
Jun 2007	Vanderbilt University	Nashville, TN	Design Choices in Image Exchange co-taught with Vanderbilt Prof. David Owen
Nov 2007, 2005, 2004	Georgia State University	Atlanta, GA	Regulatory change drives innovation

Invited Speaker at Government Agencies

Dec 2014	Federal Reserve Mobile Payments Industry Workgroup	Boston, MA	Panel moderator on POS Wallet Platforms
Aug 2012	Federal Financial Institutions Examination Council (FFIEC) Mobile Payments Conference	Washington, DC	Mobile banking panelist
Mar 2011	Center for the Study of Intelligence	Langley, VA	<i>The Coming Mobile-Centric World</i>
Feb 2010	Federal Reserve Board	Washington, DC	<i>Cash, check or cell phone? Protecting customers in a mobile finance world</i>
Oct 2006	FBI, Dept of the Treasury	Washington, DC	Check 21 panelist

Updated August 2023