

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

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

TABLE OF CONTENTS

I.	Background and Qualifications	2
A.	Educational Background	2
B.	Career History	2
C.	Materials and Other Information Considered	4
II.	Understanding of the Law	4
A.	Legal Standard for Anticipation.....	4
B.	Legal Standard for Obviousness	5
C.	Legal Standard for Claim Construction	10
III.	The '171 Patent.....	15
A.	Background of Technology.....	15
1.	Payment Process	15
2.	Chip Card and Contactless Chip Card Payments	17
3.	Mobile Payments.....	19
B.	The '171 Patent	19
C.	Prosecution History Summary of the '171 Patent.....	20
IV.	Priority Date of the '171 Patent.....	21
V.	Level of Ordinary Skill in the Art	24
VI.	Claim Construction.....	25
VII.	Summary of the Prior Art	25
A.	Collinge (Ex[1011])	26
1.	Collinge Disclosure.....	26
2.	Collinge is Supported by its Provisional Applications.....	30
B.	Fiske (Ex[1012]).....	36
VIII.	Grounds of Invalidity.....	38
A.	Grounds 1 and 2: Claims 1-33 Are Anticipated and Rendered Obvious by Collinge in View of Knowledge of a POSA	38

1.	Claim 1	38
2.	Claims 2 and 18: “wherein the mobile device is an NFC emulating device, wherein ... data associated with the account are received via a data connection over the internet” ..	57
3.	Claims 3 and 19: “wherein the response cryptogram is a hash”	58
4.	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”	59
5.	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”	60
6.	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”	61
7.	Claims 7 and 23: “wherein the mobile device does not have connectivity to the wireless network during the interrogation”	62
8.	Claim 8	62
9.	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”	63
10.	Claims 10 and 27	64
11.	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”	67
12.	Claims 12 and 29: “wherein the POS command communications comprise the unpredictable data”	68
13.	Claims 13 and 30: “wherein the authorization data further comprises values from the transaction”	68
14.	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”	68
15.	Claims 15 and 32: “wherein the application is [configured/executable] to generate the response cryptogram according to a card specification”	69
16.	Claims 16 and 33: “wherein the first and second non-permanent cryptographic key are associated with an issuer master key”	69
17.	Claim 17	70
18.	Claim 24: “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation”	75
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”	75
B.	Grounds 3 and 4: Claims 1-33 Are Anticipated and Rendered Obvious by Fiske in View of Knowledge of a POSA.....	75
1.	Claim 1	75
2.	Claims 2 and 18: “wherein the mobile device is an NFC emulating device, wherein ... data associated with the account are received via a data connection over the internet” ..	86
3.	Claims 3 and 19: “wherein the response cryptogram is a hash”	87

4.	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”	88
5.	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”	89
6.	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”	89
7.	Claims 7 and 23: “wherein the mobile device does not have connectivity to the wireless network during the interrogation”	89
8.	Claim 8.....	90
9.	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”	91
10.	Claims 10 and 27.....	91
11.	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”	93
12.	Claims 12 and 29: “wherein the POS command communications comprise the unpredictable data”	94
13.	Claims 13 and 30: “wherein the authorization data further comprises values from the transaction”	94

14.	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”	95
15.	Claims 15 and 32: “wherein the application is [configured/executable] to generate the response cryptogram according to a card specification”	95
16.	Claims 16 and 33: “wherein the first and second non-permanent cryptographic key are associated with an issuer master key”	96
17.	Claim 17	96
18.	Claim 24: “wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation”	100
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”	100
IX.	Reservation of Rights	100
X.	DECLARATION	102

LIST OF EXHIBITS

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

Exhibit No.	Description
1023	<i>EMV® Contactless Specifications for Payment Systems, Book A: Architecture and General Requirements, Version 2.1 (March 2011) (Attachment E to Byrne Declaration)</i>
1024	<i>EMV® Contactless Specifications for Payment Systems, Book B: Entry Point Specification, Version 2.1 (Attachment F to Byrne Declaration)</i>
1025	<i>EMV® Contactless Specifications for Payment Systems, Book C-1: Kernel 1 Specification, Version 2.1 (March 2011) (Attachment G to Byrne Declaration)</i>
1026	<i>EMV® Contactless Specifications for Payment Systems, Book C-2: Kernel 2 Specification, Version 2.1 (March 2011) (Attachment H to Byrne Declaration)</i>
1027	<i>EMV® Contactless Specifications for Payment Systems, Book C-3: Kernel 3 Specification, Version 2.1 (March 2011) (Attachment I to Byrne Declaration)</i>
1028	<i>EMV® Contactless Specifications for Payment Systems, Book C-4: Kernel 4 Specification, Version 2.1 (March 2011) (Attachment J to Byrne Declaration)</i>
1029	<i>EMV® Contactless Specifications for Payment Systems, Book D: EMV Contactless Communication Protocol Specification, Version 2.1 (March 2011) (Attachment K to Byrne Declaration)</i>
1030	Reserved
1031	Reserved
1032	Expert Declaration of Dr. Sylvia Hall-Ellis dated August 11 (“Hall-Ellis Declaration”) and Attachments
1033	Curriculum Vitae of Dr. Sylvia Hall-Ellis
1034	Carl H. Meyer, Stephen M. Matyas, <i>Cryptography: A New Dimension In Computer Data Security. A Guide for the Design and Implementation of Secure Systems</i> (1982)
1035	Reserved
1036	Reserved
1037	Cristian Radu, <i>Implementing Electronic Card Payment Systems</i> (2003)
1038	Reserved
1039	Kefa Rabah, <i>Theory and Implementation of Data Encryption Standard: A Review</i> , Inform. Technol. J., 4: 307-325 (Apr. 2005)

Exhibit No.	Description
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	Reserved
1042	EMVCo FAQ webpage (Aug. 3, 2023, 11:43 AM), https://web.archive.org/web/20110920080137/http://www.emvco.com/faq.aspx?id=37
1043	Newton's Telecom Dictionary (25th ed. 2009)
1044	Reserved
1045	<i>OV Loop, Inc. v. Mastercard Inc.</i> , No. 7:23-cv-01773-CS, D.I. 31 (S.D.N.Y. June 8, 2023)
1046	Mike Clark, <i>SimplyTapp picks up contactless payments award</i> , NFCW (Aug. 25, 2015), https://www.nfcw.com/2015/08/25/337201/simplytapp-picks-up-contactless-payments-award/
1047	Payal Shukla, Jim Jarvie, <i>SimplyTapp Wins Best Contactless Payments Solution as Future Digital Awards</i> (Aug. 13, 2015), https://www.prweb.com/releases/2015/08/prweb12903489.htm

I. INTRODUCTION

I, Stuart Fiske, declare as follows:

1. My name is Stuart Fiske. I submit this declaration in support of a petition for *Inter Partes* Review of U.S. Patent No. 10,032,171 (“the ’171 Patent”). I have prepared this declaration as an expert witness retained by Mastercard Incorporated and Mastercard International Incorporated (“Petitioner”). Herein I give my opinions as to how a hypothetical person of ordinary skill in the art (“POSA”) would understand the scope of the claims and whether certain claims of the ’171 Patent are invalid. I provide technical bases for these opinions as appropriate.

2. This declaration contains statements of my opinions formed to date and the bases and reasons for those opinions. I may offer additional opinions based on further review of materials in this case, including opinions and/or testimony of other expert witnesses. I make this declaration based upon my own personal knowledge and, if called upon to testify, 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. My compensation is in no way contingent on the results of these or any other proceedings relating to the above-captioned patent.

I. BACKGROUND AND QUALIFICATIONS

3. In formulating my opinions, I have relied upon my training, knowledge, and experience in the relevant art. I have summarized in this section my educational background, career history, publications, and other relevant qualifications. My full curriculum vitae is attached as Exhibit 1007 to this declaration.

A. Educational Background

4. I received a B.A. degree in Physics from University of York with Honours, and I received a D. Phil. degree in X-ray also from University of York.

B. Career History

5. I have over 20 years of experience in the field of payment systems, including the area of systems specification and verification, coupled with deep knowledge of smartcards, both contact and contactless, and mobile, Near Field Communication (“NFC”) and Host Card Emulation (“HCE”). These skills include business requirements gathering and specification, functional specification, and System and Acceptance Test Specification.

6. From 1990 until 1999, I worked primarily for digital mobile network operators, helping set up the systems to support the design, acquisition, and rollout of network base stations for the One2One (now EE) network in the UK, and assisting Cellnet (now Virgin Media O2) in the delivery of early prepay propositions to the UK market.

7. From 1999 to 2013, my primary role was as the lead consultant and relationship manager to American Express, where I led projects covering many aspects of the migration of the American Express card payment product to EMV (Europay International, MasterCard International and Visa International), including the Amex Blue card launch in the United States, development of the specification and implementation of the American Express EMV application on the MULTOS platform, development of the American Express Expresspay contactless payment card based on ISO 14443, and development of American Express Expresspay for Mobile specification as used on the ISIS platform in the United States.

8. From 2014 to 2020, I led several projects in developing dual interface card payment applications and in developing a combined EMV/DESFIRE smartcard application for support of legacy ticketing on bank cards. My mobile and contactless knowledge was used in the development of prototype and proof of concept demonstrators for the use of NFC-enabled mobile payments, including the use of HCE for both payments and ticketing. I advised the Payment Schemes on the specification and certification of global payments applications for HCE-enabled mobile payments. I have also specified demonstrators for Internet of Things (IoT) connected car payments and downloadable payment terminals, and carried out two technical due diligence studies of payment processing companies on behalf of potential inventors, which resulted in successful investments.

9. I am currently a Director at Consult Hyperion, where I have been working since 1986. As Director, my roles include handling financial aspects of running the company and close supervision of projects and client relationships, analysis of new technologies as they emerge and how they can be applied within the Retail Payments and Transit/Ticketing sectors, and developing new initiatives and new lines of business. I also spent about four years at Consult Hyperion consulting for the Financial Services sector (initially Base-24 software for ATM networks and information distribution networks for the London Stock Exchange).

C. Materials and Other Information Considered

10. I have considered information from various sources in forming my opinions. I have reviewed and considered each of the exhibits listed above in the List of Exhibits in forming my opinions.

II. UNDERSTANDING OF THE LAW

11. Although 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 Anticipation

12. I understand that, once the claims of a patent have been properly construed, the next step in determining anticipation of a patent claim requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

13. I understand that a prior art reference anticipates a challenged claim, and thus renders the claim invalid, if all limitations of the claim are disclosed in that prior art reference, either explicitly or inherently (i.e., necessarily present or implied), as arranged or combined in the claim.

14. I understand that a patent is anticipated if, before such person's invention thereof, the invention was made in the United States by another inventor who had not abandoned, suppressed, or concealed it.

15. I have written this report with the understanding that in an *inter partes* review anticipation must be shown by a preponderance of the evidence.

B. Legal Standard for Obviousness

16. I understand that even if a patent is not anticipated, it is still invalid if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the pertinent art.

17. I understand that a person of ordinary skill in the art provides a reference point from which the prior art and claimed invention should be viewed.

This reference point prevents a person of ordinary skill from using one's insight or hindsight in deciding whether a claim is obvious.

18. I also understand that an obviousness determination includes the consideration of various factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the challenged claims, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations, also referred to as objective considerations, of non-obviousness.

19. I am informed that objective considerations of non-obviousness may include (1) a long felt but unmet need in the prior art that was satisfied by the invention of the patent; (2) failure of others where the invention succeeds; (3) commercial success or lack of commercial success of processes covered by the patent; (4) unexpected results achieved by the invention; (5) praise of the invention by others skilled in the art; (6) taking of licenses under the patent by others; and (7) deliberate copying of the invention. I also understand that there must be a relationship or nexus between any such objective considerations and the claimed invention. I am aware of no such evidence relevant to this case. If any such evidence is introduced by the Patent Owner, I reserve the right to consider that evidence at such time. I further understand that contemporaneous and independent invention by others is an objective consideration supporting an obviousness determination.

20. I understand that an obviousness evaluation can be based on a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but other times the nexus linking two or more prior art references may be the background knowledge of one of ordinary skill or simple common sense. I further understand that an obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

21. I understand that if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

22. I also understand that practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I further understand that a person of ordinary skill in the art looking to overcome a problem will often be able to fit the teachings of multiple publications together like pieces of a puzzle, although the prior art need not be like two puzzle pieces that must fit perfectly together. I understand that obviousness analysis therefore considers the inferences and creative steps that a person of ordinary skill in the art would employ under the circumstances.

23. I understand that a particular combination may be proven obvious by showing that it was obvious to try the combination. For example, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp because the result is likely the product not of innovation but of ordinary skill and common sense.

24. I understand that the combination of familiar elements according to known methods may be proven obvious when it does no more than yield predictable results. When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, obviousness likely bars its patentability.

25. It is also my understanding that there are additional considerations that may be used as further guidance as to when a claim is obvious, including the following:

- the claimed invention is a simple substitution of one known element for another to obtain predictable results;
- the claimed invention uses known techniques to improve similar devices or methods in the same way;

- the claimed invention applies a known technique to a known device or method that is ready for improvement to yield predictable results; and
- there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims.

26. It is further my understanding that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill in the art, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

27. I understand that a claim can be obvious in light of a single reference, without the need to combine references, if the limitations of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art.

28. I understand that a person of ordinary skill could have combined two pieces of prior art or substituted one prior art element for another if the substitution can be made with predictable results, even if the swapped-in element is different from the swapped-out element. The relevant question is whether prior art techniques are interoperable with respect to one another, such that that a person of skill would view them as a design choice, or whether a person of skill could apply prior art techniques into a new combined system.

29. In sum, my understanding is that prior art teachings are properly combined where a person of ordinary skill in the art having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of limitations recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the limitations of multiple prior art references in the claimed manner.

30. I have been informed and understand that the obviousness analysis requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

31. I understand that in an *inter partes* review obviousness must be shown by a preponderance of the evidence.

C. Legal Standard for Claim Construction

32. I understand that a patent may include two types of claims, independent claims and dependent claims. An independent claim stands alone and includes only the limitations it recites. A dependent claim can depend from an independent claim or another dependent claim. I understand that a dependent claim includes all the limitations that it recites in addition to all of the limitations recited in the claim or claims from which it depends.

33. I understand that the purpose of claim construction is to understand how one skilled in the art would have understood the claim terms at the time the claimed invention was made. I also understand that claim construction is a matter of law for the Patent Trial and Appeal Board to decide.

34. I understand that a claim construction analysis begins with the plain meaning or the ordinary and customary meaning of the claim term in the context of the patent in which the term is used. The ordinary and customary meaning is the meaning that the term would have to a person of ordinary skill in the relevant art at the time of the invention in light of what the patent teaches.

35. In comparing the claims of the '171 Patent to the prior art, I have carefully considered the '171 Patent and its file history in light of the understanding of a person of skill at the time of the alleged invention.

36. I understand that to determine how a person of ordinary skill would understand a claim term, one should look to those sources available that show what a person of skill in the art would have understood disputed claim language to mean. The available sources may include both evidence intrinsic and extrinsic to the patent. Intrinsic evidence includes the words of the claims themselves, the remainder of the patent's specification, including materials incorporated by reference, and the prosecution history of the patent, including materials cited and statements made during the prosecution history. Extrinsic evidence, which is evidence external to the

patent and the prosecution history, may include materials concerning relevant scientific principles, the meaning of technical terms, and the state of the art.

37. I understand that, in construing a claim term, one looks first to the intrinsic patent evidence. The extrinsic evidence may also be useful in interpreting the claim term when the intrinsic evidence alone is insufficient to correctly resolve the meaning.

38. I understand that words or terms, which may include phrases, should be given their ordinary and accepted meaning unless it appears that the inventors were using them to mean something else. In making this determination, the claims, the patent specification, and the prosecution history are of paramount importance. Additionally, the specification and prosecution history must be consulted to confirm whether the patentee has acted as its own lexicographer (i.e., provided its own special meaning to any disputed terms), or intentionally disclaimed, disavowed, or surrendered any claim scope.

39. I understand that the claims of a patent define the scope of the rights conferred by the patent. Patentees are required to particularly point out and distinctly claim the subject matter which they regard as their invention. Because patentees are required to define precisely what they claim their inventions are, it is improper to construe claims in a manner different from the plain import of the terms used consistent with a patent's specification. Accordingly, a claim construction analysis

must begin with, and remain centered on, the claim language itself. Additionally, the context in which a term is used in the challenged claim can be highly instructive. Likewise, other claims of the patent in question can inform the meaning of a claim term. For example, because claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims. Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.

40. I understand that a person of ordinary skill in the art is deemed to read a claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. For this reason, the words of the claim must be interpreted in view of the entire specification. The specification is the primary basis for construing the claims and provides a safeguard such that correct constructions closely align with the specification. Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim as set forth in the patent itself.

41. I understand that it is improper to place too much emphasis on the plain or ordinary meaning of a claim term without adequate grounding of that term within the context of the specification of the challenged patent. Hence, claim terms should

not be broadly construed to encompass subject matter that is not supported when the claims are read in light of the invention described in the specification.

42. I understand that the role of the specification is to describe and enable the invention. In turn, the claims cannot be of broader scope than the invention that is set forth in the specification. Care must be taken because a word-by-word definition, removed from the context of the patent, leads to an overall result that departs significantly from the patented invention.

43. I understand that claim terms must be construed in a manner consistent with the context of the intrinsic record. In addition to consulting the specification, one should also consider the patent's prosecution history. The prosecution file history provides evidence of how both the Patent Office and the patentee understood the terms of the patent, particularly in light of what was known in the prior art. Further, where the specification describes a claim term broadly, arguments and amendments made during prosecution may require a narrower interpretation.

44. I understand that while intrinsic evidence is of primary importance, extrinsic evidence, including expert and inventor testimony, dictionaries, and learned treatises, can also be considered. For example, technical dictionaries may help one better understand the underlying technology and the way in which one of skill in the art would understand the claim terms. Extrinsic evidence should not be considered, however, divorced from the context of the intrinsic evidence. Evidence

beyond the patent specification, prosecution history, and other claims in the patent should not be relied upon unless the claim language is ambiguous in light of these intrinsic sources. Furthermore, while extrinsic evidence can shed useful light on the relevant art, it is less significant than the intrinsic record in determining the legally operative meaning of claim language.

45. I understand that in general, a term or phrase found in the introductory words of the claim, referred to as the preamble of the claim, should be construed as a limitation if it recites essential structure or steps, or is necessary to give life, meaning, and vitality to the claim. Conversely, a preamble term or phrase is not limiting where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention. In making this distinction, one should review the entire patent to gain an understanding of what the inventors claim they actually invented and intended to encompass by the claims.

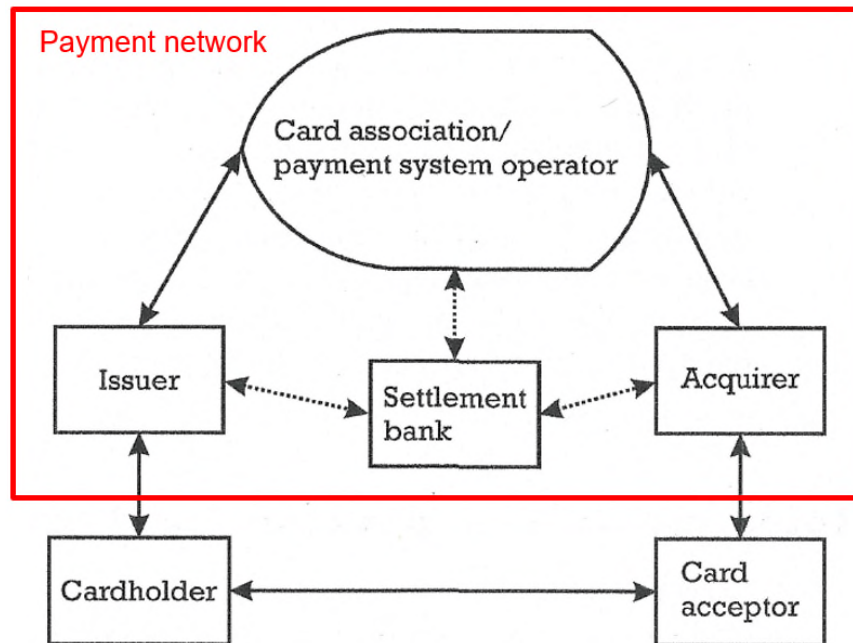
III. THE '171 PATENT

A. Background of Technology

1. Payment Process

46. Card payments, such as a debit or credit card transaction, generally rely on standardized infrastructure. Consumers typically have a credit card issued by a financial institution (known as the “issuer,”) while merchants typically have an

account for receiving payments at a financial institution known as the “acquirer.” Ex[1037] at 18. There are further players, such as payment system operators like Mastercard or Visa who may facilitate the transaction, as shown below, as part of a payment interchange network.



Ex[1037] at 18.

47. The typical transaction process involves the merchant reading information from the card or payment mobile device (such as card number, and authentication information) with a reader, a process known in the art as “interrogation,” *e.g.* Ex[1015], [0062], [0070], and such information, together with other information provided by the merchant and a point-of-sale (“POS”) terminal such as transaction amount, is sent to a payment network for further processing. The

portion of the system beyond the POS terminal may be collectively referred to as the payment network.

48. After the interrogation, the POS terminal typically generates a message known as an “authorization request,” which is transmitted to the issuer, which performs authentication that the card is genuine (a process known as “card authentication”), and performs financial/fraud checks, before returning an approval or non-approval message. Ex[1037] at 13-19, 20-33, 56-64.

2. Chip Card and Contactless Chip Card Payments

49. As of the '171 Patent's priority date, chip cards and contactless chip cards (with which a user can make a contactless transaction by tapping or waving the card at the reader, using technology such as near-field communication or NFC) of major payment brands such as Mastercard, Visa, as well as corresponding POS readers, conformed to or were migrating to industry standards and best practices. One important set of such standards or best practices are known as the EMV Specifications, Exs[1019]-[1029], 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 International, MasterCard International and Visa International. Ex[1042]. Payments made under EMV Specifications are referred to as “EMV transactions.”

50. One feature contactless payment transactions (such as EMV transactions) that helps combat fraud is card authentication with dynamically generated message authentication codes, or “*cryptograms*,” that differ for each transaction, such as an Authorization Request Cryptogram (“ARQC”), Ex[1040] § 2.1.1.1, or a CVC3, Ex[1011], [0050]. Traditional magnetic stripe cards contain static data, such as primary account number (“PAN”), expiration date, and CVV verification code—which can be copied onto a fraudulent card. EMV chip cards and mobile contactless payment devices, by contrast, may generate and provide POS readers with a message authentication code (e.g. a “cryptogram”) using an on-card processor and memory by encrypting data unique to the transaction, using a one-time cryptographic key known as the “Session Key” not revealed to the POS reader. This makes it difficult to duplicate the card because a reader would get a different cryptogram for each transaction and does not know the key—a necessary piece of information—used to compute it.

51. The POS reader would then include the cryptogram in the authorization request it sends to the payment network, and the issuer server, upon receiving the request, can regenerate the same cryptogram because the issuer also knows how to derive the Session Key for the transaction and knows the data used to calculate the cryptogram; if the cryptograms match, then the issuer may approve the transaction, provided that other conditions are satisfied. Ex[1037] at 57-58

3. Mobile Payments

52. As of the '171 Patent's priority date, mobile phones were being equipped with contactless or NFC capacity to conduct contactless payment transactions. Besides NFC capacities, such transactions had also required the same tamper-resistant chips (as in the chip cards) for storing sensitive payment credentials and conducting cryptographic calculations, known as a "secure element." *Id.*; Ex[1040] § 2.3.3. Efforts were being made in the art to reduce or eliminate reliance on such hardware secure elements in the phone by, for example, moving some or all of the functionality to a remote server.

B. The '171 Patent

53. The '171 Patent relates to authorization and payment methods on mobile devices. Ex[1001], 1:25-26. It describes "using a mobile computing device in combination with a remotely hosted Secure Element representation to make payments, authorizations or exchange information with other devices." *Id.*, 1:25-30.

54. The '171 Patent explains that in smartcard payment technologies, a "microchip referred to as a 'Secure Element' (SE) is embedded into a payment card, a payment fob, a cell phone, or other mobile devices that may be used for making payments." *Id.*, 1:34-38. SE systems "typically require that the user have physical possession of a card that matches the authorization capabilities of a merchant's system where a purchase is made," which is often "inconvenient." *Id.*, 1:57-62. Thus,

the '171 Patent suggests that “more flexible and convenient systems and methods for authorizing financial transactions” are needed. *Id.*, 1:60-62.

55. Instead of providing for a hardware SE on a mobile device to store a permanent key for generating the message authentication code “cryptograms” discussed above, the proposed improvement of the '171 Patent is essentially to move the SE to a cloud (remote system), and sends only a non-permanent cryptographic key to a mobile device from a remote system, and then the mobile device can use the non-permanent cryptographic key to generate cryptograms requested by a POS terminal during the transaction. *Id.*, Claim 1. The '171 Patent suggests providing “secure application-based participation in a payment card transaction authorization process,” by receiving a non-permanent cryptographic key at a mobile device from a remote system, and using the non-permanent cryptographic key to generate response cryptograms during an interrogation between a POS terminal and the mobile device. *Id.*, Claim 1.

C. Prosecution History Summary of the '171 Patent

56. The '171 Patent was filed as App. No. 13/599,647 on August 30, 2012. Ex[1002], 132. In a Non-Final Office Action mailed on October 6, 2015, the Examiner rejected the pending claims as patent ineligible under 35 U.S.C. § 101 and other grounds. *Id.*, 189-237. In a Response dated March 22, 2016, the Applicant filed new claims 30-58. The Applicant argued the claims differed from conventional

techniques, focusing on the non-permanent key. *Id.*, 278-301. Another round of responses involved similar arguments. *Id.*, 608-621.

57. Following another rejection, the Applicant amended the claims. *Id.*, 794-812. The claims were then allowed. *Id.*, 901-912.

IV. PRIORITY DATE OF THE '171 PATENT

58. The '171 Patent claims priority to a chain of provisional applications – U.S. Provisional App. No. 61/575,846 (“’846 Provisional”), filed August 30, 2011, U.S. Provisional App. No. 61/573,476 (“’476 Provisional”), filed September 6, 2011, and U.S. Provisional App. No. 61/685,863 (“’863 Provisional”), filed March 26, 2012 (collectively “the Provisionals”). Ex[1002], 127. It is my opinion that the earliest priority date Patent Owner can claim is the filing date of the non-provisional on August 30, 2012.

59. I understand that Patent Owner bears the burden of proving the patent claims are entitled to the benefit of priority to the provisional applications by demonstrating that the provisional applications provide the full support required for each claim.

60. It is my opinion that the '171 Patent is not entitled to claim priority to any of the filing dates of the Provisionals, including the '846 Provisional, which is the earliest filed provisional application. For example, all of the '171 Patent's independent claims recite retrieving, using, and re-retrieving a ***non-permanent***

cryptographic key, whereas the '846 Provisional does not disclose any non-permanent or temporary cryptographic key. Ex[1001], Claim 1. Moreover, neither the '476 Provisional nor the '863 Provisional disclose the claimed non-permanent cryptographic key.

61. The '846 Provisional only mentions the word “key” 6 times, none of which discuss a “temporary” or “non-permanent” key, and rather describe a permanent key or an unrelated key for network connection. Ex[1005], [0007], [0039], [0050], [0052], Fig. 9. For example, one reference to “key” in the '846 Provisional describes keys located in a Secure Element (i.e., permanent keys, as explained by Patent Owner during prosecution history, Ex[1002], 291-297). Ex[1005], [0007], [0039]. The same deficiency exists in the '476 Provisional, which added concepts about caching certain static responses to be sent to the POS terminal that do not require calculations using a cryptographic key, but does not contain any new references to or expand on the concept of the “key.” Ex[1004], Fig. 9. Similarly, the '863 Provisional does not add disclosure of a temporary or non-permanent “key.” Ex[1003], [0007], [0064], [0075], [0077], Figs. 9 & 12.

62. It was not until the filing of the non-provisional application to the '171 Patent (No. 13/599,647) that any disclosure of a non-permanent or temporary key

appears.¹ Ex[1001], Claim 1, Claim 17, 27:33-36 (“the term ‘temporary cryptographic key’ refers to a cryptographic key that changes (or is dynamic) from one interrogation to the next over the life of a digital credential (e.g., an SE representation)”); 27:42-46 (“the term ‘cryptographic key’ means a ‘permanent cryptographic key’” and “the term ‘encryption key’ means ‘a permanent cryptographic key’”). Indeed, as explained above, Patent Owner emphasized during prosecution that a non-permanent key was crucial to patentability of the claims, specifically that “the application generates response cryptograms during interrogations based on a non-permanent key that changes between at least two interrogations.” Ex[1002], 289-300.

63. Accordingly, it is my opinion that none of the Provisionals support any of the ’171 Patent’s claims, and the earliest priority date the ’171 Patent can claim is the August 30, 2012 filing date of the ’647 non-provisional.

¹ Indeed, the references to “key” were vastly expanded, with 157 new references to “key,” including references to “temporary key” and “temporary cryptographic key.” *E.g.*, Ex[1001] at 26:33-42, 28:15, 28:47, 28:58, 30:7-13, 30:35-42, 30:65, 40:5-18, 40:63.

V. LEVEL OF ORDINARY SKILL IN THE ART

64. In determining the characteristics of a hypothetical person of ordinary skill in the art (“POSA”) of the ’171 Patent at the time of the claimed invention, I considered several things, including various prior art techniques 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 the 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 that would be necessary to understand the ’171 Patent. I also considered the prior art references discussed below that may indicate the level of skill in the relevant art. Finally, I placed myself back in the relevant period of time, and considered the academics, and engineers that I had worked with in the field.

65. I came to the conclusion that as of August 30, 2012, the characteristics of a person of ordinary skill in the field of art of the ’171 Patent would have been a person with a Bachelor’s degree in Electrical Engineering or Computer Engineering or equivalent knowledge with sufficient mathematical background to understand basic cryptographic techniques, and with two to four years of academic or industry experience in payment systems. 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

66. 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.

67. 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-ADPU 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

68. There are many patents and publications which constitute prior art to the '171 Patent. I have reviewed and considered the following prior art patent and

printed publications, which I believe were all publicly available prior to August 30, 2012. A description of these references follows.

A. Collinge (Ex[1011])

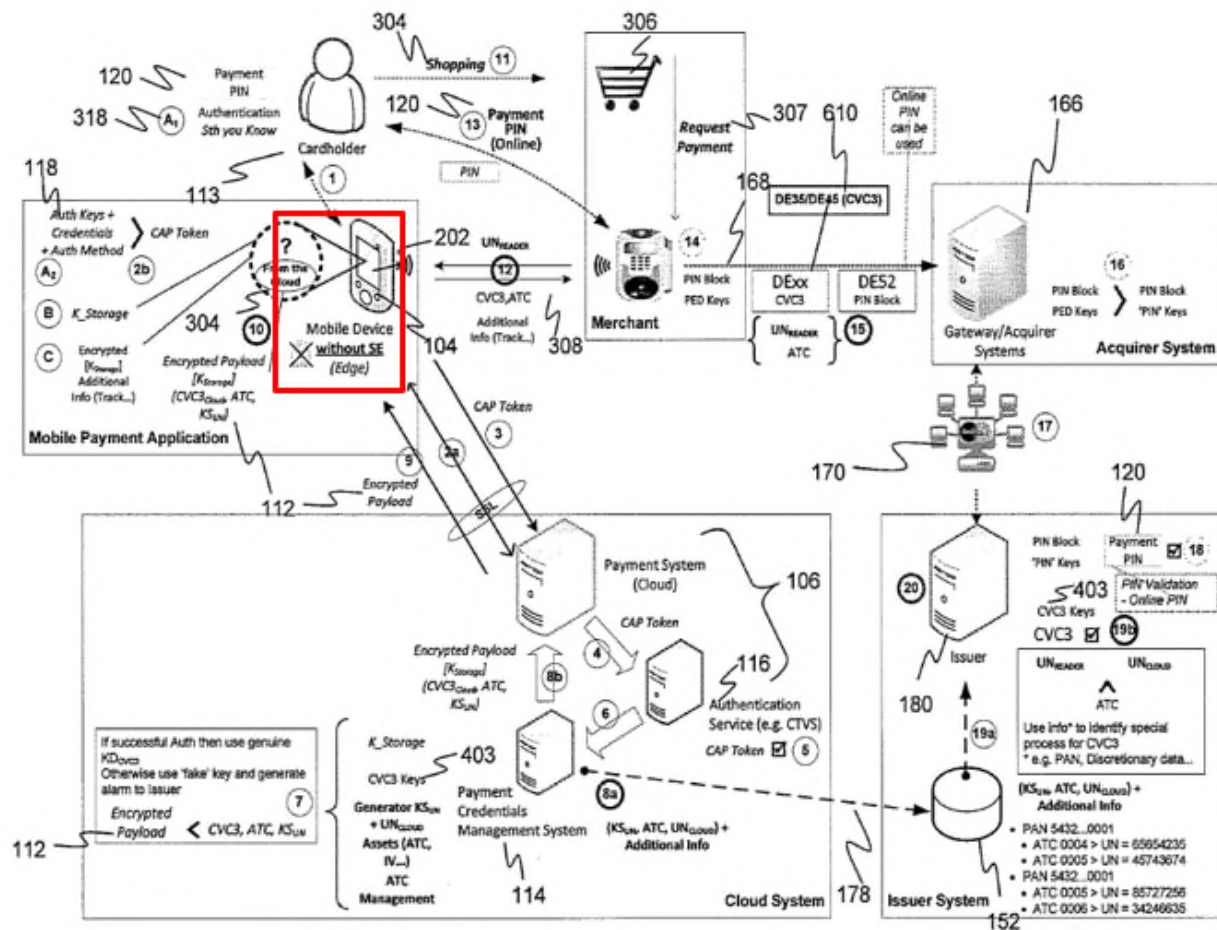
69. As explained below, U.S. Publication No. 2013/0262317A1 to Collinge et al., (“Collinge”) (Ex[1011]) properly claims priority to U.S. provisional applications 61/619,095 filed April 2, 2012 (“’095 Provisional”) (Ex[1009]), and 61/635,248 filed April 18, 2012 (“’248 Provisional”) (Ex[1010]). Ex[1011], Cover. Collinge was filed on March 14, 2013, published on October 3, 2013, and issued as U.S. Patent No. 10,515,359 on December 24, 2019. Ex[1011].

1. Collinge Disclosure

70. Like the ’171 Patent, Collinge relates to financial transactions on mobile devices. Ex[1011], [0001]-[0002]; Ex[1009], [0001], [0003]; Ex[1010], [0001]-[0003]. Collinge enables a “mobile device lacking a secure element to conduct contactless payment transactions.” Ex[1011], [0005]. *See also* Ex[1009], [0002]-[0003]; Ex[1010], [0002]-[0003]. In particular, Collinge teaches a remote system (100) separate from a user mobile device, that generates payment credentials, including a “single use key” transmitted “to the mobile device, wherein the mobile device is not required to have a secure element.” Ex[1011], [0007], [0039], [0043]. The “single use key” is used by the user’s mobile device to “generate a payment cryptogram valid for a single payment transaction.” Ex[1011], [0043]. *See also*

Ex[1009], [0010]; Ex[1010], [0010]. The remote system and the mobile device “may communicate using dual channel communication.” Ex[1011], [0043].

71. Collinge discloses a mobile device including a mobile payment application configured to conduct payment transactions with a POS terminal via NFC without the use of a SE. Ex[1009], [0033] (“[M]obile payment application 104 may be configured to receive and store payment credentials and conduct payment transactions via near field communication without the use of a secure element...”); *see also* Ex[1009], [0002]-[0003], [0075]; Ex[1010], [0002]-[0003].



Ex[1009] Fig. 7 (annotated); *see also* Ex[1011] Fig. 7.

72. “[P]ayment credentials corresponding to the payment account may be stored in a remote-SE (remote-secure-element) system 110 for provisioning to the mobile device.” Ex[1011], [0042]; *see also* Ex[1009], [0061] (Table 1, Steps 1-2); Ex[1010], [0084] (Table 1, Steps 1-2). The mobile device can also receive an encrypted payload from the cloud system. Ex[1011], [0054]-[0055] (“The cloud system 302 may then generate unpredictable numbers, and may generate an

encrypted payload... The encrypted payload may be transmitted to the mobile device 104...”); *see also* Ex[1009], [0038], [0056], Claim 1; Ex[1010], [0047], [0076].

73. A message authentication code cryptogram (e.g., CVC3) is generated using a single use key, KS_{UN} , an unpredictable cryptographic key. Ex[1011], [0043] (“The card profile 116 may include the payment credentials, and the single use key 118 may be a single use (e.g., one-time use) key used to generate a payment cryptogram valid for a single payment transaction.”); *see also id.*, [0009] (explaining the encrypted payload, including KS_{UN} , a session key derived from an unpredictable number and an ATC, may be transmitted to the mobile device), [0013], [0050], [0070], [0077], [0083] (explaining the encrypted payload includes KS_{UN}), [0132]-[0136], Fig. 16, Fig. 17; *see also* Ex[1009], [0056], [0061], [0068], [0071], [0075], Claim 1; Ex[1010], [0047], [0084], [0094], [0095]. The mobile device is configured to transmit the generated payment cryptogram (CVC3) and payment credentials to a POS terminal. Ex[1011], [0044], [0020], [0086]; Ex[1009], [0040], [0044]; Ex[1010], [0050], [0053]. Further, based on Collinge’s references to well-known transaction systems such as “PayPass” Ex[1009], [0002], and terminologies (e.g. “CVC3,” “application cryptogram”), Ex[1011], [0050], a POSA reading Collinge would understand it as disclosing devices, systems, and methods compatible with mainstream contactless payment transactions including EMV transactions.

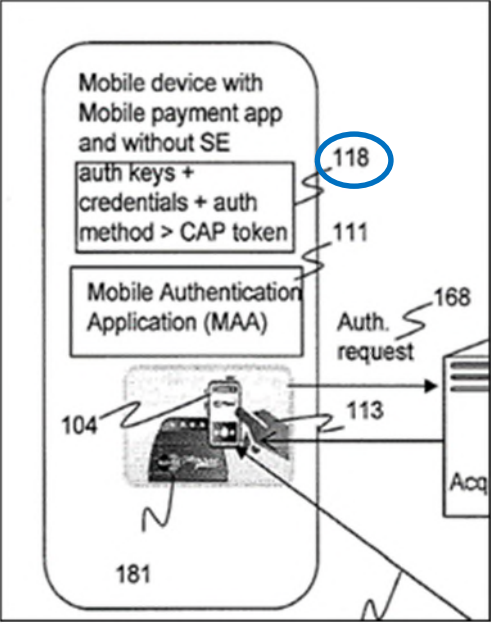
2. Collinge is Supported by its Provisional Applications

74. It is my opinion that the '095 Provisional and the '248 Provisional enable and provide written description support for all elements of at least one independent claim of Collinge.

75. For example, the following chart shows that the earliest filed provisional, the '095 Provisional (Ex[1009]), discloses every limitation of at least claim 20 of Collinge (Ex[1011]):

Collinge (Ex[1011]), Claim 20	Support from '095 Provisional (Ex[1009])
20. A method for generating and provisioning payment credentials to a mobile device lacking a secure element, comprising:	“...processing electronic payments initiated from a mobile device <i>without requiring a secure element (SE)</i> in the mobile device...” Ex[1009], [0001] (emphasis added). <i>“generation of the payment credentials 174 and provisioning of the payment credentials 174 to the MAA 111 is then performed” Id., [0062] (emphasis added).</i> <i>See also id., [0005], [0030], [0037], FIGs. 3-8.</i>
storing, in a database, at least a storage key, a plurality of dynamic card validation code keys, and an application transaction counter associated with a mobile application program;	“At time of the authentication credentials provisioning, <i>a storage key</i> is also stored in the Mobile Payment Application.” <i>Id.</i>, [0061], Table 1, Step A2 (emphasis added). “The cloud-based transaction data generation system 106 also includes a payment credentials management system 114...” <i>Id.</i>, [0038], [0043], [0046], [0065], FIGs. 1, 3-8.

	“System 100 can obtain authentication keys 118, CVC3 keys 403, and payment credentials 174 from a cloud-based transaction data generation system 106 and provisioning the retrieved payment credentials 174 to the MAA 111.” <i>Id.</i>, [0062]. “The principles for the synchronization process (Cloud to Issuer) are: 1. The Cloud_CVC3TRACK2 generation is managed in the Cloud. This encompasses the generation of KSUN and UNCLOUD, and the ATC [application transaction counter] management.” <i>Id.</i>, [0056] (emphasis added). <i>See also id.</i>, [0061], Table 1, Steps 8b-10, [0068], [0071], FIG. 4.
provisioning, to the mobile device, at least the storage key, an authentication component, and static payment credentials, wherein the static payment credentials are associated with a payment account;	“The Authentication component (using MAA technology) has to be provisioned. At time of the authentication credentials provisioning, a storage key is also stored in the Mobile Payment Application. ... At time of the authentication credentials provisioning, static payment credentials are also provisioned.” <i>Id.</i>, [0061], Table 1, Step A2-C (emphasis added). “System 100 can obtain authentication keys 118, CVC3 keys 403, and payment credentials 174 from a cloud-based transaction data generation system 106 and provisioning the retrieved payment credentials 174 to the MAA 111.” <i>Id.</i>, [0062]; <i>see also</i> [0061] (Table 1, Step 2a) (emphasis added).

	“Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below:... Authentication process between Mobile and Cloud to retrieve credentials[:] Identification (Virtual Card Profile ID (which may be any identifier defined by the Issuer and known by the Cardholder (e.g., Masked PAN...)).” <i>Id.</i>, [0068].  <i>Id.</i>, Fig. 1 (annotated).
receiving, from the mobile device, a chip authentication program (CAP) token;	“The Cardholder uses the MAA component of the Mobile Payment Application to generate a CAP Token for the authentication transaction.” <i>Id.</i>, [0061] (Table 1, Step 2b) (emphasis added). <i>See also id.</i>, [0066], [0068].
validating, by a validation device, the authenticity of the received CAP token;	“Mobile Payment Application sends a CAP Token to the Cloud. The Payment System (in the Cloud) validates the CAP Token using a CAP Token Validation Service (CTVS). The

	CTVS validates the CAP Token.” <i>Id.</i> , [0061] (Table 1, Steps 3-5). <i>See also id.</i> , [0066], [0068].
generating, by a processing device, a session key unpredictable number (KSUN);	“The principles for the synchronization process (Cloud to Issuer) are: 1. The Cloud_CVC3TRACK2 generation is managed in the Cloud. This encompasses the generation of KSUN and UNCLOUD, and the ATC management. <i>Id.</i> , [0056] (emphasis added). “Session key generation (KSUN) in the Cloud to bind (ATC, UNCLOUD, PAN and PSN) at the Edge (Mobile Payment Application.” <i>Id.</i> , [0068]. <i>See also id.</i> , [0071] (generation of KSUN).
generating, by the processing device, a cloud unpredictable number (UNCLOUD);	“The principles for the synchronization process (Cloud to Issuer) are: 1. The Cloud_CVC3TRACK2 generation is managed in the Cloud. This encompasses the generation of KSUN and UNCLOUD, and the ATC management. <i>Id.</i> , [0056] (emphasis added). “Session key generation (KSUN) in the Cloud to bind (ATC, UNCLOUD, PAN and PSN) at the Edge (Mobile Payment Application.” <i>Id.</i> , [0068]. <i>See also id.</i> , [0071] (generation of UNCLOUD).
identifying, by the processing device, an encrypted payload based on a derived dynamic card validation code key (KDCVC3), wherein the encrypted payload includes at least a dynamic card	“Upon successful authentication, a genuine KDCVC3 is used and (KSUN, Cloud_CVC3TRACK1/2, ATC) is returned.” <i>Id.</i> , [0061] (Table 1, Step 7).

validation code key of the plurality of dynamic card validation code keys, the KSUN, and the application transaction counter;	“The principles for the synchronization process (Cloud to Issuer) are: 1. The Cloud_CVC3TRACK2 generation is managed in the Cloud. This encompasses the generation of KSUN and UNCLOUD, and the ATC management. 2. (KSUN, Cloud_CVC3TRACK1/2 and ATC) are returned using an encrypted Payload to the Mobile Payment Application.” <i>Id.</i>, [0056] (emphasis added). “Encrypted (using KSTORAGE) Payload sent to the Mobile Payment Application (Valid for one contactless payment transaction)[:] • Cloud_CVC3TRACK1/2 • ATC • KSUN” <i>Id.</i>, [0071]. See also <i>id.</i>, [0071] (generation of Cloud_CVC3TRACK1/2 based on KDCVC3).
transmitting, by a transmitting device, the encrypted payload to the mobile device for use in generating a dynamic card validation code for use in a financial transaction; and	“The principles for the synchronization process (Cloud to Issuer) are: 1. The Cloud_CVC3TRACK2 generation is managed in the Cloud. This encompasses the generation of KSUN and UNCLOUD, and the ATC management. 2. (KSUN, Cloud_CVC3TRACK1/2 and ATC) are returned using an encrypted Payload to the Mobile Payment Application.” <i>Id.</i>, [0056] (emphasis added). “(KSUN, Cloud_CVC3TRACK1/2, ATC) is returned to the front-end of the Cloud system for delivery to the Mobile Payment

	Application.” <i>Id.</i>, [0061] (Table 1, Step 8b) (emphasis added). “The Mobile Payment Application use a specific process to generate the CVC3 using (KSUN, Cloud_CVC3TRACK1/2, ATC and UNREADER).” <i>Id.</i>, [0061] (Table 1, Step 12) (emphasis added). “Encrypted (using KSTORAGE) Payload sent to the Mobile Payment Application (Valid for one contactless payment transaction)[:] • Cloud_CVC3TRACK1/2 • ATC • KSUN” <i>Id.</i>, [0071].
transmitting, by the transmitting device, at least the KSUN, UNCLOUD, and application transaction counter to an issuer associated with the payment account for use in validating the generated dynamic card validation code used in the financial transaction.	“The Issuer has a mean to identify transaction that requires additional processing for CVC3 validation when the solution using SE-less Mobile Contactless Payment is used. Using the ATC provided in the Payment Transaction, the Issuer is able to retrieve the UNCLOUD and KSUN values that were used by the Payment Credential Management System to generate the CVC3 value.” <i>Id.</i>, [0061] (Table 1, Step 19a); <i>see also id.</i> [0071]-[0074] (emphasis added). “Payload sent to the Issuer[:] • Identifier (PAN...) • UNCLOUD • ATC • Authentication Status Info + Additional Generation Information (e.g., Validity)” <i>Id.</i>, [0071].

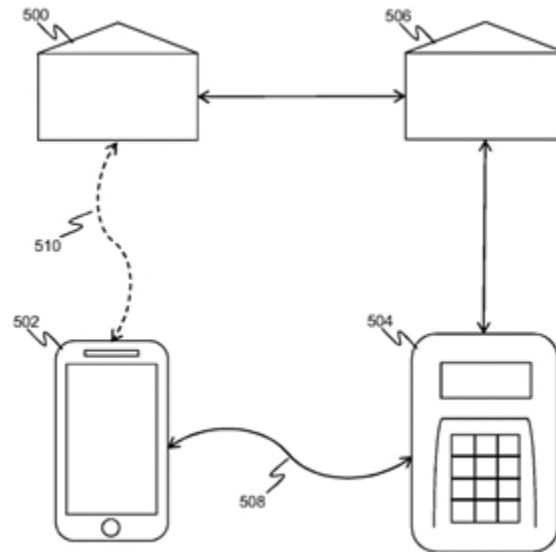
B. Fiske (Ex[1012])

76. U.S. Patent No. 11,080,693 to Fiske, (“Fiske”) properly claims priority to PCT/GB2012/050737 filed on April 2, 2012. Ex[1012] at 1. Fiske was filed on October 4, 2013, and issued on August 3, 2021. Ex[1012] at 1.

77. Fiske relates to methods and systems for authorizing an EMV payment transaction between a user device and a POS terminal, where a secure element (SE) is not available for use by a payment application. Ex[1012], Abstract, 1:19-22. Fiske discloses the public availability of, and explicitly incorporates by reference, EMV transaction protocols based on EMV 4.2 Specifications or EMV Contactless Specifications. Ex[1012], 1:58-64 (“Many electronic payment systems use the EMV ... transaction protocols, as defined for example in the EMV 4.2 Specifications or the EMV Contactless Specifications for Payment Systems, which are publicly available and published by EMVCo LLC.”), 6:54-61, 9:6-11; *see also* Exs[1019]-[1029].

78. Fiske teaches a mobile payment application on a device 502 that can interact with a POS terminal 504, over a first communications channel (e.g., contactless communication interface 508”) for digital credential data. *See* Ex[1012], 2:18-26, 11:38-40 (“The user of device 502 can interact with a terminal 504 at a PoS via user device 502 in order to make a purchase from a merchant.”), 11:45-48

(“...the user device 502 can communicate with the PoS terminal via contactless communication interface 508), Fig. 5:



79. Fiske discloses that the “[u]ser device 502 is further capable of communicating with issuing bank 500 via communications interface 510.” Ex[1012], 11:49-50. Fiske discloses that the communications interface 510 can be wireless. Ex[1012], 11:53-57, 13:59-67, 17:52-61. As explained in [1.A-3], Fiske discloses that the application on the user device can request data associated with the account, such as payment keys, which are associated with an account at the issuing bank. Ex[1012], 12:45-52, 12:50-57, 13:17-24, 13:20-31, 13:63-67.

80. In particular, Fiske teaches a user device that receives a single-use session key from an issuing bank for a single payment transaction. Ex[1012], 9:59-65, 13:32-35; *see also id.*, 4:1-9, 8:30-39, 13:25-50, 14:1-20, Fig. 4. The session

key is used to generate a message authentication code “application cryptogram,” which is required during an EMV transaction. Ex[1012], 13:20-24, 13:32-35.

VIII. GROUNDS OF INVALIDITY

A. Grounds 1 and 2: Claims 1-33 Are Anticipated and Rendered Obvious by Collinge in View of Knowledge of a POSA

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:”

81. To the extent the preamble is limiting, Collinge discloses this limitation. Collinge discloses securely conducting payment transactions using a mobile device running a payment application, communicating using NFC technology and other communication mechanisms. Ex[1011], [0002]-[0003], [0040]-[0041] (“[M]obile device 103 may include a mobile payment application” “configured to...conduct payment transactions via near field communications without the use of a secure element...”), [0044] (“secure transmission of information via NFC...”), [0125]; *see also* Ex[1009]², [0001], [0005], [0009], [0030]. The system is used to perform a payment transaction, including requesting an

² In addition to providing provisional support for the disclosures of the Collinge Publication relied upon herein, the provisional application is incorporated by reference into the Collinge Publication. Ex[1011], Cover.

authorization and obtaining an authorization response. Ex[1011], [0044] (“The mobile device 104 may be further configured to transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 at a merchant.”), [0045] (“The payment network 124 may then submit an authorization response to the acquirer 122 and/or the merchant, who may then finalize the payment with the user 102.”).

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

82. Collinge discloses at a mobile device, executing a mobile payment application in an operating system of the mobile device. See Ex[1011], [0041], [0118]-[0119]; *see also* Ex[1009], [0061] (Table 1, Step 1), [0033], [0039].

c. [1.A-2]: “the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and”

83. The '171 Patent explains interrogation refers to querying or extraction of information. Ex[1001], 6:3-5 (“[c]ards containing an SE are typically presented to...[a] reader device as the interrogator that extracts information from the card”), 6:50-53 (“‘Commands’ are sometimes referred to as ‘queries’ because they originate from an ‘interrogator,’ which has a querying connotation.”), 10:58-65 (“In the case where the SEs in an array of SEs are database secure element representations, a SE card reader is not needed to

interrogate the SE representations. In such systems the data may be acquired by using an electronic processor...”). Further, 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.

84. Collinge’s mobile application is interrogable by an electronic reader, such as the POS terminal, over a first communications channel (e.g., NFC) for digital credential data. *See* Ex[1011], [0044] (“The mobile device 104 may be further configured to transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 at a merchant. The point-of-sale terminal 120 may be any type of point-of-sale terminal or device suitable for receiving payment credentials via near field communication (NFC).”), [0070], [0086] (“At stage 14, the point-of-sale terminal 120 may execute standard NFC payment transactions processes as will be apparent to persons having skill in the relevant art.”), [0120] (“In step 1406, a NFC payment method may be executed between the user 102, the mobile device 104, the mobile payment application 106, and the point-of-sale terminal 120.”), Fig. 14; *see also* Ex[1009], [0014], [0030] (“while the exemplary POS terminal 181 is depicted as a MasterCard PayPass® terminal, other contactless POS terminals 181 with NFC capabilities can be used”), [0033] (“any mobile

computing device 104 having near field communications (NFC) capabilities to make purchases with a payment account”), [0040], [0060]-[0062].

85. To the extent that Collinge does not disclose interrogation, a POSA would understand that “interrogation” is an obvious way to implement Collinge’s NFC disclosure Collinge explains that “the point-of-sale terminal 120 may execute standard NFC payment transactions processes” Ex[1011], [0086]. A POSA would understand that standard NFC payment transactions entails interrogation of the payment token (payment card, mobile payment application) by a POS reader. Ex[1015], [0062], [0070].

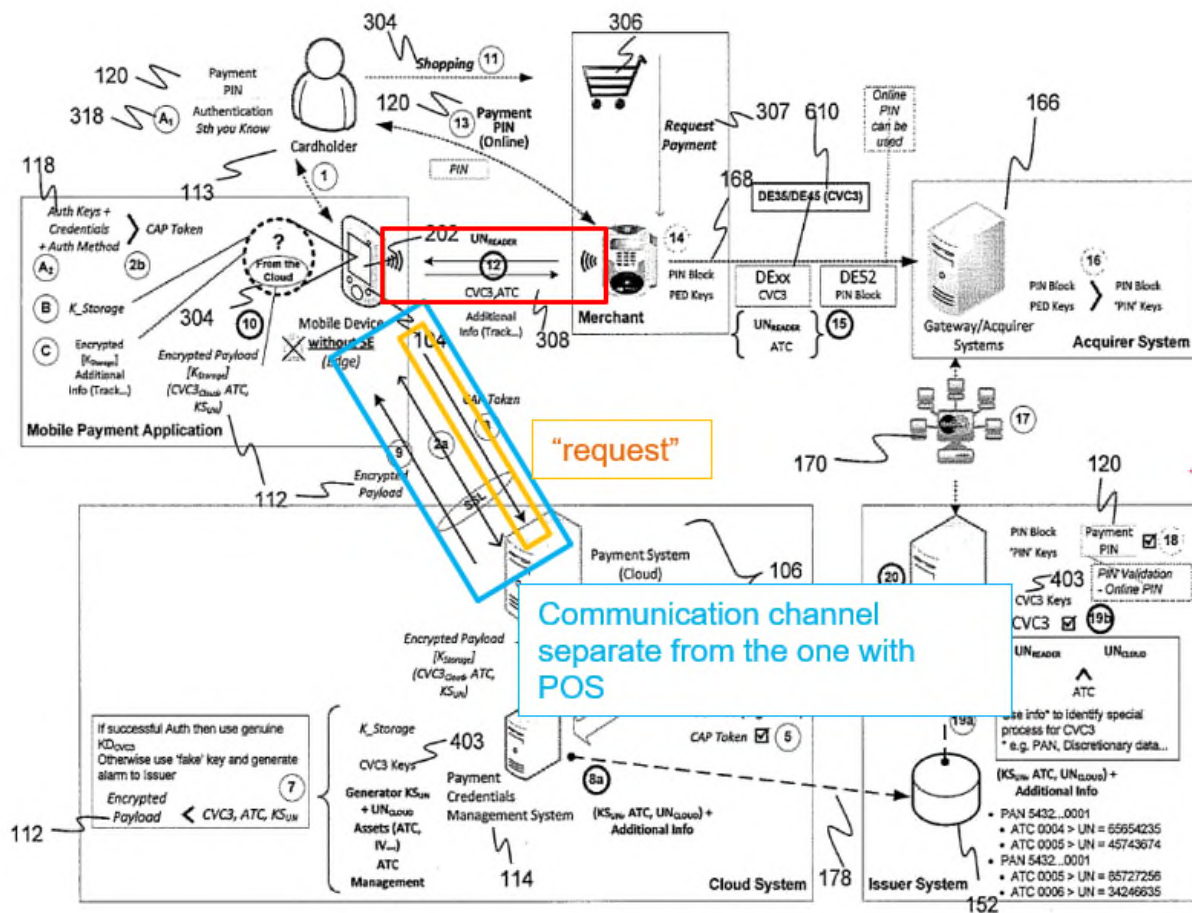
86. As explained, a POSA reading Collinge will understand its disclosure as compatible with mainstream contactless payment transactions including EMV transactions. *Supra* § VII. It was well known that in an mainstream EMV transaction, a “card application” runs in a payment “Card,” and the POS terminal’s application “sends commands as a client to the card application, which responds as a server.” Ex[1037] at 47-48. The POS will select an application on a “Card,” such as a Mastercard or Visa transaction, Ex[1023] § 5.8.2; Ex[1026] § 2.3.3-2.3.4, Ex[1027] § 2.4.1, and the application on the “Card” will return “digital credential data”—data necessary for approval of a transaction, Ex[1001], 7:3-7, including account information (*e.g.*, PAN) and Application Cryptogram (or equivalently, a CVC3 cryptogram). 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[1026] §§ 3.4.2, 3.5.1–3.5.3, 5.8.3; Ex[1021] at § III, § 7.2, 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”), 5.2.2.3, 5.4.3.2.

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”

87. Collinge discloses that “[p]ayment credentials corresponding to the payment account may be stored in a remote-SE (remote-secure-element) system 110 for provisioning to the mobile device.” Ex[1011], [0042], [0071] (“If there are no single use keys 118 remaining, then, the method 500 may return to step 510 where connection may be made with the remote-SE system 110 and a new single use key 118 provisioned to the mobile device 104”), Fig. 7; *see also* Ex[1009], [0061] (Table 1, Steps 1-2: The Cardholder “uses a SE-less Mobile *PayPass* Payment Application,” and the “Cardholder connects to the Cloud to retrieve Payment Credentials.”). Further, “the mobile payment application 106 may transmit the generated CAP token to the remote-SE system 100,” Ex[1011], [0081], which causes the remote-SE system to generate and return payment credentials in an encrypted payload after

verification of CAP token, *id.* [0082]-[0083], [0085]. A POSA would understand that sending of CAP token initiates, and thus constitutes a request for server to return payment credentials. Further, as shown in Collinge Fig. 7, the communication between the remote/cloud system to the phone is a different (second) communication channel (e.g., SSL/TLS) from the channel used to communicate with the POS reader/merchant (first communication channel, shown by the near-field communication symbols). *See* Ex[1011], Fig. 7, [0043] (regarding dual channel communication between the mobile device and remote system), [0058] (dual-channel communication), [0150] (regarding suitable networks, including LAN, WiFi, WAN, satellite, Internet, etc.); *see also id.*, [0035] (“[t]he communication links depicted in the system 100 between the various components can be through public and/or private networks or virtual private networks (e.g., the Internet and mobile networks particularly with respect to communications with mobile device 104, and private networks such as payment processing network 170).”). *See* Ex[1011], Fig. 7 (annotated), [0081] (connection with cloud system via SSL authenticated session), [0085] (communicate with POS terminal via NFC):



88. To the extent Collinge does not explicitly disclose that the application would request a first set of data from the remote computer system, in light of the fact that such data is retrieved from a remote system, a POSA would have found it obvious to configure the mobile application to request it as that was one of a finite number of predictable ways to retrieve data. Ex[1011], [0082], [0083]. Moreover, it would be a waste of bandwidth and resources for the issuer to push information regardless of the status of the user device. In addition, because Collinge discloses keys that are single-use keys, which need to be replenished as they are used, it is

obvious that, for security reasons, a POSA would want to limit the number of keys on the mobile device that could be compromised in case the mobile is hacked, and thus, it would have been obvious for the device to pull or request the data from the issuer.

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”

89. Collinge discloses that “the mobile device 104 may ... transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 ... via near field communication (NFC).” Ex[1011], [0043]; *see supra* § [1.A-3]; Ex[1011], [0085], [0043] (“[C]ard payment profile 116 may include the payment credentials, and the single use key 118 may be a single use (e.g., one-time use) key used to generate a payment cryptogram valid for a single payment transaction ... remote-SE system 110 and the mobile device 104 may communicate using dual channel communication...”); *see also* Ex[1009], [0061] (Table 1, Step 15), [0044] (“cryptogram 178 may be generated using key management services (i.e., through CVC3 validation, including dynamic CVC3 validation).”), [0056], [0068] (“Session key generation (KS_{UN}) in the Cloud to bind (ATC, UN_{CLOUD} , PAN, and PSN) at the Edge (Mobile Payment Application)”).

90. The application does not access a permanent cryptographic key issued for the digital credential because the CVC3 cryptogram is generated using a single use key, “session key” (KS_{UN}) in the card profile. Ex[1011], [0043] (“The card profile 116 may include the payment credentials, and the single use key 118 may be a single use (e.g., one-time use) key used to generate a payment cryptogram valid for a single payment transaction.”), [0050], [0070], [0077], [0085], [0136], [0145] (“device may generate a payment CVC3 value based on at least ... the session key unpredictable number ... the generated payment CVC3 value... may be transmitted, via near field communication to the point-of-sale terminal 120 for including in an authorization request in a financial transaction”), Fig. 16; *see also* Ex[1009], [0056] (“The Cloud_CVC3_{TRACK1/2} generation is managed in the Cloud. This encompasses the generation of KS_{UN} and UN_{CLOUD} and the ATC management. (KS_{UN} , Cloud_CVC3_{TRACK 1/2} and ATC) are returned using an encrypted Payload to the Mobile Payment Application”), [0068] (“Session key generation (KS_{UN}) in the Cloud to bind (ATC, UN_{CLOUD} , PAN, and PSN) at the Edge (Mobile Payment Application)”), [0071] (disclosing KS_{UN} , a non-permanent cryptographic key, which is included in an encrypted payload and is generated by UN_{CLOUD}), [0075] ($UN_{UNpredictable}$ Number”), Claim 1 (an encrypted payload, “comprising at least one of a session key generated using an unpredictable number (KS_{UN})...”). It is well understood in the art that the “session key” (KS_{UN}) is unique to each

transaction because it is generated based on the ATC (Application Translation Counter) and changes with each transaction. Ex[1009], [0071] (“KS_{UN}” section).

91. A POSA would also find it obvious to implement Collinge in the manner described above because using a “Session Key” generated from ATC (hence, unique to each transaction and non-permanent) to generate a cryptogram in a transaction was a standardized operation in secure payment transactions, and thus entailed applying a known technique (changing cryptographic key) to yield predictable results (improved resistance to security attacks). Ex[1020] §§ 8.1.2.2, A1.2, A1.3, D3.

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;”

92. As explained in [1.A-3] above, Collinge discloses this element, where a first set of data is the digital credential associated with the account.

93. A POSA would also have found it obvious to configure the mobile application to make a request, either together with transmitting a CAP token or separately (e.g., before transmission), for purposes of efficiency and resources, as explained in [1.A-3].

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 ... 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;”

94. As explained in [1.A-3] above, Collinge discloses that the mobile payment application can receive an encrypted payload and payment credentials from the cloud system over a wireless network. Ex[1011], [0009], [0013], [0083], [0141]. The encrypted payload can include a “single use key,” including a generating key for generation of CVC3 cryptogram or Application Cryptogram. Ex[1011], [0050]. The generating key may be a KS_{UN} , Ex[1011], Fig. 17; *see also* Ex[1009], [0068] (“CVC3_{TRACK1/2}” section describing CVC3 generation using KS_{UN}), which is non-permanent (unique to each transaction) and associated with the account because it is generated in response to an account-specific request, Ex[1011], [0082]-[0083], and uses the account-specific ATC (Application Transaction Counter) in its generation, Ex[1009], [0068] (“ KS_{UN} ”).

95. It is well known in the art 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 and it would be obvious to implement Collinge in this way to ensure

interoperability with EMV-standardized devices. Ex[1037] at 46-48; Ex[1021] § 6.5.

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

96. As explained in [1.C], KS_{UN} is a non-permanent cryptographic key associated with the account. KS_{UN} is transmitted to the mobile device as part of an encrypted payload, is used by the mobile device to generate a cryptogram (CVC3) and as such, KS_{UN} is locally stored in the mobile device. Ex[1011], [0009] (explaining the encrypted payload, including KS_{UN} , may be transmitted to the mobile device), [0083] (explaining the encrypted payload includes KS_{UN}), [0085] (“[T]he encrypted payload may be...stored in the storage.”), Fig. 17; *see also* Ex[1009], [0061] (Table 1, Step 10: “(KS_{UN} , Cloud_ CVC3_{TRACK 1/2}, ATC) and the additional assets are stored.”).

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

97. As explained in [1.A-2], Collinge discloses the application participating in an interrogation between a POS terminal and the mobile device.

(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;”

98. Collinge explains that at the purchase stage, “[t]he point-of-sale terminal may generate a reader unpredictable number (UN_{READER}) and transmit the UN_{READER} to the mobile payment application 106, which may then generate the payment CVC3 value using the information in the encrypted payload and the UN_{READER}.” Ex[1011], [0085], [0145]. The communication between the POS terminal and mobile device is over a first communications channel (e.g., NFC). Ex[1011], [0002]-[0003], [0044].

99. Because the POS terminal generates an unpredictable number for the mobile device to generate the cryptogram (CVC3), and the mobile device generates CVC3 in response to that communication from the POS terminal, a POSA would understand the communication from the POS terminal containing the unpredictable number is a command or request for the mobile device to generate the cryptogram. This is also consistent with standardized EMV transactions, (with which a POSA reading Collinge will understand its disclosure as compatible, *supra* § VII), where the mobile device (“Card”) generates an application cryptogram in response to a

COMPUTE CRYPTOGRAPHIC CHECKSUM, GENERATE AC, or GPO command. Ex[1026] §§ 3.4.2, 3.4.3, 5.2, 5.3; Ex[1027] § 2.4.1.

100. The cryptogram and other data is “digital credential data” necessary for approval of transactions because the POS device will later “generate an authorization request for the payment transaction, which [will] include the UN_{READER}, the generated CVC3 value, [and] the application transactions counter” Ex[1011], [0138]. The communication between the POS terminal and mobile device is over a first communications channel (e.g., NFC). Ex[1011], [0002]-[0003], [0044] (“point-of-sale terminal 120 may be any type of point-of-sale terminal or device suitable for receiving payment credentials via near field communication (NFC)”).

101. A POSA would also have found it obvious to implement Collinge in the manner described above because these are standardized operations in secure payment transactions and are therefore applying a known technique (using EMV standard POS-card messaging) to yield predictable results (permitting EMV terminal to assemble an authorization request/payment message for transmission).

(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”

102. Collinge explains that the mobile device sends a generated payment cryptogram and payment credentials to the POS terminal. Ex[1011], [0044] (“mobile device 104 may be further configured to transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 at a merchant”), [0055], [0070], [0077]; *see also* Ex[1009], [0061] (Table 1, Step 15), [0064]. “The payment cryptogram may be, for example, an application cryptogram or a dynamic card validation code (CVC3).” Ex[1011], [0077]; *see also* Ex[1009], [0044]. The mobile payment application “generate[s] the payment CVC3 value using the information in the encrypted payload and the UN_{READER} .” Ex[1011], [0085]. As explained in [1.C] and [1.D], the encrypted payload can include KS_{UN} , an unpredictable cryptographic key, which is locally stored. Ex[1011], [0009], [0013], [0083] (“As part of the encrypted payload, the payment credentials management system 704 may generate a session key unpredictable number (KS_{UN})...”), [0085] (“At stage 10, the encrypted payload may be decrypted using the K_{STORAGE} and stored in the storage 304”), Fig. 17; *see also* Ex[1009], [0061].

103. A single-use key, such as KS_{UN} to generate a cryptogram results in a cryptogram that does not include the single-use key. Ex[1034], 17-18 (explaining message authentication code (MAC) generation); Ex[1039] (showing single-use key is not present in the MAC/cryptogram).

104. A POSA would find it obvious to implement Collinge in the manner described above because these are standardized operations in secure payment transactions and are therefore applying a known technique (MAC computation using key known only by both parties) to yield predictable results (e.g. allowing issuer to verify card authenticity).

(3) [1.E-3]: “responding to the at least one POS command communication ... 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;”

105. As explained above, the R-APDU Term here (“at least one response application data protocol unit containing the response cryptogram and an account identifier for the account”) is potentially subject to two alternative constructions. *Supra* § V. However, under either construction, it is my opinion that the Term is disclosed or rendered obvious by Collinge.

106. As explained in [1.E] and [1.E-1], the card (or device) being interrogated would respond to a command APDU (C-APDU) from the POS terminal with response APDU. As explained in [1.A-2], the application on the mobile device interacts with the POS terminal, over a first communications channel (e.g., NFC). Ex[1011], [0002]-[0003], [0044].

107. As explained in [1.A-2], [1.E-1], and [1.E-2], Collinge discloses that the mobile device sends payment credential data, which a POSA would understand to include generated payment cryptogram and other “common payment credential information,” such as account information (e.g., PAN),³ to the POS terminal in response to a POS communication. *See supra* [1.A-2], [1.E-1], [1.E-2]; *see also* Ex[1011], [0044], [0055], [0070], [0077]; Ex[1009], [0061] (Table 1, Step 15), [0064]. A POSA would understand that this can be implemented in the manner directed by either Construction 1 or Construction 2. *Supra* § V.

108. Alternatively, under Construction 1, where the Term could mean one or more APDUs collectively containing the response cryptogram and an account identifier for the account, this is satisfied by Collinge’s reference to PayPass card

³ The term “account identifier” is not defined in the ’171 Patent’s specification, but a POSA would understand that in the very least, an account number, such as a PAN, is an account identifier.

specification in the provisional application, incorporated by reference. Ex[1009], [0003], [0029]-[0032], [0040], [0061]. It is understood in the art that during a Mastercard interrogation, the “Card” (user device) would provide, in R-APDUs, account information such as a Primary Account Number (PAN) in response to a READ RECORD command, and a response cryptogram (CVC3 or Application Cryptogram) in response to a COMPUTE CRYPTOGRAPHIC CHECKSUM or GENERATE AC command APDU. Ex[1026] §§ 3.4.2, 3.4.3, 3.5.1–3.5.3, 5.2, 5.3.1.

109. Further, because a POSA reading Collinge will understand its disclosure as compatible with EMV transactions, *supra* § VII, it would have been obvious to a POSA to implement Collinge to carry out EMV transactions to expand their market opportunity by allowing interoperability with existing and expected future payment infrastructure. Under Construction 1, as explained above, a Mastercard transaction would satisfy this element. Further, in an EMV mode contactless Visa transaction, the POS Kernel 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). Ex[1027] § 2.4.1, Table E-6. The “Card” may return an ARQC Application Cryptogram in the ***same message*** in response to the GPO command. Ex[1027] §§ 2.4.1, 5.2.2.3, 5.4.3.2. Therefore, either Mastercard or Visa transaction, carried out using Collinge’s invention, would satisfy this claim element.

110. Under Construction 2, the Term could refer to one or more APDUs, each of which contains **both** the response cryptogram and an account identifier for the account. *Supra* § V. As explained above, a EMV mode Visa transaction would also satisfy this claim element. Ex[1027] §§ 2.4.1, 5.2.2.3, 5.4.3.2.

j. [1.F]-[1.G]: “... requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account ... comprising a second non-permanent cryptographic key associated with the account; and”

111. As explained in [1.A-3], Collinge discloses that the “set of data associated with the account” may include generating key for generating CVC3 (KS_{UN}) in an encrypted payload. As further explained in [1.A-4], the generating key for generating CVC3 or KS_{UN} is a non-permanent, single-use key generated for the session. Therefore, a new KS_{UN} will be required for a subsequent transaction for the same reason as discussed in [1.A-3], [1.B], and [1.C]. Ex[1011], [0013], [0083], [0140], Fig. 17; *see also* Ex[1009], [0068], [0071]. It would thus be natural that the new KS_{UN} for a subsequent transaction would be requested subsequent to a prior transaction, which consumed the KS_{UN} for the prior transaction. In other words, the “second set of data” in a given transaction may correspond to the “first set of data” [1.A-3] of a subsequent transaction. Therefore, by disclosing [1.A-3], [1.B], and [1.C], Collinge discloses these elements.

112. A POSA would also find it obvious to request and receive the “second set of data” to be used as the “first set of data” for next transaction, because otherwise the “second set of data” would be unused, and the request thereof would be meaningless and wasteful. Additionally, a POSA would find it obvious to request a new KS_{UN} once a prior KS_{UN} had been used, to ensure additional transactions could be conducted.

k. [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.”

113. For the reasons discussed in [1.D], [1.F], and [1.G], Collinge discloses this element. Indeed, as explained earlier, the local cryptographic key KS_{UN} must be stored in a local memory because the cryptogram is generated by the application on the phone, as explained in [1.E-2].

2. Claims 2 and 18: “wherein the mobile device is an NFC emulating device, wherein ... data associated with the account are received via a data connection over the internet”

114. Collinge discloses this element. 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. Collinge discloses that the mobile device could be an NFC emulating device, i.e., the mobile device would act as a contactless payment card, for example, where the first communications channel

is an NFC communications channel. *See* Ex[1011], [0044] (regarding NFC communication between the mobile device and POS terminal), [0070] (“mobile device 104 may conduct a contactless/NFC payment transaction using the mobile payment application 106...”), [0086], [0120], [0150], Fig. 14; *see also* Ex[1009], [0014] (“provisioning payment credentials from a Cloud-based system using a ‘mobile cloud account’ to an NFC-enabled mobile device”), [0033], [0053].

115. For reasons discussed in [1.C] and [1.G], Collinge discloses the first set of data associated with the account and the second set of data associated with the account can be received via a data connection over the internet. *See also* Ex[1011], [0150] (“The network may be any network suitable for performing the functions as disclosed herein and may include [...] a wireless network (e.g., WiFi), a mobile communication network, a satellite network, the Internet.”).

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

116. Collinge discloses this element. The '171 Patent describes “hash” as “[e]ncrypted data that cannot be un-encrypted,” Ex[1001], 25:39-40. It is well known in the art that the response cryptogram (CVC3) is a hash of a multiple block message and is a hashed message authentication code in the Mastercard payment network. Ex[1009], [0071]; Ex[1011], [0085] (“point-of-sale terminal may generate a reader unpredictable number (UN_{READER}) and transmit the UN_{READER} to the mobile payment application 106, which may then generate the payment CVC3 value using

the information in the encrypted payload and the UN_{READER}”). Additionally, the provisional application, incorporated by reference in Collinge, explains that the CVC3 is the “two least significant bytes” of a cryptographic (DES3) computation using single-use key KS_{UN}. Ex[1009], [0071] (“CVC3_{TRACK1/2}” section). It was well understood in the art that this results in loss of information in the input data, making it impossible to de-crypt. Ex[1034], 17-18. Accordingly, Collinge discloses this element because CVC3 is a hash.

4. 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”

117. Collinge discloses this element. The provisional application, incorporated by reference, expressly references making transactions compliant with the PayPass card specification. Ex[1009], [0003], [0029]-[0032], [0040]. Collinge also refers to “m/chip payment transactions,” which a POSA would understand to refer to known payment system specifications defining sets of inputs and responses. Ex[1011], [0044].

118. Further, a POSA would have found this limitation obvious, at least because card specifications were well known in the art and a POSA would be motivated to make their systems compliant with such specifications including

Mastercard Paypass or EMV Specifications to expand their market opportunity by allowing interoperability with existing and expected future payment infrastructure.

5. 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”

119. For reasons stated above, it would have been obvious for a POSA to implement Collinge in a way compliant with specifications such as EMV Specifications, because a POSA reading Collinge will understand its disclosure as compatible with EMV transactions. *Supra* § VII. However, it would not be clear to a POSA what this claim element means by reciting responding to a request for a first cryptogram with a second cryptogram. To the extent that the claim element means responding to a request for a second cryptogram after a request for a first cryptogram, the EMV Specifications disclose 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.*

120. On the other hand, to the extent the claim element means responding to the same (first) request for cryptogram with a cryptogram not requested, the EMV Specifications also disclose this. For example, in response to a first request for

cryptogram (GENRATE AC or GPO) from the POS terminal requesting for an approval (TC) cryptogram, a “Card” may respond with a decline (AAC) cryptogram if it decides that the transaction should be declined, or with an ARQC if it decides that online approval from issuer would be required. Ex[1021] § 9.3.1.

6. 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”

121. It was common knowledge in the art that a response cryptogram like CVC3 is generated using DES calculation because it is the predominant symmetric encryption algorithm in financial applications—specifically, triple DES (DES executed three times). Ex[1034], 17-18 (explaining that message authentication code (MAC) is generated by DES); Ex[1016], [0053] (explaining CVC3 is a MAC); *see also* Ex[1011], [0085], Ex[1009], [0071] (“CVC3_{TRACK1/2}” section), [0075] (disclosing DES and DES3), Claim 2 (“wherein the cryptographic process uses the triple Data Encryption Standard (DES) algorithm to generate the CVC3 value and wherein transaction data comprises the CVC3 value”). Because only 2 bytes of the longer cryptogram are included in the response, the response includes less than the entire output. *Id.*

122. A POSA would find it obvious to use DES calculation to encrypt inputs and take the two bytes from the output to derive the response cryptogram, Ex[1009],

[0071] (“CVC3_{TRACK1/2}” section), which is standard operation in the industry, thus applying a known technique to yield predictable results. Ex[1020] §§ 8.1.2, A1.2, A1.3, B1.1.

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

123. As explained in [1.A] and [1.E-1], the interrogation between the mobile device and the POS terminal does not require wireless network connectivity, and indeed, occurs on a communications channel separate from the wireless network used to communicate with the cloud.

124. A POSA would have understood that in many situations, the mobile device would not have connectivity to the wireless network when interrogated by a POS terminal, such as when the POS terminal is in a facility below ground (e.g., transit), in a geographic area with poor cellular service, or for other reasons.

8. Claim 8

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

125. For the reasons discussed in [1.A] and [1.A-3], Collinge discloses this limitation.

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”

126. For the reasons discussed in [1.A-3], [1.B], [1.C], and [1.E-3], a POSA would have understood or found it obvious that Collinge discloses this limitation.

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.”

127. For the reasons discussed in [1.F] and [1.G], Collinge discloses this limitation.

9. 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”

128. For the reasons discussed in [1.B], Collinge discloses this limitation. Collinge discloses that “[p]ayment credentials corresponding to the payment account may be stored by a remote-SE (remote-secure element) system 110 for provisioning to the mobile device.” Ex[1011], [0042]; *see also* Ex[1009], [0061].

10. 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:”

129. To the extent the preamble is limiting, Collinge discloses this limitation. For example, Collinge discloses performing an authorization process at a payment network. Ex[1011], [0045] (submitting the authorizing request for payment transaction at a payment network), [0056]-[0057], [0086]-[0087]; *see also* Ex[1009], [0061] (Table 1, Steps 14-15).

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;”

130. Collinge discloses that the “point-of-sale terminal 120 may generate an authorization request for the payment transaction, which may include the UN_{READER}, the generated CVC3 value, [i.e. response cryptogram], the application transaction counter...” Ex[1011], [0086]-[0087]; *see also* Ex[1009], [0061] (Table 1, Step 19a-19b), [0073]-[0074]. Additionally, Collinge explains the POS terminal “may transmit the received payment information [from the mobile device] and any additional transaction information.” Ex[1011], [0077]. The authorization request would include an account identifier as that was a standard part of any authorization message, including the standard “m/chip” or mag stripe message mentioned in

Collinge. Moreover, Collinge explains that the authorization response includes determining whether the transaction is authorized based on “available ... credit, etc. for the payment account”, and thus a POSA would understand the authorization request to contain the account identifier. Ex[1011], [0077].

131. To the extent not disclosed, a POSA would find it obvious that the authorization request would include a response cryptogram and an account because this is well established standard practice in the art and would be an obvious way to permit the issuer to authorize the transaction and associate it with the correct account. Ex[1037] at 57-58.

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

132. Collinge discloses that “the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER} , UN_{CLOUD} , and application transaction counter,” by retrieving (“determining”) the UN_{CLOUD} and KS_{UN} (hence the session key associated with the account and unique to transaction, as explained in [1.A-3]) values that were used by the Payment Credential Management System to generate (“calculating”) the CVC3 value. Ex[1011], [0087]; *see also* Ex[1009], [0061] (Table 1, Step 19a-19b) (during the “additional processing for CVC3

validation,” the Issuer is “able to retrieve the UN_{CLOUD} and KS_{UN} values that were used by the Payment Credential Management System to generate the CVC3 value.”). Because this CVC3 value is calculated using the same input and key—hence would be the same as—the CVC3 value included in the authorization request if the request originated from an authentic card, a POSA would understand that the “verifying” would simply involve comparing whether those two CVC3 values are the same. Ex[1037] at 58.

133. To the extent the foregoing is not disclosed, as Collinge has acknowledged, “[m]ethods for validating a cryptogram will be apparent to persons having skill in the relevant art,” Ex[1011], [0077], and a POSA would find it obvious to implement Collinge in the manner described above because these are standardized operations in secure payment transactions and are therefore applying a known technique to yield predictable results.

d. [10.E]/[27.E]: “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. Collinge discloses this limitation, i.e., “issuer 108 may submit a response based on the validation.” Ex[1011], [0078], [0087].

11. 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. Collinge discloses this limitation. Collinge discloses that the CVC3 may be validated using unpredictable numbers, such as UN_{READER} and UN_{CLOUD}, both unpredictable numbers. Ex[1011], [0083] (“[T]he payment credentials management system 704 may generate a session key unpredictable number (UN_{READER}), a cloud unpredictable number (UN_{CLOUD})...”), [0085] (“The point-of-sale terminal 120 may generate a reader unpredictable number (UN_{READER})...”), [0087] (“[T]he issuer 108 may validate the payment CVC3 value using at least the UN_{READER}, UN_{CLOUD}, and application transaction counter.”); *see also* Ex[1009], [0073]-[0074]. The payment CVC3 value, which is the cryptogram, can be generated using the input information such as KS_{UN} (which is typically part of the encrypted payload) and reader unpredictable number UN_{READER}, which is unpredictable data included in the authorization data in authorization request. Ex[1011], [0083] (“The encrypted payload may include at least one CVC3 key, the KS_{UN} (*sic*), and the application transaction counter...”), [0085] (“[T]he mobile payment application 106 ... may then generate the payment CVC3 value using the information in the encrypted payload...”), [0087].

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

136. As discussed for Claims 11 and 28, Collinge discloses that unpredictable data UN_{READER} is generated by POS terminal and transmitted to the mobile device. Ex[1011], [0085].

137. To the extent not disclosed, a POSA would understand that data transmission from a POS terminal to a mobile device or card are command APDU messages, hence POS commands, and thus, it is obvious that the unpredictable data would be included in a POS command. Ex[1037] at 46-48.

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

138. Collinge explains the authorization data includes “transaction information (e.g., transaction amount, merchant identifier, etc.)”, hence value from transaction. Ex[1011], [0077].

14. 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”

139. Collinge discloses this limitation because a POSA would understand the first cryptographic key is shared by a remote authorization process, which begins with a request in the form of sending a CAP token, as described in Collinge, Ex[1011], [0082], and the first key in the current transaction is the second

cryptographic key in reference to a previous transaction, as explained in [1.G]-[1.H].

Thus, Collinge discloses this element.

140. To the extent not explicitly disclosed, the understanding above would be obvious to a POSA for the reasons explained in [1.G]-[1.H].

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

141. For similar reasons as Claims 4 and 20, Collinge discloses this limitation.

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

142. Collinge, via the provisional application incorporated by reference, explains that the non-permanent, single-use keys (KS_{UN}) are associated with an issuer master key “IMK”) because those keys are generated using intermediate key (using KD_{UN}) which itself is generated from an issuer master key IMK. Ex[1011], [0083] (“As part of the encrypted payload, the payment credentials management system 704 may generate a session key unpredictable number (KS_{UN}), a cloud unpredictable number (UN_{CLOUD}) and may identify and/or store a plurality of dynamic card validation code (CVC3) keys...”); Ex[1009], [0071] (“ KD_{UN} ” section, describing generation using IMK_{UN}).

143. Additionally, a POSA would have found it obvious that the keys are associated with an issuer master key because using issuer master keys to generate card-specific and transaction specific keys for generating authentication cryptograms was well-known. Ex[1009], [0071]; Ex[1020] §§ A1.3 (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) to produce a *k*-bit ICC Session Key (SK).”), A1.4 (derivation of Session Key from ICC Master Key generated from issuer master key), § D3

17. Claim 17

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

144. For the reasons discussed in [1.PRE] and [1.E], Collinge discloses this limitation.

b. [17.A]: “a mobile device comprising: a controller configured to route communications received over a communication channel from an electronic reader;”

145. For the reasons discussed in [1.A] and [1.E], Collinge discloses this limitation by disclosing a “mobile device 104 [that] may conduct a contactless/NFC payment transaction,” Ex[1011], [0070], which necessarily has a controller

configured to route communications received over a communication channel from an electronic reader.

146. A POSA would understand that such a controller would obviously be necessary to enable NFC/contactless communications.

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

147. For the reasons discussed in [1.A-3], Collinge discloses this limitation by disclosing that “the mobile payment application 106 may connect with the remote-SE system 110 via the cloud system 302, such as by using SSL authentication or any other suitable method for authenticated transmission,” which a POSA would understand to require a “wireless interface” for a device to be “mobile” (without a cable). Ex[1011], [0081].

148. A POSA would understand that such an interface would obviously be necessary to enable connection described above.

d. [17.C]: “a processor;”

149. Collinge discloses the mobile device having a processor. Ex[1011], [0041] (“executed by a processor included in the mobile device”); *see also* Ex[1009], [0076]-[0083], [0089]-[0090].

e. [17.D]: “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:”

150. For the reasons discussed in [1.A], Collinge discloses this limitation because Collinge discloses that “mobile device 104” which executes the application and carries out the recited functions “may be implemented in the computer system using ... computer readable media having instructions stored thereon ...” Ex[1011], [0146].

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

151. For the reasons discussed in [1.A-3] and [1.B], Collinge discloses this limitation.

g. [17.F]: “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;”

152. For the reasons discussed in [1.C], Collinge discloses this limitation.

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

153. For the reasons discussed in [1.D], Collinge discloses this limitation.

i. [17.H]: “during an interrogation:”

154. For the reasons discussed in [1.E], Collinge discloses this limitation.

(1) [17.H-1]: “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;”

155. For the reasons discussed in [1.E-1], Collinge discloses this limitation.

(2) [17.H-2]: “access the local cryptographic key associated with the account;”

156. For the reasons discussed in [1.D] and [1.E-2], Collinge discloses this limitation because CVC3 is generated using KS_{UN} stored on the mobile device. *See also* Ex[1011], [0009], [0013], [0083], [0085], Fig. 17; *see also* Ex[1009], [0061].

(3) [17.H-3]: “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”

157. For the reasons discussed in [1.E-2], Collinge discloses this limitation.

(4) [17.H-4]: “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;”

158. For the reasons discussed in [1.E-3], Collinge discloses this limitation.

j. [17.I]: “subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;”

159. For the reasons discussed in [1.F], Collinge discloses this limitation.

k. [17.J]: “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”

160. For the reasons discussed in [1.G], Collinge discloses this limitation.

l. [17.K]: “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.”

161. For the reasons discussed in [1.H], Collinge discloses this limitation.

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

162. For the reasons discussed in [1.F]-[1.G] and [17.I]-[17.J], Collinge discloses this limitation.

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”

163. For the reasons discussed in [8.A]-[8.B], Collinge discloses this limitation.

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

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:”

164. To the extent the preamble is limiting, Fiske discloses this limitation. Fiske discloses securely conducting payment transactions using a mobile device running a payment application, communicating using NFC technology and other communication mechanisms. Ex[1012], 1:19-22, 2:19-26, 11:37-44, 11:49-60, 12:25-44. The system is used to perform a payment transaction, including requesting an authorization and obtaining an authorization response. Ex[1012], 14:35-63, 15:59-16:30, Fig. 7.

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

165. Fiske discloses at a mobile device, executing a mobile payment application in an operating system of the mobile device. Ex[1012], 11:37-44, 11:49-60, 12:25-44.

(2) [1.A-2]: “the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and”

166. As explained in Grounds 1-2, the '171 Patent suggests that interrogation refers to querying or extraction of information. Ex[1001], 6:3-5, 6:50-53, 7:3-7, 10:58-65. Also, as explained in Grounds 1-2, the application on the “Card” will return “digital credential data” required for authorization of transaction. Ex[1001], 7:3-7. Fiske’s mobile application is interrogable by an electronic reader, such as the POS terminal, over a first communications channel (e.g., NFC) for digital credential data. See Ex[1012], 2:18-26, 11:38-40 (“The user of device 502 can interact with a terminal 504 at a PoS via user device 502 in order to make a purchase from a merchant.”), 11:45-48 (“...the user device 502 can communicate with the PoS terminal via contactless communication interface 508. This may be via a short range wireless communication protocol, such as NFC.”), 12:9-24. Fiske describes the POS terminal issuing a “READ RECORD” command to the payment device to “read all of the transaction related data parameters” from

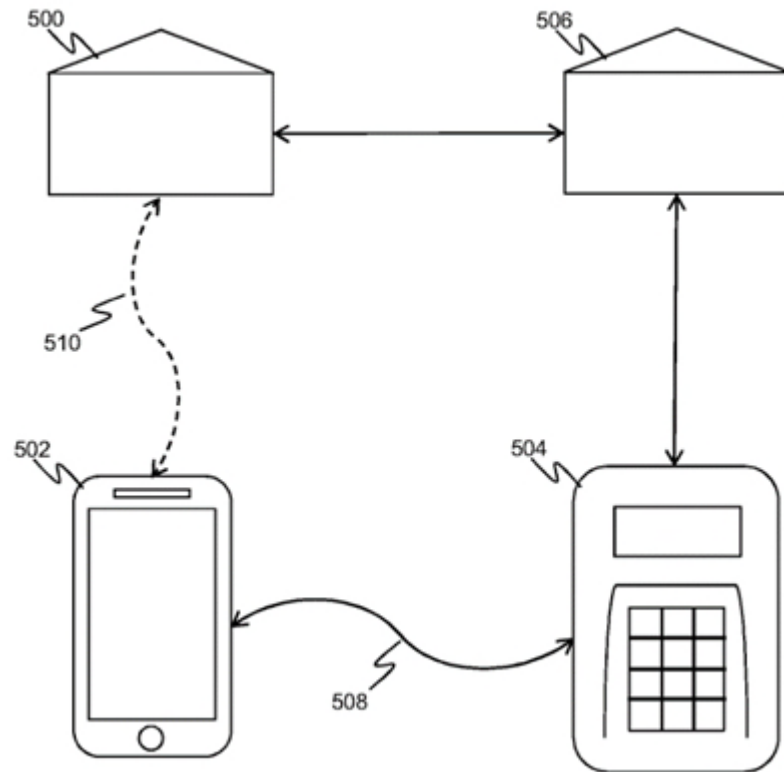
the device, including the primary account number (PAN). Ex[1012], 3:26-46, 2:63-67; 5:28-30.

167. A POSA would have understood that “interrogation” is an obvious way to implement Fiske’s NFC teaching of transmission of information between the mobile device and POS device. *See* Ex[1015], [0062], [0070]. Moreover, Fiske explains its techniques are applicable to “authorizing an EMV payment transaction between a user device and a point-of-sale terminal.” Ex[1012], 1:54-59 (“Many electronic payment systems use the EMV (Europay®, Mastercard®, Visa®) transaction protocols, as defined for example in the EMV 4.2 Specifications or the EMV Contactless Specifications for Payment Systems, which are publicly available and published by EMVCo LLC.”), 2:58-64, 6:54-61, 9:6-11. For example, as explained in [1.A-2], the EMV Specifications similarly disclose an application interrogable by a reader over a communication channel.

(3) [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. Fiske discloses this element. Indeed, Fiske discloses that the “[u]ser device 502 is further capable of communicating with issuing bank 500 via communications interface 510.” Ex[1012], 11:49-50. As shown below, Fiske discloses that the communications interface 510 between the issuing bank and the

user device, is different from the communications interface 508 between the user device 502 and the POS terminal. Ex[1012], 11:45-50, Fig. 5:



169. Fiske discloses that the communications interface 510 can be wireless. Ex[1012], 11:53-57 (“User device 502 may communicate with issuing bank 500 via the internet [or] . . . via the mobile telephony network”), 13:59-67, 17:52-61 (“via the mobile telephone network according to one or more mobile network communication protocols [or] . . . via the internet according to one or more packet based communication protocols”).

170. Fiske also discloses that the user device is equipped with data associated with the account, such as “payment keys, which are necessary for the use

of the payment application...thereby associating [the payment application] with an account at the issuing bank.” Ex[1012], 12:45-52, 12:50-57, 13:17-24. The payment keys or session keys are provisioned or requested to the user device from the issuing bank, Ex[1012], 13:20-31, 13:63-67.

171. To the extent not explicitly disclosed, for reasons similar to those explained in [1.A-3], Grounds 1-2, a POSA would find it obvious for the device to *request* the data from the issuer.

(4) [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”

172. Fiske discloses this element. Fiske explains that an application cryptogram, typically required to complete an EMV transaction, is generated by an ICC Session Key generated by the issuing bank and provisioned to the user device (*i.e.* received from the remote computer system). Ex[1012], 13:20-24, 13:32-35. The application cryptogram is requested during the EMV transaction between the user device and the POS terminal. Ex[1012], 8:20-22 (“In order to respond to a GENERATE AC command issued by the terminal, the ICC must produce an Application Cryptogram”); *see also id.*, 6:54-57, 7:30-41, 8:64-67. As explained in [1.A-2], the EMV transaction is between the user device and the POS

terminal, and thus, involves interrogations over the first communications channel. Ex[1012], 1:19-22, 9:25-36. The application does not access a permanent cryptographic key issued for the digital credential during the interrogations because it uses only the ICC Session Key, which is only valid for a single transaction, and changes after each transaction. *Id.*, 9:59-65 (“a unique key associated with the payment application ... each session key is valid for use only with a single transaction ...”), 13:32-35; *see also id.*, 8:30-39, 13:25-50, 14:1-20, Fig. 4.

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

173. As explained in [1.A-3], Fiske discloses or renders obvious this element, where data associated with the account includes the single- use payment keys such as the ICC Session Key. Ex[1012], 12:45-52, 12:50-57, 13:17-24, 13:20-31, 13:63-67.

c. [1.C]: “receiving by the application, from the remote computer system, over the wireless network, 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;”

174. As explained in [1.A-3] and [1.B], Fiske discloses that the user device receives from remote servers a first set of data associated with the account, such as one or more single-use payment keys, specifically, an ICC Session Key, which are

associated with an account at the issuing bank. Ex[1012], 12:45-52, 12:50-57, 13:17-24. Fiske discloses that the user device can communicate with the issuing bank via a communications interface, which can be wireless. Ex[1012], 11:49-50, 11:53-57, 13:59-67, 17:52-61.

175. The first set of data associated with the account includes an ICC Session Key generated by the issuing bank and provisioned to the user device, which is used to generate an application cryptogram, as required during a single EMV transaction. Ex[1012], 13:20-24, 13:32-35. The ICC Session Key is a cryptographic key associated with the account, and is valid only for a single transaction, and is thus non-permanent. *Id.*, 9:59-65, 13:32-35; *see also id.*, 4:1-9, 8:30-39, 13:25-50, 14:1-20, Fig. 4.

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

176. As explained in [1.C], the ICC Session Key is a non-permanent cryptographic key stored locally at the user device, and is associated with the account. Ex[1012], 9:59-65, 13:32-35; *see also id.*, 4:1-9, 8:30-39, 13:25-50, 14:1-20, Fig. 4.

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

177. As explained in [1.A-2], Fiske discloses the application participating in an interrogation between a POS terminal and the mobile device. It is well known in the art that, in EMV transactions referred to by Fiske, Ex[1012], 1:58-64, 2:54-59, 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 46-48.

(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;”

178. When the user shops at a merchant, as part of the payment process, the POS terminal may send a communication to the mobile device for digital credential data. Moreover, Fiske discloses that “responsive to receiving a request for an application cryptogram at the payment application from the POS terminal, using the payment application to perform an authorization process.” Ex[1012], 9:42-45.

179. As explained in [1.A-4], Fiske discloses that an application cryptogram, which is required during a single EMV transaction, is generated by an ICC Session Key generated by the issuing bank and provisioned to the user

device. Ex[1012], 13:20-24, 13:32-35. The application cryptogram is requested during the EMV transaction between the user device and the POS terminal. Ex[1012], 8:20-22 (“In order to respond to a GENERATE AC command issued by the terminal, the ICC must produce an Application Cryptogram” using the single-use key); see also *id.*, 6:54-57, 7:30-41, 8:64-67.

180. For similar reasons, as Grounds 1-2, [1.E-1], a POSA would have found this element obvious.

(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”

181. Fiske explains that the application cryptogram can be generated based on inputs, such as “data sent to the ICC in the data field of the GENERATE AC command” and the ICC Session Key. Ex[1012], 8:22-24, 8:30-32, 9:47-48, 15:67-16:10; see also *id.*, 6:58-60, 8:20-39. The application cryptogram is enciphered using the ICC Session Key, Ex[1012], 9:63-65, but it is well understood in the art that the application cryptogram would not include the ICC Session Key itself because the cryptogram is generated using the Session Key as encryption key. Ex[1034], 17-18 (explaining message authentication code (MAC) generation); Ex[1039] (showing single-use key is not present in the cryptogram).

(3) [1.E-3]: “responding to the at least one POS command communication ... 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;”

182. Fiske explains that the user device transmits a generated application cryptogram to the POS device for verification, after generation of the application cryptogram. Ex[1012], 9:49-51; 15:67-16:10. Fiske also describes the POS terminal issuing a “READ RECORD” command to the payment device to “read all of the transaction related data parameters” from the device, including the primary account number (PAN), and that the mobile device would return an Application Cryptogram in response to a “GENERATE AC” command. Ex[1012], 3:26-46, 2:63-67; 5:28-30, 7:30-41. As explained in [1.E] and [1.E-1], responses from the device or card are response APDU messages, as recited in this claim element. As further explained in [1.A-2], the interrogation of the mobile device by the POS terminal in EMV transactions is over a first communications channel (e.g., NFC). Ex[1012], 2:18-26, 11:38-40, 11:45-48, 12:9-24.

183. As explained above, the R-APDU Term here is potentially subject to two alternative constructions. However, under either construction, the Term is disclosed by Fiske carrying out a contactless EMV transaction, for the same reasons

stated in [1.E-3] above—either a Master or Visa transaction would satisfy the claim element under Construction 1, and a Visa transaction would satisfy under Construction 2.

184. For similar reasons, as Grounds 1-2, [1.E-3], a POSA would have found this element obvious.

185. Thus, Fiske discloses or renders obvious this element, alone or further in view of the EMV specification.

f. [1.F]-[1.G]: “... requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account ... comprising a second non-permanent cryptographic key associated with the account; and”

186. As explained in [1.A-3] and [1.B] above, the ICC Session Key is a non-permanent, single-use key generated for the session, and is data associated for the account that would be requested from the remote server. Ex[1012], 13:51-56; *see also id.*, 14:6-34.

187. Further, because the ICC Session Key is valid for a single transaction and can be purged from the user device after the EMV transaction is completed, Ex[1012], 13:32-39, it would be natural that a new ICC Session Key for a subsequent transaction may be requested subsequent to a prior transaction, which consumed the ICC Session Key for the prior transaction. In other words, the “second set of data” in a given transaction may correspond to the “first set of data” [1.A-3] of a

subsequent transaction. Therefore, by disclosing [1.A-3], [1.B], and [1.C], Fiske discloses these elements.

188. A POSA would find it obvious to request and receive the “second set of data” to be used as the “first set of data” for next transaction, because otherwise the “second set of data” would be unused, and the request thereof will be meaningless and wasteful.

g. [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.”

189. For the reasons discussed in [1.D], [1.F] and [1.G], Fiske discloses this element. Indeed, because the application on the mobile device would generate the Application Cryptogram, the new ICC Session Key must be stored before generation of Application Cryptogram. Ex[1012], 13:32-39. Indeed, Fiske discloses that “if the previously used ICC Session Key was discarded after the completion of a transaction, the newly received session key can simply be stored.” Ex[1012], 14:1-5.

2. Claims 2 and 18: “wherein the mobile device is an NFC emulating device, wherein ... data associated with the account are received via a data connection over the internet”

190. Fiske discloses this limitation. Fiske discloses that the mobile device can include “short range wireless communications hardware, including short range

wireless antenna, which can be used to make contactless communication with a PoS terminal, and may be an NFC antenna.” Ex[1012], 12:9-13; *see also id.*, 2:19-26, 11:45-48.

191. For reasons discussed in [1.A-2], [1.C], and [1.G], the first set of data associated with the account and the second set of data associated with the account can be received via a data connection over the internet. Ex[1012], 11:53-54 (“User device 502 may communicate with issuing bank 500 via the Internet.”); *see also id.*, 11:49-50, 11:53-57, 13:59-67, 17:52-61.

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

192. Fiske discloses that the single-use session key is used to generate an application cryptogram, which is required during an EMV transaction that Fiske enables. Ex[1012], 13:20-24, 13:32-35. Application Cryptogram (AC), which is a Message Authentication Code (MAC) under EMV Specifications, is generated using the triple DES encryption algorithm. Ex[1020] §§ 8.1.1-8.1.2, A1.2-1.3, B1.1.

193. 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, A1.2.1, A1.2.2, 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), information in the input data is irreversibly lost from the resulting cryptogram (MAC), making it impossible to de-crypt and recover the input data. Ex[1034], 17-18.

194. It is obvious to a POSA because computation of Application Cryptogram as a hash is in the EMV Specifications and well known in the art.

4. 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”

195. Fiske discloses this limitation. Fiske discloses the public availability of EMV transaction protocols based on EMV Specifications, which are incorporated by reference. Ex[1012], 1:58-64 (“Many electronic payment systems use the EMV (Europay®, Mastercard®, Visa®) transaction protocols, as defined for example in the EMV 4.2 Specifications or the EMV Contactless Specifications for Payment Systems, which are publicly available and published by EMVCo LLC.”), 6:54-61, 9:6-11. These specifications describe the inputs and responses by the card to be compatible with EMV transactions. *See generally* Exs[1019]-[1029].

196. Further, a POSA would find it obvious to make the device inputs and responses conforming to a card specification to conduct EMV transactions according to EMV Specifications.

5. 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”

197. As explained for Claims 5 and 21 under Grounds 1-2, these claims are disclosed under EMV Specifications. Therefore, Fiske discloses (anticipates) these claims by incorporating EMV Specifications and purporting to enable EMV transactions, or otherwise renders these claims obvious.

6. 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”

198. Fiske explains that the Application Cryptogram (AC) (response cryptogram) can be generated based on a set of inputs, such as “data sent to the ICC in the data field of the GENERATE AC command” and the ICC Session Key, and it is well known in the art that the AC in an EMV transaction is generated using a 3DES algorithm. Ex[1012], 8:22-24, 8:30-32, 9:47-48; Ex[1020] §§ 8.1.2, A1.2, B1.1; *see also id.*, 6:58-60, 8:20-39; *see also* Ex[1034], 17-18. Thus, to the extent this is not disclosed in Fiske, it is obvious to a POSA.

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

199. As explained in [1.A] and [1.E-1], the interrogation between the mobile device and the POS terminal does not require wireless network connectivity, and

indeed, occurs on a communications channel separate from the wireless network used to communicate with the remote server. To the extent not disclosed, a POSA would find this obvious, such as when the POS terminal is in a facility below ground (e.g., transit), in a geographic area with poor cellular service, or for other reasons.

8. Claim 8

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

200. For the reasons discussed in [1.A], Fiske discloses this limitation.

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”

201. For the reasons discussed in [1.B]-[1.C], Fiske discloses this limitation.

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.”

202. For the reasons discussed in [1.F]-[1.G], Fiske discloses this limitation.

9. 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”

203. For the reasons discussed in [1.A-3] and [1.B], Fiske discloses this limitation by disclosing remote servers such as the issuing bank hosting digital credential data including the ICC Master Key used to generate the ICC Session Key, thereby achieving a secure element representation remotely. Ex[1012], 13:16-20; see *also id.*, 8:30-42, 10:1-17 (“By holding the ICC Master Key at the issuing bank ... embodiments of the present invention are able to reduce the risk associated with a successful attack on the payment application ... By reducing the risk associated with a successful attack on the payment application, embodiments of the present invention facilitate the provisioning of the payment application in a manner that does not require the use of security features provided by a secure element.”), Fig. 4.

10. 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:”

204. To the extent the preamble is limiting, Fiske discloses this limitation. Fiske discloses performing an authorization process at the issuing bank. Ex[1012], 7:38-50, 9:1-11, 14:35-63, 15:59-16:30, Fig. 7.

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;”

205. Fiske discloses that “[i]n response to receiving the Application Cryptogram, the terminal identifies the type of Application Cryptogram sent by the user device ... and forwards the ARQC [Authorization Request Cryptogram] to the issuer ... for authorization of the transaction.” Ex[1012], 16:6-10; *see also id.*, 7:30-60, Fig. 7.

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

206. Fiske discloses that “[t]he issuer may identify which Session Key was used to generate the ARQC” Ex[1012], 17:13-14, Fig. 7.

d. [10.C]/[27.C]: “calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;”

207. During examination of the ARQC, which is an Application Cryptogram, it could be calculated using the Session Key identified in [10.B]/[27.B]. Ex[1020] §§ 8.1.1, 8.1.2, A1.2, A1.3, B1.1; Ex[1034], 17-18; Ex[1021] § 10.9 n.17; Ex[1037] at 58.

e. [10.D]/[27.D]: “verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and”

208. A POSA would understand that the validation process includes comparing the calculated cryptogram to the response cryptogram in EMV transactions referred to by Fiske. Ex[1037] at 57-58, or would otherwise find this obvious because it is well established practice in the art.

f. [10.E]/[27.E]: “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.”

209. Fiske discloses that the “issuer reports its decision to the PoS terminal,” after examining the ARQC. Ex[1012], 16:19-30, Fig. 7.

11. 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”

210. The set of inputs, authorization data, and calculated cryptogram would comprise unpredictable data, because Fiske explicitly incorporates by reference EMV specification, which 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.

211. The “authorization data” refers to such data contained in the authorization request (Claims 10 and 27). It was well understood in the art that, in

EMV transactions, the authorization request would include the “unpredictable number.” Ex[1037] at 57. Further, it was well understood in the art that, 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). Ex[1021] § 10.9 n.17; Ex[1037] at 58.

212. To the extent these claim elements are not disclosed in Fiske, because Fiske explicitly refers to the invention as “for authorizing an EMV transaction,” a POSA would have found it obvious to implement Fiske in a manner compliant with the EMV specification, as explained above.

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

213. For similar reasons to Claims 11 and 28, Fiske discloses this limitation.

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

214. A POSA would understand that the authorization data includes “[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, or would otherwise find this obvious because it is well established practice in the art.

14. 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”

215. As explained in [1.F]-[1.G], a POSA would understand the first cryptographic key in the current transaction may be a second cryptographic key in reference to a previous transaction. Further, because the Session Key is unique to each transaction, Ex[1012], 8:32-35, a POSA would understand that the new Session Key should be requested *upon completion (authorization) of a transaction* that consumes the last ICC Session Key on the device (hence as part of an authorization process), so that the Session Key can be ready for the next transaction, because it is uncertain that the user would have wireless connection when intending to conduct the next transaction.

216. To the extent the above is not disclosed, a POSA would find it obvious for the reasons stated above.

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

217. For similar reasons as stated for Claims 4 and 20, Fiske discloses this limitation.

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

218. Fiske discloses that the ICC Session Keys are “generated by the issuing bank on the basis of the ICC Master Key.” Ex[1012], 13:20-23; *see also id.*, 8:30-42, 8:54-60, 9:59-61, 10:1-5, 17:3-7, Fig. 4; *see also* Ex[1020] § A1.3, A1.4, D3.

17. Claim 17

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

219. For the reasons discussed in [1.PRE] and [1.E], Fiske discloses this limitation.

b. [17.A]: “a mobile device comprising: a controller configured to route communications received over a communication channel from an electronic reader;”

220. For the reasons discussed in [1.A] and [1.E], Fiske discloses this limitation. Fiske also discloses that the user device has “conventional computational hardware including a processing portion 602 ... and other standard hardware such as an input/output controller, display controller etc.” Ex[1012], 11:61-65. The user device “includes short range wireless communications hardware ... which can be used to make contactless communication with a PoS terminal.” Ex[1012], 12:9-11; *see also id.*, 11:45-47. Fiske explains that short range wireless antennas can be controlled via a dedicated communication channel. Ex[1012], 12:14-17.

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

221. For the reasons discussed in [1.A-3], Fiske discloses this limitation. *See also* Ex[1012], 11:53-57, 13:59-67, 17:52-61.

d. [17.C]: “a processor;”

222. Fiske also discloses that the user device has “conventional computational hardware including a processing portion 602” Ex[1012], 11:61-65.

e. [17.D]: “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:”

223. For the reasons discussed in [1.A], Fiske discloses this limitation. Fiske also discloses “[s]tandard application environment 620 ... comprises a payment application deployed on device 600,” Ex[1012], 12:25-26, Fig. 6, which a POSA would understand to disclose this element.

224. It would have been obvious to a POSA that the user device could contain a computer readable storage medium accessible by the processor storing an application executable in an operating system of the mobile device.

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

225. For the reasons discussed in [1.B], Fiske discloses this limitation.

g. [17.F]: “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;”

226. For the reasons discussed in [1.C], Fiske discloses this limitation.

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

227. For the reasons discussed in [1.D], Fiske discloses this limitation.

i. [17.H]: “during an interrogation:”

228. For the reasons discussed in [1.E], Fiske discloses this limitation.

(1) [17.H-1]: “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;”

229. For the reasons discussed in [1.E-1], Fiske discloses this limitation.

(2) [17.H-2]: “access the local cryptographic key associated with the account;”

230. For the reasons discussed in [1.E-2], Fiske discloses this limitation. Fiske discloses that the ICC Session Key is generated by the issuing bank and provisioned to the user device for generation of Application Cryptogram. Ex[1012], 13:20-24, 13:32-35.

(3) [17.H-3]: “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”

231. For the reasons discussed in [1.E-2], Fiske discloses this limitation.

(4) [17.H-4]: “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;”

232. For the reasons discussed in [1.E-3], Fiske discloses this limitation.

j. [17.I]: “subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;”

233. For the reasons discussed in [1.F], Fiske discloses this limitation.

k. [17.J]: “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”

234. For the reasons discussed in [1.G], Fiske discloses this limitation.

l. [17.K]: “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.”

235. For the reasons discussed in [1.H], Fiske discloses this limitation.

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

236. For the reasons discussed in [1.F]-[1.G] and [17.I]-[17.J], Fiske discloses this limitation.

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”

237. For the reasons discussed in [8.A]-[8.B], Fiske discloses this limitation.

IX. RESERVATION OF RIGHTS

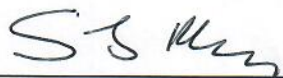
238. My opinions are based upon the information that I have considered to date. I am unaware of any evidence of objective considerations with respect to the '171 Patent that would render any of the challenged claims non-obvious. I reserve

the right, however, to supplement my opinions in the future to respond to any arguments raised by the owner of the '171 Patent and to consider new information that becomes available to me.

X. DECLARATION

239. 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 11, 2023.



Stuart Fiske