UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARDWARE INC.,

Patent Owner

Case No. IPR2025-01147
U.S. Patent No. 10,628,820

DECLARATION OF DR. CLIFFORD NEUMAN

TABLE OF CONTENTS

CLAIM LISTING

Claim Designation	Claim Language
Claim 1(Pre)	A payment system comprising:
Claim 1(a)	a thin shaped body having no fixed payment numbers disposed thereon;
Claim 1(b)	a memory;
Claim 1(c)	a cryptographic processor coupled to the memory; and
Claim 1(d)	a reader interface, including at least one interface selected from a set comprising: a magnetic-stripe, a smart card reader interface, a magstripe inductor interface, an RF interface, an NFC interface, and a wireless interface, and
Claim 1(e)	wherein payment information for a transaction is operable to be conveyed via the reader interface and comprises limited-use payment information, and
Claim 1(f)	wherein further the limited-use payment information is to be used in place of card issuer payment information for payment transactions by said device at payment card reader facilities.
Claim 2	The device of claim 1, wherein the body comprises fixed payment information disposed thereon and wherein the fixed payment information includes only: a card-holder name; a payment issuing logo; and a card payment network logo, and wherein further, the body is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.
Claim 3(a)	The device of claim 1, wherein the limited-use payment information is conveyed via the magnetic stripe and is unique to the payment device and to the magnetic stripe, and
Claim 3(b)	wherein the limited-use payment information is limited to use by the payment device and is operable for conveying payment information to a magnetic-stripe payment card reader, and
Claim 3(c)	wherein said limited-use payment information has a limited period of valid use, and
Claim 3(d)	wherein said limited-use payment information is not valid when used other than through a magnetic stripe payment card reader.

Claim Designation	Claim Language
Claim 4	The device of claim 1, wherein said limited-use payment information is provided by a card issuing authority for use by the payment device and wherein the card processing authority rejects as invalid, any use of said limited-use payment information obtained via any means other than: a payment card reader reading said limited-use payment information from the reader interface.
Claim 5(a)	The device of claim 1, wherein a request for payment includes at least one of a set comprising: payment information, transaction information, merchant information, and payment card reader information, and
Claim 5(b)	wherein a card-present transaction is one including the limited-use payment information, and valid payment card reader information, and wherein a card-not-present transaction is one including at least a portion of said limited-use card payment information, and not including valid payment card reader information; and,
Claim 5(c)	wherein a processing authority is operable to approve as valid, a card-present payment transaction; and,
Claim 5(d)	wherein said card processing authority is operable to reject, as not valid, a use of the limited-use card payment information in a card-not-present payment transaction; and
Claim 5(e)	wherein a card issuing authority receiving said request for payment is operable to decline a transaction not involving a valid card-present use of a limited-use card payment information portion used in place of card issuer supplied payment information.
Claim 6	The device of claim 1, wherein a card processing authority is operable to reject as invalid, a use of the limited-use payment information provided via the reader interface, in online payment transactions.
Claim 7(Pre)	The device of claim 1, wherein a card issuer providing the limited-use payment information, for use by the payment device, limits valid approval of said limited-use payment information to performing a card-present payment transaction by the card device, and wherein said card issuer declines as

Claim Designation	Claim Language
	invalid a use of said limited-use payment information in transactions other than wherein the payment device is present, and
Claim 7(a)	wherein a card issuer limits said card payment information to use for a finite amount of time, and declines as invalid use when said amount of time has expired, and
Claim 7(b)	wherein a card issuer limits use to payment for transactions with the user approving, and declines as invalid use when the card user is denying an approval, and
Claim 7(c)	wherein a card issuer limits to use in place of card issuer information for payments by the payment device.
Claim 8(a)	The device of claim 1, wherein the reader interface is operable to wirelessly receive cardholder transaction information and to identify a valid user through at least one user-validation action, selected from a set of [sic]comprising:… a device user interface receiving a user entered a valid PIN or Key-Code; a device user interface receiving a user entered a valid password; a device user interface reading a user swipe or gesture; a user tapping a predetermined sequence on the device; a user motioning the device in accordance with a sequence; a skin-contact sensing identifying a valid user; a device sensor array reading a touch of an identified user; a device biometric recognition of a valid user; and
Claim 8(b)	wherein a display of the device is operable to display transaction information through a user interface, and wherein transaction information includes at least one of a set comprising: a transaction time; a transaction amount; transaction merchant information; a transaction location; a transaction facility; card information; a partial card number; graphical card images; and
Claim 8(c)	wherein upon validating the user, the user-interface is operable to receive a valid user input, of at least one user action selected from a set comprising: a payment approval authorization; a payment denial; and an adjustment of a transaction payment.
Claim 9(a)	The device of claim 1, wherein a dynamically-generated one-time limited-use payment information portion is generated by

Claim Designation	Claim Language
	said processor when coupled to a reader interface accessible to said processor, and
Claim 9(b)	wherein the payment information conveyed to a payment card reader, at the time of transaction, includes at least one of a portion of: a static limited-use portion; and a dynamically-generated limited-use portion, and
Claim 9(c)	wherein said static limited-use payment information is provided by a card issuing authority for use in place of a card issuer payment information.
Claim 10(a)	The device of claim 1, wherein the processor cryptographically dynamically generates a one-time limited-use number based on combination of a card device transaction sequence count, and
Claim 10(b)	at least one of a set of information including: a user information; a user card account number; a device account number; device secret keys; card issuer keys; a time; a merchant; a location; an online address; a payment information; a card reader information; an account information;
Claim 10(c)	wherein the processor increments the card device transaction sequence count on each transaction.
Claim 11(Pre)	An online payment system, the system comprising:
Claim 11(a)	a thin payment device comprising no fixed payment numbers visible thereon; and
Claim 11(b)	a personal computing device, wherein the personal computing device comprises:
Claim 11(c)	a processor;
Claim 11(d)	a memory;
Claim 11(e)	a wireless interface;
Claim 11(f)	a display operable to provide a visual user-interface operable for performing online transactions; and
Claim 11(g)	a user-interface coupled to the processor, and
Claim 11(h)	wherein the wireless interface is operable to wirelessly obtain card device payment account information, and

Claim Designation	Claim Language
Claim 11(i)	wherein the processor is operable to generate limited-use payment information based on the card device payment account information, and
Claim 11(j)	wherein the personal computing device is operable to generate complete payment information, including the limited-use payment information, and to convey said complete payment information via at least one interface of a set comprising: said display; and the wireless interface, and
Claim 11(k)	wherein the limited-use payment information is configured to be used in place of a card issuer payment information.
Claim 12	The system of claim 11, wherein the thin payment device bears no fixed payment numbers, and bears only: the cardholders name; a brand logo; and the card payment network logo.
Claim 13(a)	The system of claim 11 wherein the personal computing device is configured for presenting on the display a limited-use card security code number for use in payments in place of card issuer payment information, and
Claim 13(b)	wherein the personal computing device is further configured to generate said limited-use card security code responsive to an input request from a valid user, via said user-interface, and
Claim 13(c)	wherein said limited-use number is generated on the personal computing device from at least one information from a set comprising: a payment device user information; a payment device account number; a payment device sequence counter; a payment device identifier; payment device secrets; a payment device key; computing device secrets; computing device keys; payment device issuer secrets; payment device issuer keys; a time; an expiration date; an amount; a merchant locality; an online location; a transaction information; and a cryptographic combination of at least two of the above.
Claim 14(a)	The system as described in claim 11 wherein the personal computing device is configured for presenting on the display, a limited-use card account number, and a limited-duration expiration date, for use in payments in place of a card issuer payment information, and

Claim Designation	Claim Language
Claim 14(b)	wherein said personal computing device is further configured to generate said limited-use card payment information responsive to an input request from a valid user, and
Claim 14(c)	wherein the personal computing device is configured to identify a valid device-user through at least one user-validation input available to the personal computing device, of a set comprising: a touch ID sensor operable to identify the touch a valid user; a user entering of a valid passcode on a touch sensor-array; a user entering of a valid passcode on a key-pad; a user entering of a valid PIN or Key-Code on the user-interface a user entering of a valid password on the user-interface; a valid user swiping or gesturing on a touch sensor-array; a valid sequence of a user tapping of the device detectable by device accelerometer; a valid user sequence of user motioning of the device detectable by device motion sensor unit; a skin-contact sensing identifying a valid user on a device contact sensor; a touching of an identified user's skin on a device touch sensor array; a device biometric recognition of a valid user via a device biometric sensing; and a biometric sensing of the device remaining continuously in the proximity possession of a valid user via device skin-proximity sensor;
Claim 14(d)	and, wherein the personal computing device conveys the limited-use payment information through the user interface.
Claim 15(Pre)	An online payment system comprising:
Claim 15(a)	a thin card-shaped payment card device that bears no fixed payment numbers on the card device; and
Claim 15(b)	a computing device operable for completing an online payment transaction and comprising:
Claim 15(c)	a display;
Claim 15(d)	a user-interface;
Claim 15(e)	a processor; and
Claim 15(f)	a memory for storing a payment card information accessible to the processor,
Claim 15(g)	wherein card issuer provided payment card information is wirelessly downloaded into the computing device, and

Claim Designation	Claim Language
Claim 15(h)	wherein at least one of the set comprising: the computing device; and the card-shaped payment device, is configured to dynamically generate a limited-use payment information, upon the authorization of a valid computing device user, and
Claim 15(i)	wherein the payment information provided by the computing device is used in online transactions in place of a card issuers payment card information.
Claim 16	The system of claim 15 wherein the card device bears no fixed payment numbers, and bears only: the cardholders name; the brand logo; and the card payment network logo.
Claim 17	The system of claim 15 wherein the dynamically generated limited-use payment information is displayable on a display of the computing device.
Claim 18(a)	The system of claim 15 wherein the limited-use payment information includes a static limited-use card account number, a limited-duration card expiration date, and a limited-use card security code and,
Claim 18(b)	wherein the dynamically generated limited-use payment information is conveyed by the computing device to complete an online transaction.
Claim 19(a)	The system of claim 15 wherein the computing device is operable to generate a limited-use card security code number, for use in place of a card issuers card security code by generating said limited-use number via cryptographically combining information from at least one of a set comprising: a user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; a transaction information; and a cryptographic combination of at least two of the above set,
Claim 19(b)	and wherein the computing device is operable to display the generated limited-use card security code on the display.
Claim 20(a)	The system of claim 15 wherein the computing device is further operable to obtain a user payment approval through at

Claim Designation	Claim Language
	least one user-interface element of the computing device, from a set comprising: a display interface, a touch-screen interface, a touch ID button, input buttons, a touch key-pad, a key-pad, a key-board, an optical sensor array, a motion detection unit, an accelerometer, the swiping of a recognized user skin over a device sensor array, a biometric sensor, a wireless interface, an NFC interface, an RF interface, a device biometric sensing the device is continuously remaining in contact with a valid user; and,
Claim 20(b)	wherein the computing device is operable to display at least one of a set comprising: the transaction information, the merchant information, the time, the location of the transaction, the payment bank logo, the card issuer icon, the payment card image, and the amount, on a display of the computing device, and,
Claim 20(c)	a user input providing for at least one user action from a set comprising: an approving of a transaction, a denying of a transaction, and an adjusting of a transaction, via the user-interface.

I, Dr. Clifford Neuman declare the following:

I. INTRODUCTION

1. I have been retained by counsel for Petitioners as a technical expert in the above-captioned case. Specifically, I have been asked to render certain options regarding the IPR petition with respect to U.S. Patent No. 10,626,820 (the "'820 Patent"). I understand that the Challenged Claims are 1-20, and my opinions herein are limited to those claims. A true and correct copy of my Curriculum Vitae, which provides further details about my background and experience, is appended to this Declaration.

A. Educational Background and Professional Experience

2. My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Appendix A. The following is a brief summary of my relevant qualifications and professional experience. I received a Ph. D. in Computer Science in 1992 and an M.S. in Computer Science in 1988 from the University of Washington, and an S.B. (Bachelor's) in Computer Science and Engineering in 1985 from the Massachusetts Institute of Technology.

3. Since receiving my doctorate, I have devoted my career to the field of distributed computer systems development and research with a significant portion of my experience in the area of electronic commerce and internet payments. I have

studied, taught, practiced, and researched in the field of computer science for over forty years.

4. I am currently an Associate Professor of Computer Science Practice in the Department of Computer Science at the University of Southern California (USC), where I have taught since 1992. I am also the Director of the Center for Computer Systems Security, an affiliated Scientist at USC's Information Sciences Institute, and I direct the Computer Security Curricula within the Data Science Program at USC. I teach and have taught numerous courses at USC, including advanced courses in computer science for upper-level undergraduates and graduate students, on topics such as distributed systems and computer and network security.

5. As part of my research at USC, I have worked in a number of areas, including research in distributed computer systems with emphasis on scalability and computer security, especially in the areas of authentication, authorization, policy, electronic commerce, and protection of cyber-physical systems and critical infrastructure such as the power grid. I have worked on the design and development of scalable information, security, and computing infrastructure for the Internet. I am also the principal designer of the Kerberos system, an encryption-based authentication system used among other things as the primary authentication method for most versions of Microsoft's Windows and for many other enterprise computer

systems. I have also developed systems that used Kerberos as a base for more comprehensive computer security services supporting authorization, audit, and electronic payments.

6. In addition to my academic experience, I have many years of practical experience designing computer security systems. For example, from 1985-1986, I worked on Project Athena at MIT, to produce a campus-wide distributed computing environment. I also served as Chief Scientist at CyberSafe Corporation from 1992-2001. I have designed systems for network payment which build upon security infrastructure to provide a secure means to pay for services provided over the Internet. For example, I designed the NetCheque and NetCash systems, which are suitable for micropayments (payments on the order of pennies where the cost of clearing a credit card payment would be prohibitive). In 2000 and 2001, I was on the advisory board for NetResearch Inc, d/b/a BayBuilder, which was a company developing online auction platforms.

7. As part of my research on improving authentication and the security of electronic commerce in the late 1990s, I was involved with the integration of smart cards and PCMCIA cryptographic processors into security services used by end-point computing devices such as personal computers. Also in the late 1990's I

worked with the Financial Services Technology Consortium on their electronic check project.

8. I have authored or co-authored over 50 academic publications in the fields of computer science and engineering. In addition, I have been a referee or editor for the following academic journals: ACM Transaction on Information and Systems Security and International Journal of Electronic Commerce. My curriculum vitae includes a list of publications on which I am a named author. I am also a member of the IEEE, Association for Computer Machinery (ACM), and the Internet Society (ISOC), among others. I have also served as program and/or general chair of the following conferences: The Internet Society Symposium on Network and Distributed System Security and the ACM Conference on Computer and Communications Security.

II. MATERIALS CONSIDERED

9. I have relied upon my education, knowledge, and experience with payment systems, including mobile payment systems, as well as the other materials discussed in this declaration in forming my opinions.

10. In developing my opinions, I have considered the following materials:

Exhibit	Description
1001	U.S. Patent No. 10,628,820 ("*'820 Patent*")
1002	File History of the '820 Patent ("*'820 File History*")

1004	U.S. Patent Publication No. 2013/0262317 to Collinge et al. ("*Collinge*")
1005	U.S. Provisional Patent Application No 61/619,095 to Collinge et al. ("*'095 Provisional*")
1006	U.S. Provisional Patent Application No 61/635,248 to Collinge et al. ("*'248 Provisional*")
1007	U.S. Provisional Patent Application No 61/735,383 to Collinge et al. ("*'383 Provisional*")
1008	U.S. Provisional Patent Application No 61/762,098 to Collinge et al. ("*'098 Provisional*")
1009	U.S. Patent Publication No. 2006/0122931 A1 to Walker et al. ("*Walker*")
1010	U.S. Patent Publication No. 2007/0208671 to Brown et al. ("*Brown*")
1011	U.S. Patent Publication No. 2007/0055630 A1 to Gauthier et al ("*Gauthier*")
1012	U.S Patent Publication No. 2012/0143754 to Patel ("*Patel"*)
1013	U.S. Patent Publication No. 2010/0125509 to Kranzley et al. ("*Kranzley*")
1014	U.S. Patent Publication No. 2013/0068366 to Eng ("*Eng*")
1015	U.S. Patent No. 8,103,588 B2 to Patterson (*"Patterson")*
1016	"Computer," MERRIAM-WEBSTER DICTIONARY (1997)
1017	*This Month in History: The First Credit Card,* BANKER & TRADESMAN (Sept 25, 2022), https://bankerandtradesman.com/this-month-in-history-the-first-credit-card/ ("*Banker & Tradesman*")
1020	IBM, *The Magnetic Stripe*, IBM, https://www.ibm.com/history/magnetic-stripe. ("*IBM*")
1021	VEDAT COSKUN, NEAR FIELD COMMUNICATION: THEORY TO PRACTICE (John Wiley & Sons, 1st ed. 2012) ("*Coskun*")
1022	MAGTEK, MAGNETIC STRIPE CARD STANDARDS, (MagTek Inc. eds., 2011) ("*MagTek*")
1023	EMVCO, LLC, EMV INTEGRATED CIRCUIT CARD SPECIFICATIONS FOR PAYMENT SYSTEMS: BOOK 2 – SECURITY AND KEY MANAGEMENT (EMVCo, LLC eds., Version 4.3 2011) ("*EMV*")
1024	KLAUS FINKENZELLER, RFID HANDBOOK (John Wiley & Sons, 3rd ed. 2010) ("*Finkenzeller*")

1025	MasterCard, *MasterCard PayPass ™ in Action*, MASTERCARD (Jun. 11, 5:35 PM), https://www.mastercard.com/us/company/en/ourbusiness/paypass_in_action.html#:~:text=MasterCard%20PayPass%E2%84%A2%20in%20Action&text=Developed%20to%20replace%20the%20need,the%20way%20they%20view%20cash. ("*PayPass*")
1026	SMART CARD ALLIANCE, EMV AND NFC: COMPLEMENTARY TECHNOLOGIES THAT DELIVER SECURE PAYMENTS AND VALUE-ADDED FUNCTIONALITY (Smart Card Alliance, Inc. eds., 2012) ("*Smart*")
1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. ("*Pitroda*")
1028	MasterCard, *MasterCard Approved Mobile Devices*, MASTERCARD (Aug. 3, 2012), http://www.mastercard-mobilepartner.com/docs/MasterCard_Approved_Mobile_Devices.pdf, [https://web.archive.org/web/20120906234255/http://www.mastercard-mobilepartner.com:80/docs/MasterCard_Approved_Mobile_Devices.pdf] ("*MasterCard Mobile Partner*")
1029	U.S. Patent Publication No. 2013/0054474 to Yeager ("*Yeager*")
1030	EMVCo, LLC, *EMV Chip At-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World*, EMVCO (2002), https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf ("*EMVCo*")
1031	SCOPING SIG & TOKENIZATION TASKFORCE PCI SECURITY STANDARDS COUNCIL, PCI DATA SECURITY STANDARD (PCI DSS) – INFORMATION SUPPLEMENT: PCI DSS TOKENIZATION GUIDELINES (pci Security Standards Council eds., Version 2.0 2011) ("*PCI SSC*")
1032	ALESSANDRO VIZZARRI ET AL., SECURITY IN MOBILE PAYMENTS (2013) ("*Vizzarri*")
1033	U.S. Patent Publication No. 2008/00110983 to Ashfield ("*Ashfield*")
1034	EMVCO, LLC, EMV INTEGRATED CIRCUIT CARD SPECIFICATIONS FOR PAYMENT SYSTEMS: BOOK 3 – APPLICATION SPECIFICATION (EMVCo, LLC eds., Version 4.3 2011) ("*EMV4.3 Book 3*")

1035	Tore Fjellheim, *Over-the-air Deployment of Applications in Multi-Platform Environments*, IEEE, PROCEEDINGS OF THE 2006 AUSTRALIAN SOFTWARE ENGINEERING CONFERENCE (ASWEC'06) (2006)
1036	GEOFFREY R. GERDES ET AL., THE 2013 FEDERAL RESERVE PAYMENT STUDY – RECENT AND LONG-TERM TRENDS IN THE UNITED STATES: 2003-2012 (Federal Reserve System, Rev. 2014) ("*Study Summary*")
1037	GEOFFREY R. GERDES ET AL., THE 2013 FEDERAL RESERVE PAYMENT STUDY – RECENT AND LONG-TERM TRENDS IN THE UNITED STATES: 2000-2012 (Federal Reserve System, 2014) ("*Study*")
1038	ConsumerWorld, *Two Months After the Deadline, Most Major Retailers Still Can't Read Chipped Credit Cards,* CONSUMERWORLD (Dec. 7, 2015), https://www.consumerworld.org/pages/creditcardreaders.htm ("*ConsumerWorld Survey*")
1039	Ann Cavoukian, *Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private*, IPC (2011), https://www.ipc.on.ca/sites/default/files/legacy/Resources/mobile-nfc.pdf ("*Cavoukian*")
1040	ANNIKA PAUS, NEAR FIELD COMMUNICATION IN CELL PHONES (2017) ("*Paus*")
1041	Ashis K. Mahapatra, *Touch Screen Systems*, ORISSA REVIEW (2005), https://magazines.odisha.gov.in/orissareview/jun2005/engpdf/touch_screen_system.pdf ("*Mahapatra*")
1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. ("*Hotelling*")
1043	U.S. Patent Publication No. 2008/0122796 to Jobs et al. ("*Jobs*")
1044	U.S. Patent No. 7,793,851 to Mullen ("*Mullen*")
1045	WIPO International Publication No. WO 2010/039337 to Lin et al. ("*Lin*")
1046	Mike Rosulek, *The Joy of Cryptography OE*, OREGON STATE UNIVERSITY, CHAPTER 12:HASH FUNCTIONS (1ST ED. 2017), https://open.oregonstate.education/cryptographyOEfirst/chapter/chapter-12-hash-functions/ ("*Rosulek*")
1047	U.S. Patent Publication No. 2014/0006276 to Grigg et al. ("*Grigg*")
1048	Anup K. Ghosh & Tara M. Swaminatha, *Software Security and*

	Privacy Risks in Mobile E-Commerce, 44 CACM 51 (2001) ("*Ghosh*")
1049	CardWare's Preliminary Infringement Contentions

11. I have considered these materials from the viewpoint of a POSITA as of the priority date of the '820 Patent. For the purposes of this declaration, I have been asked to assume that the earliest priority date of the '820 Patent is March 15, 2013. I note that my opinions provided in this Declaration are made from the perspective of a POSITA as of this priority date of the '820 Patent unless expressly stated otherwise. To the extent that I use any verb tense in this Declaration that is present tense (e.g., "a POSITA would understand" instead of "a POSITA would have understood"), such verb tense should be understood to be my opinion as of the '820 Patent's priority date (again, unless expressly stated otherwise). I merely use the present verb tense for ease of reading.

III. OVERVIEW AND LEGAL STANDARDS

12. In formulating my opinions, I have been instructed to apply certain legal standards. I am not a lawyer. I do not offer any testimony regarding what the law is. Instead, the following sections summarize the law as I have been instructed to apply it in formulating and rendering my opinions found later in this declaration. I understand that, in an *inter partes* review ("IPR") proceeding, patent claims may be deemed unpatentable if it is shown that they are anticipated or rendered obvious

in view of the prior art. I understand that prior art in an IPR review is limited to patents or printed publications that predate the priority date of the patent at issue. I understand that questions of claim clarity (definiteness) and enablement cannot be considered as a ground for considering the patentability of a claim in these proceedings.

A. Person of Ordinary Skill in the Art

13. I understand that the ’820 Patent, the record of the proceedings at the Patent Office (which I understand is called the “File History” or “Prosecution History”), and the teachings of the prior art are evaluated from the perspective of a person of ordinary skill in the art (“POSITA”). I understand that the factors considered in determining the ordinary level of skill in the art may include: (i) the levels of education of the inventor; (ii) the types of problems encountered in the art; (iii) prior art solutions to those problems; (iv) the rapidity with which innovations are made; (v) the sophistication of the technology; and (vi) the educational level of persons working in the field.

14. I understand that a person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors above. The hypothetical person is presumed to have the same level of skill as the typical practitioner of the art and is presumed to have knowledge of all

prior art in the relevant field. I understand that the inventor's actual knowledge or lack of knowledge of prior art reference is irrelevant to the obviousness determination.

B. Obviousness

15. I understand that a claim may be invalid under 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been "obvious" to a POSITA in view of a single or combination of prior art references at the time the claimed invention was made. I further understand that a POSITA is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent-in-suit and all analogous prior art. I understand that obviousness in an IPR review proceeding is evaluated using a preponderance of the evidence standard, which means that the claims must be more likely obvious than nonobvious.

16. I also understand that an obviousness determination includes the consideration of various factors including: (1) the scope and content of the prior art, (2) the differences between the prior art and the claim at issue, and (3) the level of ordinary skill in the pertinent art. I understand that secondary considerations of non-obviousness such as commercial success, long-felt but unresolved needs, failure of others, and so forth may be assessed as well. I have been informed that an

obviousness analysis must focus on the state of the art at the time of the invention to avoid impermissibly using hindsight to invalidate a patent.

17. In considering whether certain prior art renders a particular patent claim obvious, I have been informed that I can consider the scope and content of the prior art, including the fact that a POSITA would regularly look to the disclosures in patents, trade publications, journal articles, conference papers, industry standards, product literature and documentation, texts describing competitive technologies, requests for comment published by standard setting organizations, and materials from industry conferences, as examples.

18. I have been informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be "analogous art" to the claimed invention. A reference is analogous art if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). For a reference to be "reasonably pertinent" to the problem, it must logically have commended itself to an inventor's attention in considering the problem. In determining whether a reference is reasonably pertinent, one should consider the problem faced by the inventor, as reflected either explicitly or implicitly, in the specification. I believe that

the documents I considered in forming my opinions in this IPR are well within the range of documents a POSITA would have consulted to address the type of problems described in the Challenged Claims.

19. I have been informed that to establish that a claimed invention was obvious based on a combination of prior art elements, an articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I have been informed that the prior art, either as a single reference or a combination of multiple items of prior art, renders a patent claim obvious when there was an apparent reason for a POSITA, at the time of the invention, to combine or modify the prior art. Rationales for combining or modifying the prior art include, but are not limited to, any of the following: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art;

or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

20. I have also been informed that where there is a motivation to combine, claims may be rejected as obvious provided a POSITA would have had a reasonable expectation of success regarding the proposed combination. I have also been informed that common sense may be considered. Common sense teaches that familiar items may have obvious uses beyond their primary purposes. I have been informed that if the combination was obvious to try (regardless of whether it was actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than non-obvious innovation.

21. I have been informed that the existence of an explicit teaching, suggestion, or motivation to combine known elements of the prior art is a sufficient, but not a necessary, condition to a finding of obviousness. In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose described in the patent-in-suit controls. I have been further informed that the obviousness analysis may consider the effects of demands known to the technological community or present in the marketplace and the background knowledge possessed by a POSITA. These issues may be considered to determine

whether there was an apparent reason to combine the known elements in the fashion claimed by the patent.

22. I have been informed that it is improper to combine references where the references teach away from their combination. A reference may be said to teach away when a POSITA, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the patent applicant. I have also been informed that a reference does not teach away if it merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into the invention claimed.

23. I am informed that even if a case of obviousness is established, the final determination of obviousness must also consider "secondary considerations" if presented. Secondary considerations include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unsatisfied need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) lack of independent simultaneous invention within a comparatively short space of time; and (h) teaching away from the invention in the prior art.

24. I have been further informed that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be based on prior art features. The establishment of a nexus is a question of fact. While I understand that Patent Owner here has not offered any secondary considerations at this time, I will supplement my opinions should Patent Owner raise secondary considerations during the course of this proceeding.

C. Claim Construction

25. I understand that the claim terms in an IPR proceeding are construed according to their plain and ordinary meaning as understood in light of the claim language, the patent's description, and the prosecution history viewed from the perspective of a POSITA. I further understand that where a patent defines claim language, the definition of the patent controls, even if there are other definitions that might be understood by those working in the art. I have applied these principles when interpreting the Challenged Claims and in rendering the opinions provided in this declaration.

26. I understand that Petitioner does not assert that any claim terms require express construction for purposes of this IPR.

IV. PRINTED SUBJECT MATTER

27. I have been informed and understand that limitations that are directed to the presence or absence of printed matter are not entitled to patentable weight if the printed matter has no functional or structural relationship to the associated physical substrate.

V. LEVEL OF A PERSON OF ORDINARY SKILL

28. Based on my review and analysis of the ’820 Patent, the cited prior art, and the ordinary skill factors described in this section, a POSITA in the field of the ’820 Patent at the time of the earliest possible priority date (March 15, 2013) would have been knowledgeable regarding the field of payment processing and digital authentication. In my experience in this field, most workers of ordinary skill in the art as of the earliest possible priority date of March 15, 2013 would have had at least a bachelor’s degree in computer science, computer engineering, electrical engineering or the equivalent, and one or two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technology such as NFC. Additional industry experience or technical training may offset less formal education, while advanced degrees or additional formal education may offset lesser levels of industry experience. When I refer to the understanding of a POSITA, I am referring to the understanding of such a person as of March 15, 2013.

29. As of March 15, 2013, I had more than ordinary skill in the art. I am, however, familiar with the skills and knowledge possessed by those I would have considered to be of ordinary skill in the art as of that date.

30. My opinions provided in this declaration would not change in view of minor modifications to this level of ordinary skill.

VI. OVERVIEW OF THE '820 PATENT

A. Summary of the '820 Patent

31. The '820 Patent describes emulating a standard credit card with a device "capable of generating a programmed magnetic field of alternating polarity…when used in electronic credit card readers." *'820 Patent (Ex.1001)*, 2:17-23. The '820 Patent also describes "generating a limited-duration credit card number…which is limited in scope to a predetermined number of authorized transactions." *Id.* at 2:28-32.

B. Field of Endeavor

32. I have been informed that the field of endeavor of the claimed invention can be determined by reference to explanations of the invention's subject matter in the patent application, including the embodiments, function, and structure of the claimed invention.

33. The '820 Patent defines the "Field of the Invention" as relating to "electronic or smart multi-function electronic devices and, more specifically, to

more secure, smart multi-function electronic payment devices and transaction processing thereof." *'820 Patent (Ex.1001),* 1:27-31. After reviewing the '820 Patent, it is my option that a POSITA would understand that the field of endeavor of the '820 Patent includes more secure payment cards, devices and systems.

34. The '820 Patent's specification criticizes existing systems as "susceptible to theft and/or compromise." 1:66-2:3. For these reasons, a POSITA would have understood that the '820 Patent is trying to solve the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

C. Problem Solved by the Inventors of the '820 Patent

35. I have been informed that a prior art reference is "reasonably pertinent" if a POSITA would have consulted it and applied its teachings when faced with the problem that the inventor was trying to solve. As such, I have been asked to analyze the '820 Patent and determine the problem that the inventors were trying to solve.

36. The '820 Patent notes that a concern with "credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise" and therefore they "have security limitations." *'820 Patent (Ex.1001),* 1:66-2:3. The '820 Patent also noted that "cards employing smart integrated circuit chips and RF technology are not in wide use at present because

they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards." *'820 Patent (Ex.1001),* 2:3-7. To solve these problems, the "Summary of the Invention" describes "multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe" for the "purpose of emulating a standard credit card." *'820 Patent (Ex.1001),* 2:17-21. The "Summary of the Invention" further describes a method of performing a transaction that includes "generating…a limited duration credit card number." *'820 Patent (Ex.1001),* 3:28-30. Thus, a POSITA would understand that the '820 Patent is directed to solving the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

D. File History of the '820 Patent

37. I have reviewed the prosecution history for the '820 Patent. The '820 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. The '820 Patent did not face any prior art rejections during prosecution. *'820 File History (Ex.1002)*.

VII. BACKGROUND OF TECHNOLOGY

38. I was asked to briefly summarize the background of the prior art from the standpoint of a person having ordinary skill in the art prior to March 15, 2013. As explained below, a POSITA would have understood that the payment system

features described in the ’820 Patent (including, for example, limited-use payment information, transaction sequence counts, device account numbers, and secrets) had long been a feature of payment systems that were developed by leading payment processors (including Mastercard and Visa) years before the earliest filing date of the ’820 Patent.

39. As described below, all of the hardware components and functionalities encompassed by the Challenged Claims were well-known to a POSITA in the industry prior to the invention of the ’820 patent.

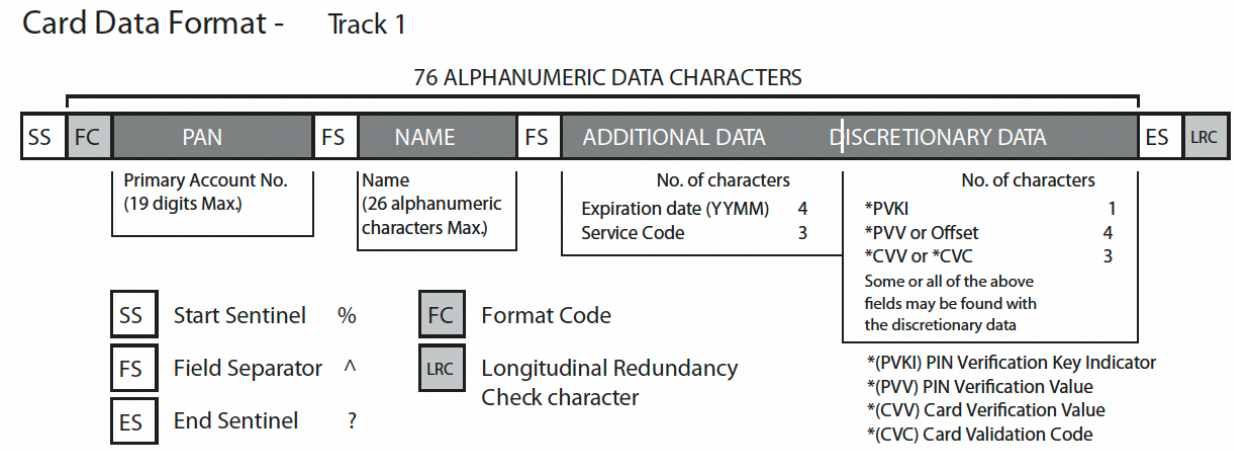
40. The evolution of electronic payment systems can be traced back several decades, marked by key technological milestones that have transformed how financial transactions are processed. Early developments in this field centered on introducing magnetic stripe technology for payment card transactions. Before the late 1960s, credit card transactions primarily consisted of “a tiny printing press to record raised letters and numbers from a card onto a form made of pressure-sensitive paper with carbon copies.” *IBM (Ex.1020),* 1. However, this process was “insecure, slow, and prone to errors” therefore a need for magnetic stripe cards arose. *IBM (Ex.1020),* 1.

A. The Evolution of Payment Cards

1. Magnetic Stripe Cards

41. In the 1960s, "[t]he process of attaching a magnetic stripe to a plastic card was invented by IBM [.]" *Coskun (Ex.1021),* 59. "A magnetic stripe card is one that contains a digital storage space where the data are loaded during the manufacturing phase. The stripe is made up of tiny magnetic particles in a resin. It is traditionally a read-only item. It is read by physical contact by swiping the card past a device with a magnetic reading head." *Coskun (Ex.1021),* 6.

42. Data encoded on the back of the magnetic stripe is called track data such as what is defined in the with ISO/IEC 7813, 7810, and 7811. *MagTek (Ex.1022),* 1. For example, track 1 data includes the following:

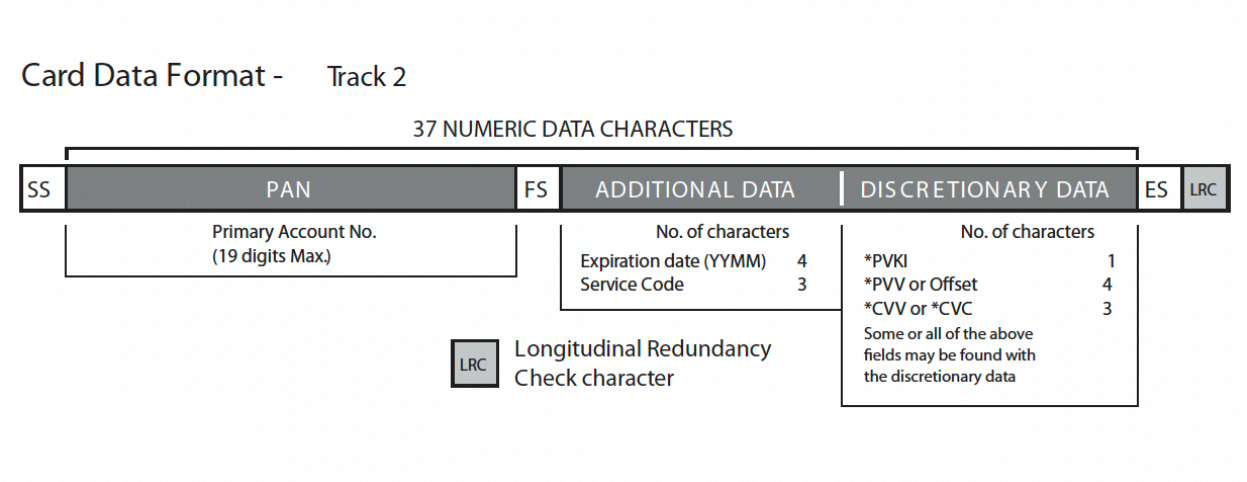


MagTek (Ex.1022), 1. On a card's track:

> "there is a Discretionary Data (DD) segment that allows for the issuer to include some relevant information to use in the transaction authorization process. The typical DD segment includes the static CVV (VISA) or CVC (MASTERCARD) values, which are allotted three characters. Replacing the

three character CVV or CVC data with a three digit dynamic code (dCVV in Visa, Inc. terms, or CVC3 in MasterCard, Inc. terms), including the dCVV of CVC3 indicator character (e.g., a status flag indicating that dynamic data is present), and including a four character Application Transaction Counter value allows the card issuer to use a set of data unique to each transaction to authorize a transaction."

Bona, (Ex.1019), [0102]. Track 2 data includes the following data:



MagTek (Ex.1022), 1.

43. The mag stripe "approach that IBM had helped develop was adopted as a US standard in 1969 and as an international standard two years later, enabling mag stripe cards to be used anywhere in the world." *IBM (Ex.1020),* 1. The global standardization of magnetic stripe cards paved the way for global adoption.

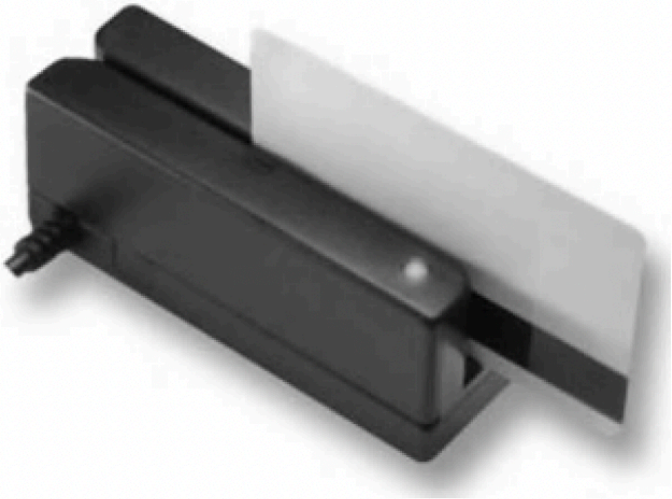


Figure 2.15 Magnetic stripe card.

Coskun (Ex.1021), Figure 2.15.

44. "In recent years, chip-enabled cards that encrypt cardholder data have begun to replace mag stripe cards, which carry static data directly in the magnetic stripe. However, demand for magnetic stripe cards remains strong because of their low cost, reliability and the huge, global installed base of card readers. And even though the job performed by magnetic stripes can now be done with chip cards and mobile phones, the global financial and transaction systems that thrive today are a legacy of the unassuming magnetic stripe." *IBM (Ex.1020),* 2.

2. Smart/Chip Cards

45. Smart cards were well known in the art all the way back to the "1970s." *Coskun (Ex.1021),* 60. "The first mass use of the cards was for telephone

payments in the 1980s. In the meantime, microprocessor smart cards were introduced. Microchips were integrated into debit cards in the 1990s. Smart card based electronic purse systems which store values on a card and do not need network connectivity, began to be used in Europe from the mid 1990s." *Coskun (Ex.1021),* 60.

46. One major improvement "in smart card technology occurred in the 1990s; smart card based SIMs were introduced and started to be used in GSM based mobile phone environments in Europe. The use of smart cards increased with the ubiquity of mobile phones in Europe. In 1993, the international payment brands Europay, MasterCard, and Visa (EMV) collaborated to develop new specifications for smart cards in order to use them in payments both as a debit and a credit card." *Coskun (Ex.1021),* 60 (explaining the first EMV standards were released in 1994).

3. Europay, MasterCard, and Visa (EMV) Standard

47. The EMV standard established a global framework for secure, chip-based payment card transactions. It introduced dynamic data generation, such as cryptograms to prevent replay attacks and authenticate transactions securely. *EMV (Ex.1023),* 71-74 ("generation of the combined dynamic signature and Application Cryptogram"); *EMV (Ex.1023),* 74-77 ("Dynamic Signature Verification"); *EMV*

(Ex.1023), 87-91 "generation of the Application Cryptograms (TC, ARQC, or AAC) generated by the ICC and the Authorisation Response Cryptogram (ARPC) generated by the issuer and verified by the ICC.") The EMV standard defined clear steps in the transaction process, including cardholder verification (e.g., PIN or signature). *See EMV (Ex.1023),* 81-86. The EMV standard laid the foundation for modern secure payments, including contactless and mobile EMV solutions.

B. Contactless Payments

1. Near Field Communications

48. Near Field Communication (NFC) "enables communication between an NFC enabled mobile phone at one end, and another NFC-enabled mobile phone, an NFC reader, or an NFC tag at the other end." *Coskun (Ex.1021),* 1. In terms of distance, "NFC is restricted to within very close proximity." *Coskun (Ex.1021),* 1. This proximity is often "within 4 cm[.]" *Coskun (Ex.1021),* 32.

49. Around 2006-2007, several companies began tested contactless NFC payments. For example, in April 2006, Visa conducted "the world's first mobile Visa payWave payment pilot" involving about "2000 merchants and 200 participants." *Coskun (Ex.1021),* 341-342. As another example, HSBC partnered with MasterCard "tested the use of NFC enabled mobile handsets in payment." *Coskun (Ex.1021),* 342. This "payment service was used where payment by contactless credit card and

MasterCard PayPass was accepted. About 36 000 merchants accepted the MasterCard PayPass payment option at that time." *Coskun (Ex.1021),* 342.

50. NFC has been used to facilitate contactless transactions in payment cards and mobile devices, enabling consumers to make payments simply by tapping their cards. *Smart (Ex.1026),* 7. NFC "technology is defined by the NFC Forum founded by Nokia, Philips, and Sony which allow communication based on RFID technology and ISO/IEC 14443 infrastructures." *Coskun (Ex.1021),* 71.

51. For communication "between two NFC interfaces, the individual NFC interface can take on different functions, i.e. that of an NFC initiator (master device) or an NFC target (slave device). Communication is always started by the NFC initiator. In addition, NFC communication distinguishes between two different operational modes, the active and the passive mode." *Finkenzeller (Ex.1024),* 57.

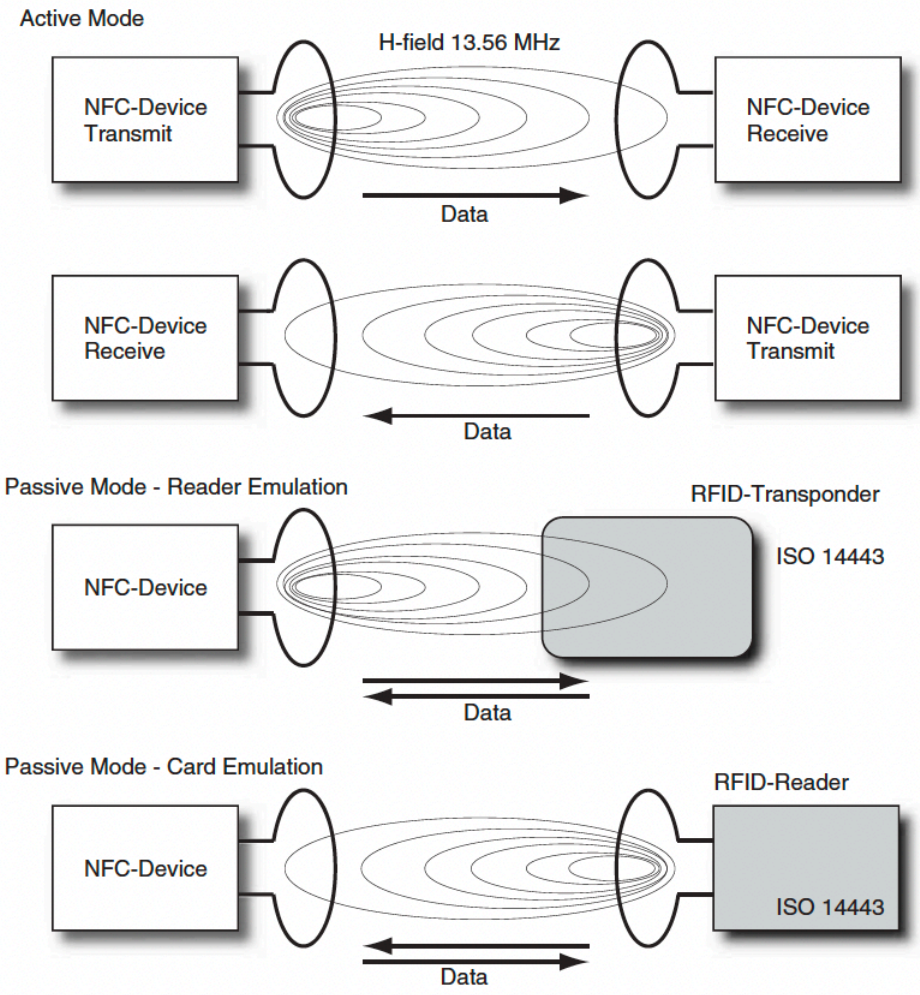


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzeller (Ex.1024), 58.

2. Active Mode

52. An NFC device, for example a mobile phone or payment card, can send information via NFC to another NFC interface. For example, "to transmit data between two NFC interfaces in active mode, at first one of the NFC interfaces activates its transmitter and thus works as the NFC initiator. The high-frequency

current that flows in the antenna induces an alternating magnetic field *H* which spreads around the antenna loop. Part of the induced magnetic field moves through the antenna loop of the other NFC interface which is located close by. Then a voltage *U* is induced in the antenna loop and can be detected by the receiver of the other NFC interface. If the NFC interface receives signals and the corresponding commands of an NFC initiator, this NFC interface automatically adopts the roll of an NFC target." *Finkenzeller (Ex.1024),* 57.

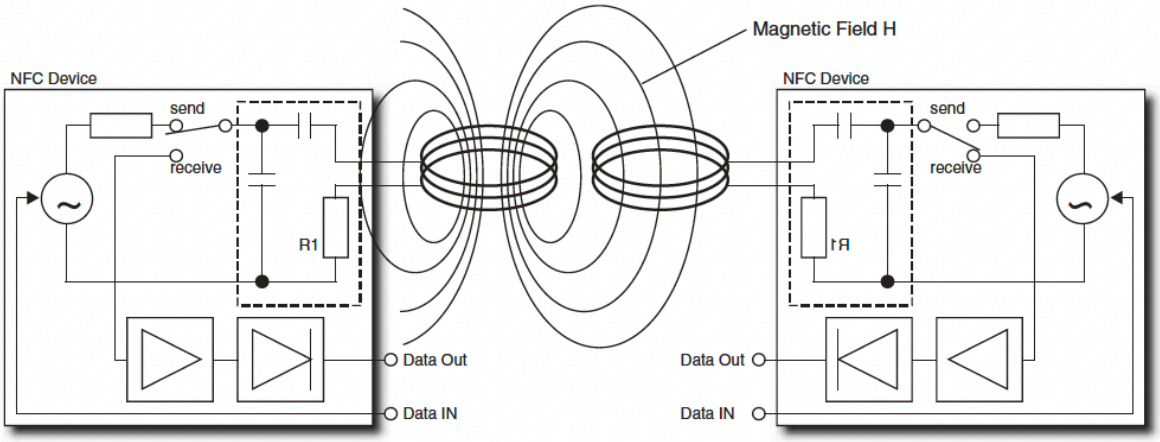


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (Ex.1024), 58.

53. A mobile device or card is also able to receive an NFC request. For example, "[t]he transmission direction is reversed in order to send data from the NFC target to the NFC initiator. This means that the NFC target activates the transmitter and the NFC initiator switches to receiving mode. Both NFC interfaces

alternately induce magnetic fields where data is transmitted from transmitter to receiver only." *Finkenzeller (Ex.1024),* 59.

3. Passive Mode

54. In passive mode "the NFC initiator induces a magnetic alternating field for transmitting data to the NFC target. The field's amplitude is modulated in line with the pulse of the data to be transmitted (ASK modulation). However, after having transmitted a data block, the field is not interrupted, but continues to be emitted in an unmodulated way. The NFC target now is able to transmit data to the NFC initiator by generating a *load modulation*. The load modulation method is also known from RFID systems." *Finkenzeller (Ex.1024),* 59.

55. The NFC interface "that is the target is also able to establish, in addition to other NFC interfaces, the communication to compatible passive transponders (e.g. according to ISO/IEC 14443) that the NFC target supplies with power and that, via load modulation, can transmit data to the NFC interface. This option enables electronic devices equipped with NFC interfaces, such as NFC mobile phones, to read and write on different transponders such as smart labels or e-tickets. As the NFC interface in this case behaves similar to an RFID reader, this option is also called 'reader mode' or '*reader-emulation mode*'." *Finkenzeller (Ex.1024),* 59.

56. If an NFC interface "is located close to a compatible RFID reader (e.g. according to ISO/IEC 14443), the NFC reader is also able to communicate with a reader. Here, the NFC interface adopts the roll of an NFC target and can transmit data to the reader using load modulation. This option enables RFID readers to exchange data with an electronic device with NFC interface, such as NFC mobile phones. From the reader's perspective, the electronic device behaves like a contactless smart card; this option is also called 'card mode' or '*card-emulation mode*'." *Finkenzeller (Ex.1024),* 59.

4. The Development of Near Field Communications

57. Around 2006-2007, several companies began tested contactless NFC payments. For example, in April 2006, Visa conducted "the world's first mobile Visa payWave payment pilot" involving about "2000 merchants and 200 participants." *Coskun (Ex.1021),* 341-342. As another example, HSBC partnered with MasterCard "tested the use of NFC enabled mobile handsets in payment." *Coskun (Ex.1021),* 342. This "payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36 000 merchants accepted the MasterCard PayPass payment option at that time." *Coskun (Ex.1021),* 342.

5. Contactless EMV Payment Cards

58. "From a contactless smart card technology perspective, the major progress was the agreement of Visa and MasterCard in 2004–2006 to implement

contactless payment and ticketing applications such as mass transit and highway tolls in the USA. With the introduction of contactless smart cards such as the MIFARE proximity smart card by Philips, contactless smart card applications started to have a considerable market share in Europe and the US." *Coskun (Ex.1021),* 60. As an example, in 2006, Mastercard "worked with the Ohio Turnpike Commission to bring a consumer trail of *PayPass* payments" using "payment cards for self-service toll transactions." *PayPass (Ex.1025),* 1.

59. As of 2012, the typical contactless payment card working in the US were not EMV-compliant but instead utilized a NFC-enabled chip that transmitted the magnetic stripe data (MSD) included on the associated payment card along with a dynamic value or cryptogram to facilitate transactions. *Smart (Ex.1026),* 6.

6. Mobile Devices and Mobile Wallets

60. Mobile devices performing contactless payments were well known before the '820 Patent.

61. Around 2006-2008, several companies began testing mobile contactless NFC payments. As an example, HSBC partnered with MasterCard to test "the use of NFC enabled mobile handsets in payment." *Coskun (Ex.1021),* 342. This "payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36 000 merchants accepted the

MasterCard PayPass payment option at that time." *Coskun (Ex.1021),* 342. In 2008 the ING Bank also "tested the viability of NFC technology in mobile payment systems for low value purchases in Romania[]" using MasterCard (PayPass). *Coskun (Ex.1021),* 344.

62. A mobile phone can perform these contactless payments via the use of a mobile wallet. A mobile or electronic wallet is similar to "a person's leather, physical wallet[.]" *Pitroda (Ex.1027),* [0025]. An "electronic wallet contains one or more identification cards, credit cards, or the like. The electronic wallet is an electronic collection of one or more of these types of physical materials that can be reviewed, viewed and used electronically to achieve similar results to the physical analogs." *Pitroda (Ex.1027),* [0025].

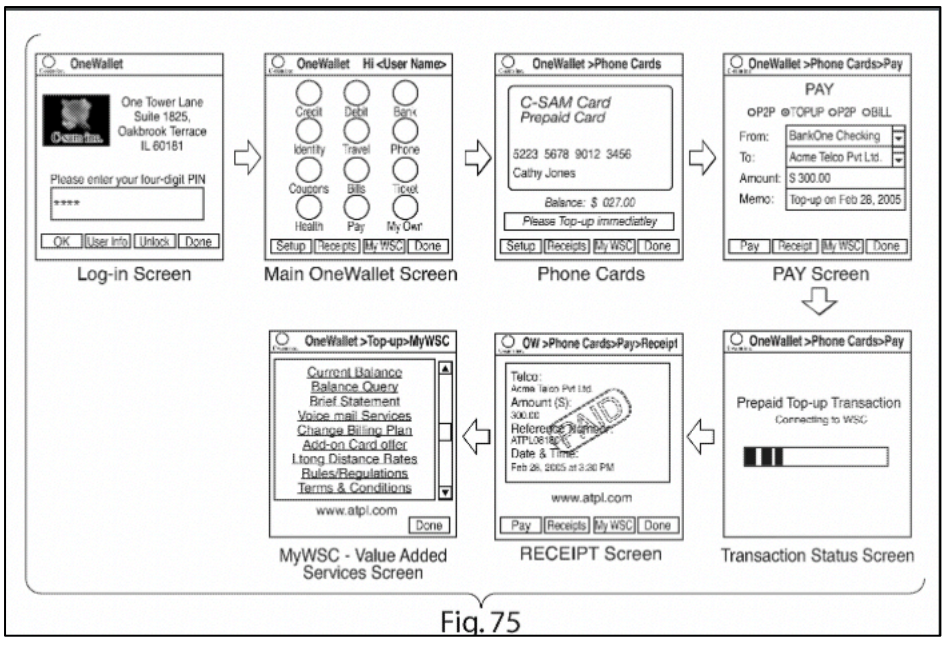


Fig. 75

Pitroda (Ex.1027), Fig. 75. A user can "view and manage mobile payment cards and other applications…through the mobile wallet graphical user interface." *Smart (Ex.1026),* 11.

63. In 2007, a Q2 Wallet trial was run. The Q2 Wallet "eliminates the need for users to carry Oyster smart cards in their wallets. Users can pay for their travel expenses through the Oyster application by simply touching their mobile phones to the Oyster NFC readers at London underground tube stations, on buses, and on trams." *Coskun (Ex.1021),* 35; *see* also *Coskun (Ex.1021),* 346. Nokia 6131, one of the first NFC enabled phones was the piolet test phone for the Q2 Wallet. *Coskun (Ex.1021),* 346. ("About 500 O2 mobile network subscribers participated in the pilot and they were equipped with Nokia 6131 NFC enabled mobile phones.")

Figure 9.8 O2 Wallet [1]. Photographed by Juha Sarkkinen, The City of Oulu, Smart Touch Project.

Coskun (Ex.1021), 347.

64. As another example, "Yapı Kredi Bank and the MNO Turkcell collaborated in the NFC enabled mobile-wallet service. The service is launched commercially in 2011 [7]." *Coskun (Ex.1021),* 345. Turkcell's mobile wallet software is preloaded and "supports more than one bank-issued application." *Id.*

65. By 2012 the use of mobile phones with mobile wallets was well known. For example, MasterCard PayPass Wallet was released. *PayPass (Ex.1025),* 1. ("integrate PayPass Wallet into its mobile application.") MasterCard also released a list of 42 "Approved Mobile Devices"—including phones from Google, Intel, LG, Asus, HTC, Nokia, BlackBerry, Samsung, Zony, and ZTE—all of which supported at least one mobile payment wallet. *MasterCard Mobile Partner (Ex.1028)*, 1.

7. *Card Emulation Mode*

66. A mobile phone can perform transactions via the mobile wallet using card-emulation mode. *Finkenzeller (Ex.1024),* 59. ("the electronic device behaves like a contactless smart card; this option is also called 'card mode' or '*card-emulation mode*'."); *see also Coskun (Ex.1021),* 78. ("card emulation mode provides smart card capability for mobile phones.")

67. In "card emulation mode, the RF interface is based on the ISO/IEC 14443 (Type A, Type B) standard and FeliCa." *Coskun (Ex.1021),* 96. "Either an

NFC enabled mobile phone emulates an ISO 14443 smart card or a smart card chip integrated in a mobile phone is connected to the antenna of the NFC module." *Coskun (Ex.1021),* 111. A NFC application needs a Graphical User Interface (GUI) and Secure Element (SE) application. *Coskun (Ex.1021),* 152 ("GUI (Graphical User Interface) application which must be present for all operating mode applications and provides both a GUI for the user and the capability to read NFC components…Secure Element (SE) application which is needed in order to provide a secure and trusted environment for applications"). The SE may be within the mobile phone or a remote-SE.

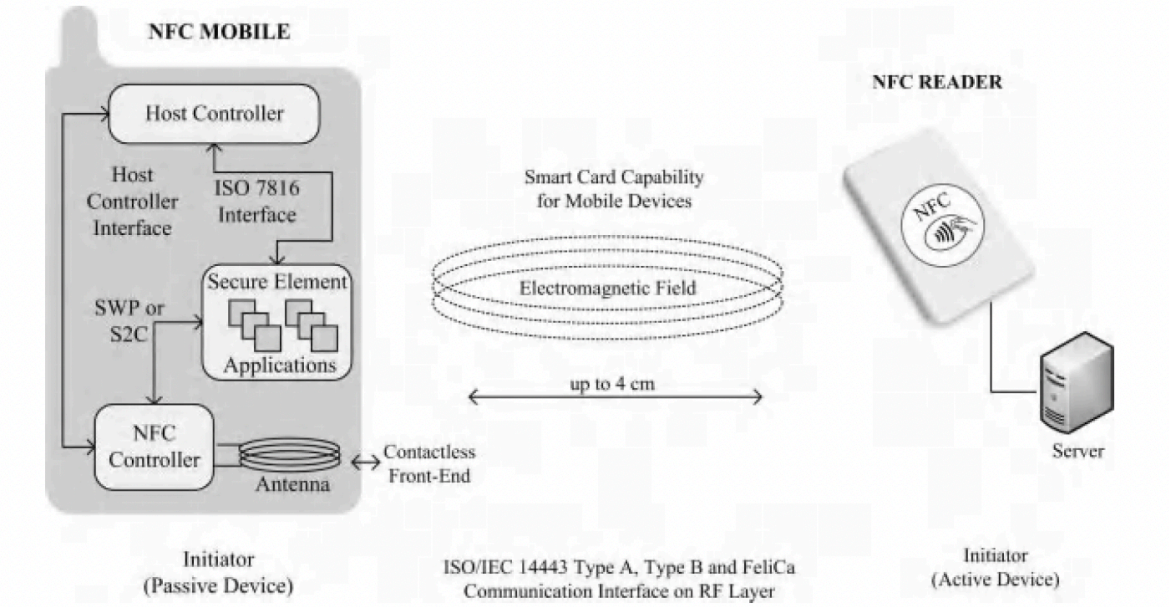


Figure 3.32 Communication architecture of card emulation operating mode.

Coskun (Ex.1021), Figure 3.32. It is worth noting that the above phone includes a secure element.

68. In the instance where a phone does not include a secure element, the mobile phone still needs a way to provide a secure and trusted environment for applications. Often, the mobile phone will have a remote-SE located outside of the mobile phone's hardware. As an example, "the NFC mobile device has the ability to use a SE for the transaction that is not physically located in the mobile device. This may be done be creating a data connection to a remote SE for which is used for the payment transaction. In step 757, while the phone is being placed into card emulation mode, the connection to the remote SE that will be used for emulation is attempting to connect. As illustrated in step 758 there is a chance that the connection is already open in which case the flow in FIG. 14 will simply allow the ISO/IEC 7816-4 APDU data to pass directly through the connection to the remote SE and back 763successfully completing the transaction 764. There is also a chance that the connection to the remote SE does not exist and needs to be created, as described subsequently in step 762." *Yeager (Ex.1029),* [0089].

C. Payment Credential Security Features

69. With the increase in contactless payment transactions came additional opportunities for malicious intent to gain unauthorized access to a user's payment information. Below, I describe an exemplary group of prior art attempts to prevent fraud and protect sensitive information.

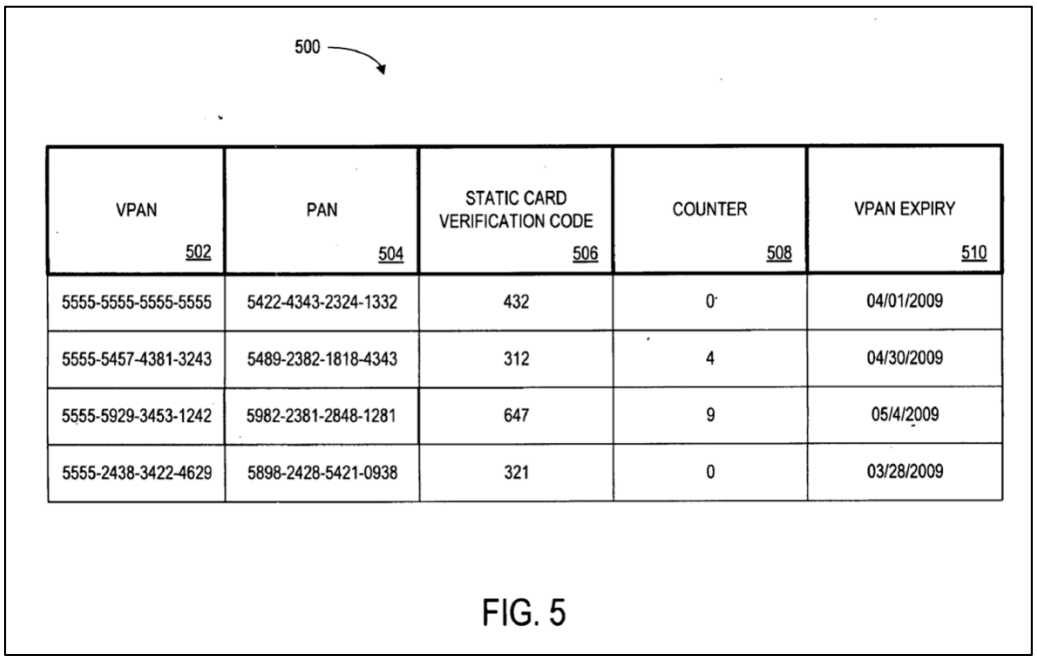
1. Alternatives to a Payment Account Number (PAN)

70. Early payment cards (e.g., magnetic stripe cards) lacked significant security protocols to protect customer's payment account numbers (PAN). However, the integration of tokenization—replacing a PACN with a cryptographically created replacement called a token—into the payment card industry allowed for substantially more secure payment transactions. *EMVCo (Ex.1030),* 6, 9.

71. Using these limited-use numbers or tokens in place of the PAN was well-known long before the Critical Date. In fact, in August of 2011, PCI SSC adopted tokenization guidelines. *PCI SSC (Ex.1031),* 5. Tokenization replaces "sensitive PAN values with non-sensitive token values." *PCI SSC (Ex.1031),* 5. Non-sensitive means that the number does "not require any security or protection" because "the token has no value to an attacker." *PCI SSC (Ex.1031),* 5. These limited-use tokens are either "single-use or multi-use." *PCI SSC (Ex.1031),* 5. Using tokens "instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment[.]" *PCI SSC (Ex.1031),* 3. PCI SSC also teaches that "[o]ne of the primary goals of tokenization solution should be to replace sensitive PAN values with non-sensitive token values." *PCI SSC (Ex.1031),* 5.

72. Another alternative to the PAN is called a virtual PAN (VPAN). As an example, Kranzley teaches that each "VPAN 502 is associated with a PAN 504.

That is, each VPAN 502 is associated with an actual payment account number that has been issued to a cardholders" *Kranzley (Ex.1013),* [0066]. Each VPAN is also "associated with the static card verification code 506 from the payment account." *Kranzley (Ex.1013),* [0066]. In Figure 5 "[t]he table includes entries identifying VPANs that have been issued or assigned by the payment provider 110."



VPAN 502	PAN 504	STATIC CARD VERIFICATION CODE 506	COUNTER 508	VPAN EXPIRY 510
5555-5555-5555-5555	5422-4343-2324-1332	432	0	04/01/2009
5555-5457-4381-3243	5489-2382-1818-4343	312	4	04/30/2009
5555-5929-3453-1242	5982-2381-2848-1281	647	9	05/4/2009
5555-2438-3422-4629	5898-2428-5421-0938	321	0	03/28/2009

FIG. 5

Kranzley (Ex.1013), Fig. 5. The "VPANs processed over the payment network operated by MasterCard International Incorporated, VPANs are 16 digit numeric codes in which the first 6 digits are used to identify the VPAN as a VPAN to be routed to a payment provider 110 for processing." *Kranzley (Ex.1013),* [0065].It was well known in the art that replacing a PAN with a different number increases security. For example, an article titled "Security in Mobile Payments" by Vizzarri et

al. ("Vizzarri") teaches different techniques to guarantee security in m-payment systems. *Vizzarri (Ex.1032*), 1-6. Classical methods are end-to-end encryption and tokenization. With tokenization an encrypted or random value, called token, replaces the card number (PAN) or the magnetic stripe track data in an electronic transaction. The token then becomes the reference number representing the card number, so all tokens can be referenced back to the original card number." *Vizzarri (Ex.1032*), 5. As an additional example, Grigg teaches a "mobile wallet account number" that "is a distinct number that is different from any traditional financial institution account number or any other account number associated with a payment device...[that] may be utilized for a transaction for a product." *Grigg*, [0011]. Grigg teaches that the mobile wallet on the user device 204 will be assigned a "mobile wallet account number" to be used by the user device 204 in place of a traditional account number such as a credit card number (PAN). *Grigg,* [0006], [0047], [0051]. Grigg notes that the payment device or devices are for example, "credit cards" or a "payment device account number (such as a traditional bank account number) [.]" *Grigg*, [0002], [0006]. Grigg notes that each payment device has a "different mobile wallet account number[.]" *Grigg*, [0011], [0003] ("[A] mobile wallet is typically associated with the individual's mobile device[.]"). In Grigg, the financial institution application "provide[s] the user 202 via the user device 204 the assigned mobile wallet account

number." *Grigg*, [0053]. This mobile wallet number "may be permanently associated with the mobile wallet" *Grigg*, [0051]. "[A] user 202 may use his/her user device 204 as a mobile wallet" to make payments at a point-of-transaction (POT) or online. *Grigg,* [0043].

2. Alternatives to Static Card Verification Values

73. Another method to increase security in transactions comes in the form of the card verification value (CVV- Visa) or card verification code (CVC - MasterCard). The banking industry "developed a type of "password" for use with credit and debit cards. This password takes the form of an authentication code and is commonly referred to in the industry as a "card verification value" or "CVV." *Ashfield (Ex.1033),* [0002]. A CVV is "a "3-digit security code[.]" *Id*.

74. To increase security in transactions, a one-time use dynamic CVV/CVC code may be generated. For example, this "dynamic CVV can be compared to at least a portion of a one-time password generated for the specific credit/debit card, and a transaction authorization can be sent to the merchant or vendor when the dynamic CVV matches all or a portion of the one-time password. A transaction denial can be sent when the dynamic CVV does not match." *Ashfield (Ex.1033),* [0005]. The bank "can separate the dynamic CVV from credit/debit card data, validate the credit/debit card data, and then merge the CVV with the credit/debit card

data once the dynamic CVV is authenticated to produce the transaction authorization." *Id*.

75. Mastercard uses a CVC3 value and Visa uses a dCVV value to replace the static CVV. For example, Bona teaches "the static CVV value with the dynamic dCVV or CVC3 codes (in the embodiments where the data is formatted for VISA® and MASTERCARD® transactions, respectively) [.]" *Bona (Ex.1019),* [0037]. Kranzley teaches "in the case of a MasterCard payment card, the static card verification code 506 may be the MasterCard CVC number printed on the back face of a MasterCard credit or debit card." *Kranzley (Ex.1013)*, [0066]. Bona notes that "[t]hese one-time (i.e., dynamic) codes are generated by the smart card chip and are unique to each transaction." *Bona (Ex.1019),* [0037]. Dynamic data such as a CVC3 "would provide sufficient information in the payment authorization process to eliminate both 'card present' and 'card not present' fraud." *Bona (Ex.1019),* [0037]. Yeager teaches that "[e]xamples of cryptograms at the time of this filing are defined by the following card specification in table 4." *Yeager (Ex.1029)*, [0162].

TABLE 4

Card specification	Cryptogram Designator or Name
MasterCard PayPass MSD	CVC3
Visa Contactless MSD	dCVV
Discover ZIP MSD	dCVV
EMV, Visa QVSDC, VISA VSDC, MasterCard MCHIP	AC, TC, AAC, ARQC

Yeager, Table 4. Yeager teaches "[a] "cryptogram" as used herein may be classified as "dynamic" meaning that it is always changing from one interrogation (transaction) to the next[.]" *Yeager (Ex.1029)*, [0162].

76. A cryptogram, as the name suggests, is a value created cryptographically. As an example, a cryptographic hash function can be used to map an input string of values to a fixed size output. *Rosulek, Ex.1046*. At its core, a hash function is simply a mathematical function that converts input data into an output string (called the hash) with a fixed number of characters. Hash functions are a commonly used cryptography tool because a small change in one of the inputs will create an entirely different hash. *Id.* The hash therefore can be used as as an authenticity check.

VIII. SUMMARY OF PRIOR ART REFERENCES

A. Collinge

77. Collinge was filed on March 14, 2013, and claims priority to the following provisional applications: Ex.1005 (U.S. Provisional Appl. No. 61/619,095, filed April 2, 2012 ("'095 Provisional")); Ex.1006 (U.S. Provisional Appl. No. 61/635,248, filed April 18, 2012 ("'248 Provisional). Ex.1004 (Collinge). Collinge was neither cited nor discussed during prosecution of the '820 Patent. *'820 Patent (Ex.1001),* (56); *'820 File History (Ex.1002)*. Collinge teaches "[a] method for generating and provisioning payment credentials to a mobile device lacking a secure element" which payment credentials may be used "in conducting a near field financial transaction." *Collinge (Ex.1004),* Abstract; [0002]. Collinge teaches that a user may register their mobile device for use in contactless payments and install a mobile payment application on the mobile device. *Collinge (Ex.1004),* [0065]-[0066]. Collinge teaches that after registration, the mobile payment application of the mobile device is provisioned with a card profile and single use key from a remote secure element. *Collinge (Ex.1004),* [0068]-[0069]; Fig. 5.

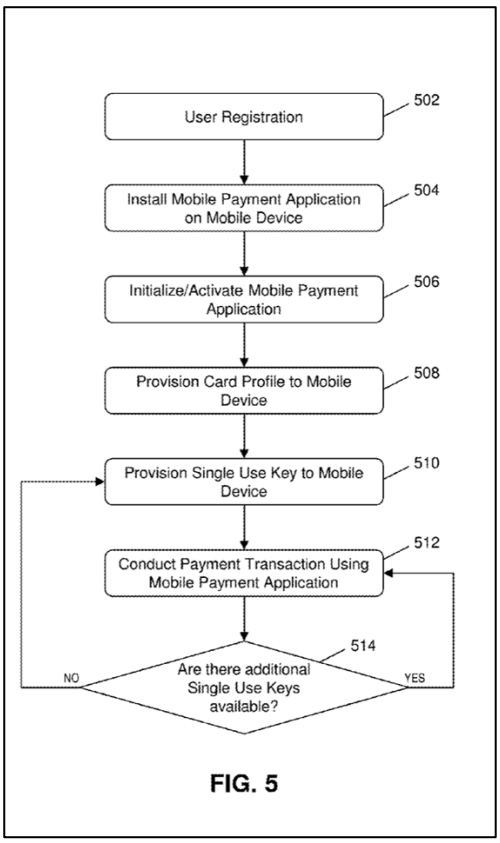


FIG. 5

Using the provisioned single use key, the mobile payment application within Collinge's mobile device generates a payment cryptogram valid for a single financial transaction. *Collinge (Ex.1004),* [0069]. The generated single-use "payment cryptogram may be, for example, an application cryptogram or a dynamic card validation code (CVC3)." *Collinge (Ex.1004),* [0077]. Collinge's mobile device "may conduct a contactless/NFC payment transaction" by "transmit[ting] the generated payment cryptogram and payment credentials to a point-of-sale terminal[.]" *Collinge (Ex.1004),* [0070], [0077].

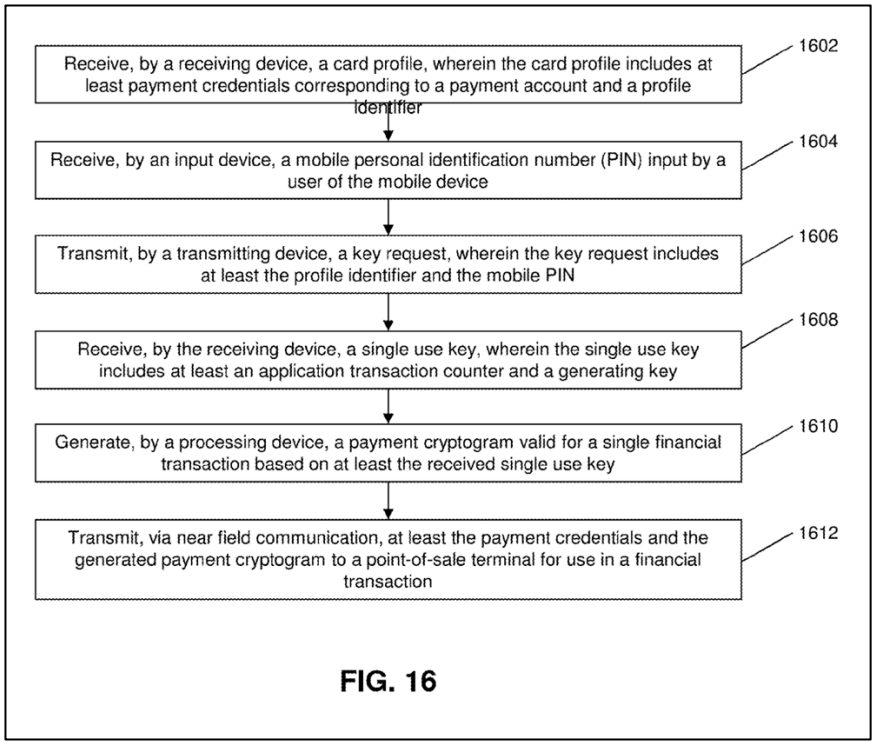


FIG. 16

Collinge (Ex.1004), Fig. 16. It is my understanding Collinge is entitled to a priority date of April 18, 2012 for the reasons discussed below. As I produced below, a table of key terminology used throughout Collinge.

Abbreviation in Collinge	***Meaning in Collinge***	***Mapping in Petition***
KS_{UN} *Collinge*, Fig. 17, [0141], [0145].	session key unpredictable number	Secret used to generate and validate a payment cryptogram. Shared with issuer.
UN_{CLOUD} *Collinge*, Fig. 17, [0141].	cloud unpredictable number	Issuer secret used to validate a payment cryptogram.
single use key Collinge, [0128]	single use key	Secret used to generate and validate a payment cryptogram. Shared with issuer.

PAN Collinge, [0048]-[0049].	Primary/payment account number	For example, a traditional 16-digit credit card number is a PAN.
ATC *Collinge*, Fig. 18, [0141], [0145].	Application transaction counter	Transaction counter, also shared with issuer
CVC3 *Collinge*, Fig. 18, [0145].	A type of payment cryptogram used in contactless magstripe transactions (AC is the other payment cryptogram used in chip transactions)	Limited-use payment information used in place of the static CVC.
UN_{READER} *Collinge*, Fig. 18, [0145].	Reader unpredictable number	Device secret used to generate a payment cryptogram.

1. Collinge is Analogous Art

78. I have been informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be "analogous art" to the claimed invention. I have been informed that a prior art reference is analogous to the claimed invention if the reference is from the same field of endeavor as the claimed invention or if it is reasonably pertinent to the particular problem that the inventor was trying to solve.

79. A POSITA would have classified Collinge within the same field of endeavor as the '820 Patent because both Collinge and the '820 Patent relate to conducting secure payment transactions. For example, Collinge describes

provisioning and storage of payment credentials for use in conducting near field financial transactions. *Collinge (Ex.1004),* [0002]. Collinge further describes a remote system that generates and provides to a mobile device payment credentials that include a payment token payload, where the payload includes a card profile and single use key. *Collinge (Ex.1004),* [0043]. The mobile device can then use the single use key to generate a payment cryptogram for use in a financial transaction. *Collinge (Ex.1004),* [0070]. The ’820 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications. *’820 Patent (Ex.1001)*, 1:31-36, 3:1-10. Similar to Collinge, the ’820 Patent describes a credit card device that generates a limited duration payment credential using the user’s payment information for use in a financial transaction. *’820 Patent (Ex.1001),* 10:55-11:17.

80. Additionally, a POSITA would have found Collinge reasonably pertinent to the problem faced by the inventors of the ’820 Patent because both Collinge and the ’820 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. For example, Collinge describes a device and process for securely generating and transmitting payment credentials from a mobile device to a payment terminal (e.g., NFC point-of-sale terminal). *Collinge (Ex.1004),* [0003]-

[0007]. Likewise, the ’820 Patent describes that its invention “address security concerns of a credit card owner” for use in RFID transactions. *’820 Patent (Ex.1001),* 9:56-62. Accordingly, a POSITA would have considered Collinge analogous art to the ’820 Patent.

2. Collinge is Prior Art

81. Collinge was filed on March 14, 2013, and is therefore prior art because it was filed earlier than the priority date of ’820 Patent’s provisional application, filed on March 15, 2013.

82. In the event that Cardware attempts to demonstrate that it is entitled to a date earlier than March 15, 2013 based on a showing of earlier conception and reduction to practice, it is additionally my understanding that Collinge is entitled to a prior date at least as early as April 18, 2012 based on Collinge’s provisional application filed on and before that date (Provisional Nos. 61/619,095 (Ex.1005), filed April 2, 2012 (“*’095 Provisional*”), and 61/635,248 (Ex.1006) filed April 18, 2012 (“*’248 Provisional*”) (collectively, “Collinge’s April 2012 Provisionals”).

83. I understand that for Collinge to be entitled to the April 18, 2012 filing date of the ’248 Provisional, Collinge’s April 2012 Provisional must contain a written description of the invention to have enabled a POSITA to practice the invention claimed in the non-provisional application. I have reviewed the Collinge

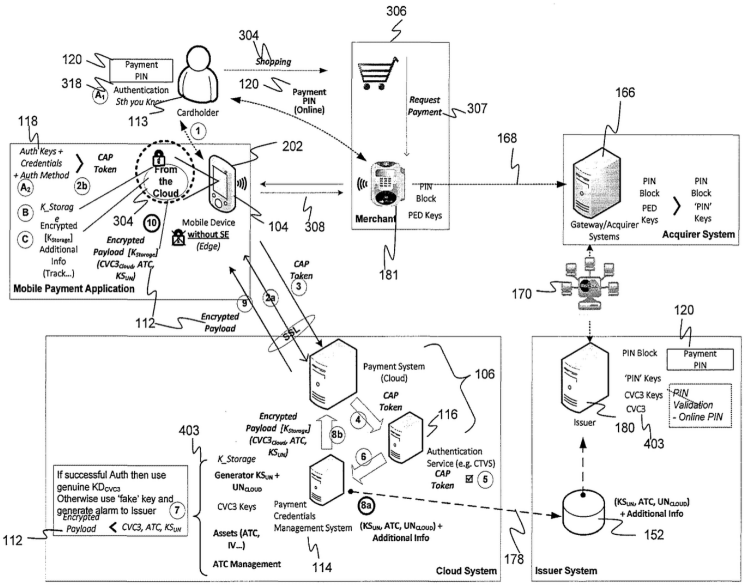
Provisional and it is my opinion Collinge's April 2012 Provisionals provide a detailed disclosure of the provisioning, storage and use of payment credentials for use in an NFC financial transaction disclosed and claimed in Collinge, including storing a storage key, a plurality of dynamic card validation codes ("DCV3"), and an application transaction counter ("ATC"); providing the storage key, an authentication component, and static payment credentials to a mobile device; validating a mobile device using a CAP token; generating a session key and cloud unpredictable number; identifying an encrypted payload, that includes a DCV3, the session key unpredictable number and ATC, based on a derived dynamic card validation code; transmitting the encrypted payload to the mobile device to generate a DCV3 for use in a financial transaction; and, transmitting the session key and cloud unpredictable number and ATC to an issuer for use in validating the DCV3 generated by the mobile device, which is similar to the level of disclosure in Collinge itself. In my opinion, Collinge's April 2012 Provisionals provide sufficient written description to enable a POSITA to practice the inventions claimed in at least claim 20 of Collinge.

84. The table below identifies where, for example, written description support can be found in Collinge's April 2012 Provisionals for claim 20 of Collinge.

The disclosure of Collinge's April 2012 Provisionals provide similar detail to Collinge itself, and enables a POSITA to practice claim 20 of Collinge.

Collinge (Ex.1004)	**Supporting Disclosure from Collinge's April 2012 Provisionals – the** *'095 Provisional*" (Ex.1005) and the *'248 Provisional* (Ex.1006).
20. A method for generating and provisioning payment credentials to a mobile device lacking a secure element, comprising:	The Collinge Provisionals disclose methods for provisioning payment credentials to a mobile device lacking a secured element. "The present disclosure is directed to a method and system providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in the mobile device using in part a financial transaction card processing system or network as a part thereof."[1] '095 Provisional (Ex.1005), ¶0001 "According to an embodiment, a set of processes deliver solutions for contactless payments, such as online transactions at a Point-of-Sale (POS), when using a mobile device but not requiring use or presence of an SE. One embodiment uses a combination of remote authentication and the provisioning of payment credentials to the mobile device for one transaction. In an alternative embodiment, remote authentication is performed and payment credentials are provisioned to a mobile device without an SE for a limited number of transactions." '095 Provisional (Ex.1005), ¶0005

[1] Unless otherwise noted, all emphasis is added.

	 '095 Provisional (Ex.1005), Fig. 5
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;	The Collinge Provisionals disclose storing in a database of the payment credentials management a storage key ($K_{Storage}$), a plurality of dynamic card validation code keys (CVC3), and an application counter (ATC) associated with a mobile application program. "As shown in Figure 1, the cloud-based transaction data generation system 106 further comprises key storage 110 for storing keys and encrypted information 113. In the exemplary embodiment of Figure 1, the encrypted information 113 has been encrypted using $K_{storage}$ and includes Track 1 data, and/or Track 2 data. As shown in Figure 1 the encrypted payload 112 is provisioned to the mobile device 104 from the cloud-based transaction data generation system 106. The cloud-based transaction data generation system 106 also includes a payment credentials management system 114 and an authentication service 116." '095 Provisional (Ex.1005), ¶0038 "The payment credentials management system 114 may manage the CVC3 keys 403." '095 Provisional (Ex.1005), ¶0066

"Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below:
▸ Storage Key ($K_{storage}$) defined at time of authentication profile and static Payment credentials provisioning."

'095 Provisional (Ex.1005), ¶0068

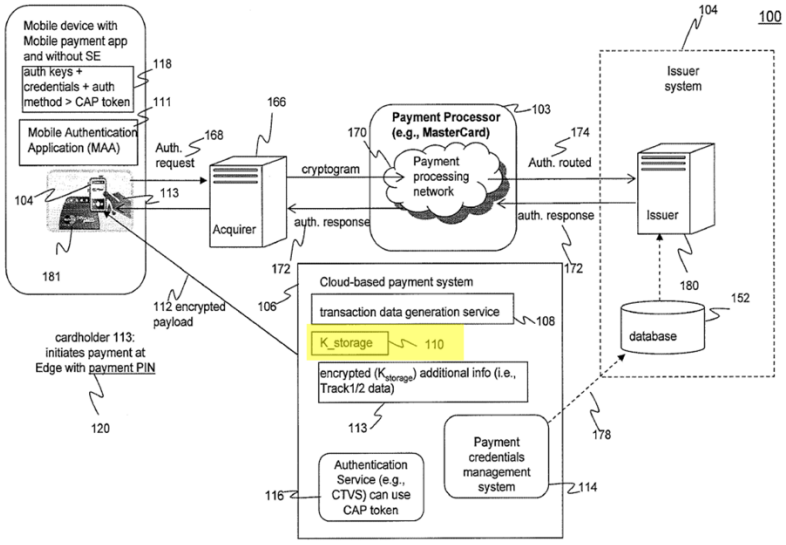
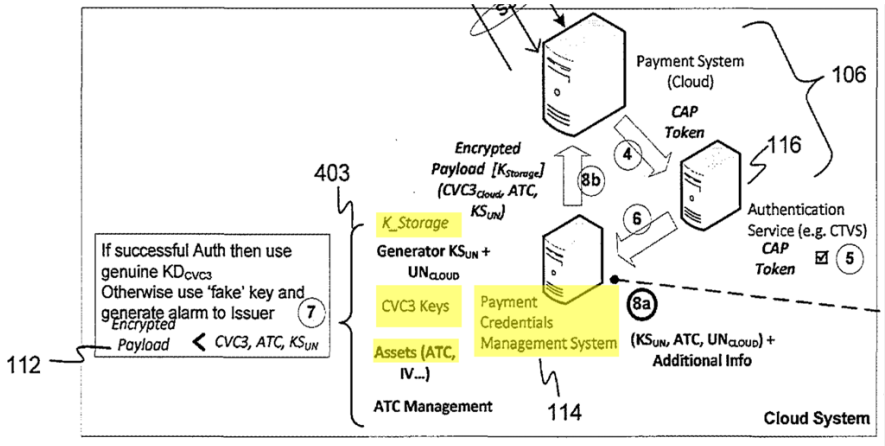


FIG. 1

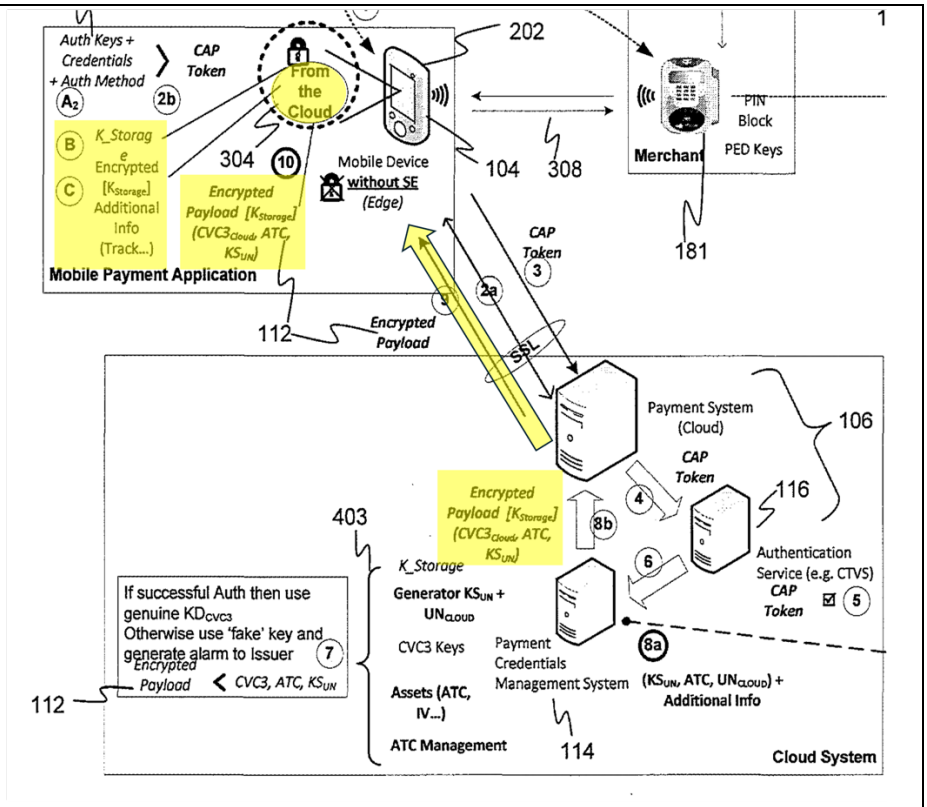
'095 Provisional (Ex.1005), Fig. 1.



'095 Provisional (Ex.1005), Fig. 5 (annotated excerpt); *see also* '095 Provisional (Ex.1005), Figs. 4, 6-8

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 Collinge Provisionals disclose providing the mobile device a storage key, an authentication component, and static payment credentials associated with a payment account. "In step 205, authentication credentials associated with a payment card are provisioned to the mobile device 104." '095 Provisional (Ex.1005), ¶0051 **B** At time of the authentication credentials provisioning, a storage key is also stored in the Mobile Payment Application. This key is used to protect the static payment credentials and the transport of the payload from the Cloud to the Mobile Payment Application **C** At time of the authentication credentials provisioning, static payment credentials are also provisioned '095 Provisional (Ex.1005), Table 1 (p. 15) "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." '095 Provisional (Ex.1005), ¶0062 "Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below: ► Storage Key ($K_{storage}$) defined at time of authentication profile and static Payment credentials provisioning. ► Authentication credentials protected using MAA rules (e.g. Key Camouflage) (Not using $K_{storage}$) *** ► The values KD_{CVC3} and $IVCVC3_{Trackl/2}$ are static (if one considers a given PAN (and PSN) value, the values KD_{CVC3} and $IVCVC3_{Trackl/2}$ remain the same during the entire lifespan of the card. Those values are static. It also means that once the value is disclosed, you can reuse it.) for a given PAN (and PSN). The PSN (if available) can be part of the KD_{CVC3}

	derivation process. This avoids mandating any change regarding the management of this value at issuer level even if the PSN may be used to identify a SE-less 'virtual card' defined for a given PAN. *** ► Delivery of Encrypted Payload [using $K_{storage}$] (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$ and ATC) to Mobile Payment Application" '095 Provisional (Ex.1005), ¶0068 "(Static) Information known by the Mobile Payment Application ◊ FCI (PPSE) ◊ AID (Application Identifier) ◊ FCI (File Control Information) ◊ AFL (Application File Locator) ◊ AIP (Application Interchange Profile) ◊ AVN (Application Version Number) ◊ Encrypted (using $K_{storage}$) Payment Credentials provisioned at time of authentication credentials provisioning." '095 Provisional (Ex.1005), ¶0071 (p. 22) "provisioning a storage key ($K_{storage}$), authentication credentials and static payment credentials associated with a payment account to the mobile device, wherein the $K_{storage}$ key is used to protect static payment credentials stored on the mobile device and the transport of a payload from the Cloud to the mobile payment application" '248 Provisional (Ex.1006), Claim 1



'095 Provisional (Ex.1005), Fig. 5 (annotated excerpt)

"As shown in Figure 9A, once these operations have been completed, the pull environment is ready, and the next phase can take place using the following processes: a process to send authentication credentials and Keys 918 and any needed static payment credentials 928 to a user (cardholder 113) of the mobile device 104, a remote authentication 824, a process to retrieve dynamic payment credentials 938 (i.e., using an encrypted payment token payload 112); and a process to synchronize 978 the cloud-based transaction data generation system 106 and issuer 180 systems."

'248 Provisional (Ex.1006), ¶0091

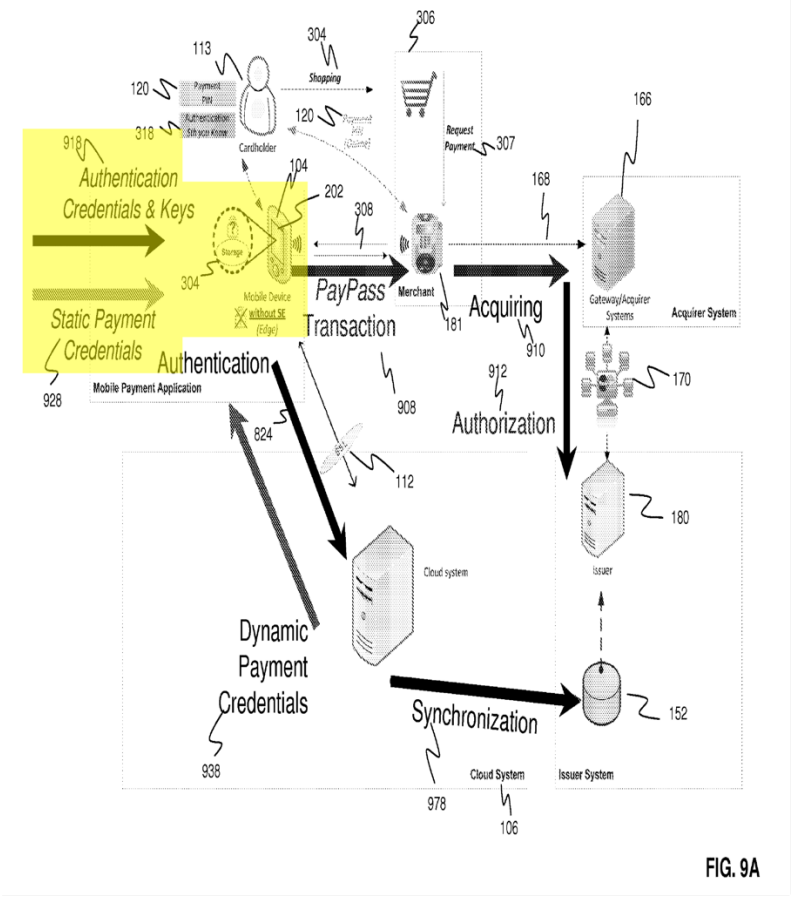


FIG. 9A

'248 Provisional (Ex.1006), Fig. 9A

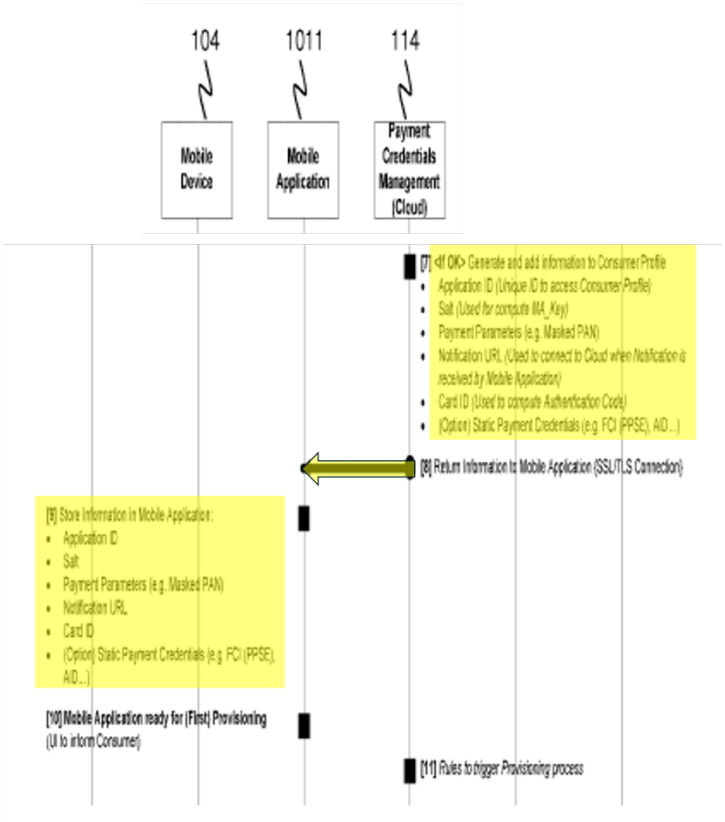
"The communications sequence depicted in Figure 11 encompasses pushing the following parameters/data to the mobile application 1011 as part of stage [7]: an application ID, which is a unique ID used to access the consumer profile (i.e., the profile for the user 113); a salt, which is a value used (in combination with the access code) in the cryptographic process (Fn_MA_Key) to generate the key used for transport and storage of the payment token payload; payment parameters including the required payment card artwork with a masked PAN value (e.g., XXXX XXXX XXXX 4321); a notification URL used to connect to the cloud-based transaction data generation system 106 to retrieve the encrypted payment token payload; and a card ID, which is a unique ID used in the generation (Fn_Auth_Code) of an authentication code. In an embodiment, the parameters

optionally further comprise some additional non-sensitive static payment credentials.

In stage [8], this information is returned to the mobile application 1011 via an SSL/TLS connection before proceeding to stage [9] where the information is stored in the mobile application 1011.

As shown in Figure 11, the information stored in stage [9], can include: an application ID, the salt, payment parameters (e.g. the Masked PAN), the notification URL, and the card ID. Optional information stored can include static payment credentials (e.g. FCI (PPSE), AID shown in Figure 11)."

'248 Provisional (Ex.1006), ¶¶0135-0137



'248 Provisional (Ex.1006), Fig. 11 (annotated excerpt)

"The following section provides further details for exemplary embodiments of the parameters, data elements and fields

	depicted in Figures 9-15 and described above with reference to those Figures. **Payment Token Payload** According to an embodiment, the Payment Token Payload contains four parts: ♦ Length ♦ Proof Information ♦ Payment Data (Static - Non Sensitive, Static - Sensitive, Dynamic) ♦ [End Tag] The Payment Token Payload is transported and stored in encrypted form using a Mobile Application Key (MA_Key). The process to derive this key is defined in *Fn_MA_Key*. *** The Payment Data contains all the data elements required to perform a Pay Pass Magstripe Transaction. In an embodiment, the detailed content of the Payment Token Payload is: ♦ *Length* ♦ *Proof Information* o Proof (Random - 5 bytes) ♦ *Static Payment Data* o FCI (PPSE) o AID o FCI (PayPass App) o AIP o APL ♦ *Static Payment Data (PayPass Transaction)* o PUNATC Track 1 o PUNATC Track 2 o PCVC3 Track 1 o PCVC3 Track 2 o NATC Track 1 o NATC Track 2 o UDOL ♦ *Static Payment Data (Sensitive Data)*

	o Track 1 Data o Track 2 Data ♦ *Dynamic Payment Data (Sensitive Data)* o IVS_CVC3 (Track 1 and Track 2) o ATC o KS_CVC3 ♦ *Control Data* o [End Tag]" '248 Provisional (Ex.1006), ¶¶0211-0213 "♦ The Mobile Payment Application can be: o A single "card". The PPSE has to be set with the AID of the "card". o Embedded in a Wallet. The AID must be added to the list of AID managed by the PPSE." '248 Provisional (Ex.1006), p. 155
receiving, from the mobile device, a chip authentication program (CAP) token;	The Collinge Provisionals disclose the mobile device sending a chip authentication program (CAP) to the cloud-based payment system. "A method for providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in a mobile device, comprising: …sending a token from a mobile authentication application (MAA) component of the mobile payment application to the Cloud; validating the token based on upon authentication credentials; …." '095 Provisional (Ex.1005), Abstract (p. 38) "The system 100 performs authentication using the MAA 111. According to an embodiment, the MAA 111 is a software implementation of MasterCard Authentication Solutions (two-factor authentication using a CAP Token). A CAP Token Generation Service (CTGS) can be integrated in a mobile application to build a MasterCard Authentication Solution for

mobile device 104 where the cardholder 113 uses the Mobile Authentication Application (MAA) to generate a CAP Token."

'095 Provisional (Ex.1005), ¶0031

"The cloud-based transaction data generation system 106 also includes a payment credentials management system 114 and an authentication service 116. In the exemplary embodiment of Figure 1, the authentication service 116 is configured to perform CVTS CAP Token validation (CTVS) and can use a Chip Authentication Program (CAP) token for authentication."

'095 Provisional (Ex.1005), ¶0038

2b	The Cardholder uses the MAA component of the Mobile Payment Application to generate a CAP Token for the authentication transaction. The Cardholder has to supply some credentials (e.g. A gesture, a password…)
3	Mobile Payment Application sends a CAP Token to the Cloud

'095 Provisional (Ex.1005), Table 1 (p. 15)

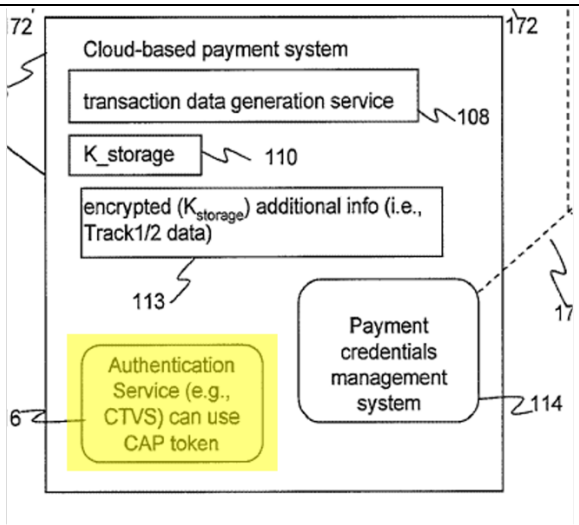
"forwarding payment credentials comprising at least one token from the Cloud to the mobile device;
receiving, at the Cloud, a token from a mobile authentication application (MAA) component of the mobile payment application;
validating the token based upon the authentication credentials and at least one additional credential received from the mobile device;"

'095 Provisional (Ex.1005), Claim 1

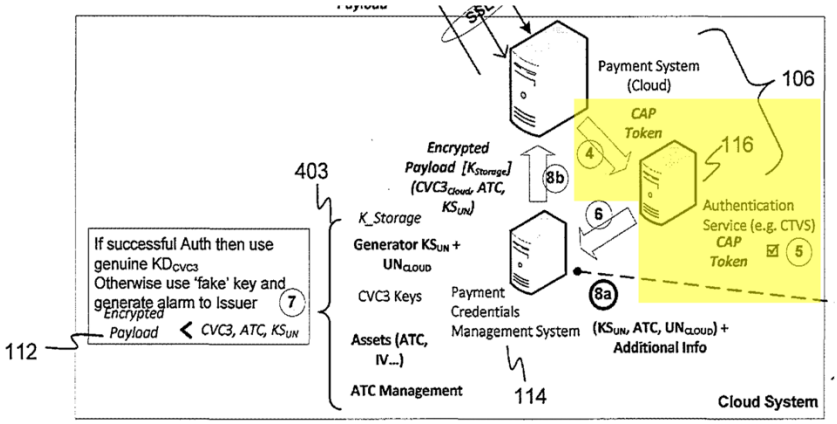
"9. The method of claim 1, wherein the token is a Chip Authentication Program (CAP) token indicating one or more controls on purchases."

'095 Provisional (Ex.1005), Claim 9

validating, by a validation device, the authenticity of the received CAP token;	The Collinge Provisionals disclose an authentication service validating the authenticity of the CAP token sent by the mobile device. "A method for providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in a mobile device, comprising: …sending a token from a mobile authentication application (MAA) component of the mobile payment application to the Cloud; validating the token based on upon authentication credentials; …." '095 Provisional (Ex.1005), Abstract "In accordance with another exemplary embodiment, mobile authentication and mobile payment services arc implemented as an online-only solution wherein a CAP token is verified online by a CAP Token Validation Service (CTVS)." '095 Provisional (Ex.1005), ¶0010 "In the exemplary embodiment of Figure 1, the authentication service 116 is configured to perform CVTS CAP Token validation (CTVS) and can use a Chip Authentication Program (CAP) token for authentication." '095 Provisional (Ex.1005), ¶0038 "As shown in Figure 5, the authentication service 512 in system 100 may be a CAP Token Validation Service (CTVS)." '095 Provisional (Ex.1005), ¶0066 **4** The Payment System (in the Cloud) validates the CAP Token using a CAP Token Validation Service (CTVS). The Payment System can be operated by MasterCard or by the Issuer. **5** The CTVS validates the CAP Token. The CTVS can be operated by MasterCard or by the Issuer. '095 Provisional (Ex.1005), Table 1 (p. 24)



'095 Provisional (Ex.1005), Fig. 1 (annotated excerpt)



'095 Provisional (Ex.1005), Fig. 5 (annotated excerpt); *see also* '095 Provisional (Ex.1005), Figs. 4, 6-8

"validating the token based upon the authentication credentials and at least one additional credential received from the mobile device;"

'095 Provisional (Ex.1005), Claim 1

"9. The method of claim 1, wherein the token is a Chip Authentication Program (CAP) token indicating one or more controls on purchases."

'095 Provisional (Ex.1005), Claim 9

generating, by a processing device, a session key unpredictable number (KS_{UN});	The Collinge Provisionals disclose a cloud-based payment system generating a session key unpredictable number (KS_{UN}). "Exemplary data flow stages depicted in Figures 5-7 are described in Table 1 below. *** 7 Upon successful authentication, a genuine KD_{CVC3} is used and (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$, ATC) is returned. " '095 Provisional (Ex.1005), Table 1 (p. 16) "Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below: *** ► Session key generation (KS_{UN}) in the Cloud to bind (ATC, UN_{CLOUD}, PAN and PSN) at the Edge (Mobile Payment Application)" '095 Provisional (Ex.1005), ¶0068 "A Glossary of terms and acronyms described above and depicted in Figures 3-8 is provided in Table 2 below: **Table 2** **Stage** **Description** *** UN Unpredictable Number '095 Provisional (Ex.1005), Table 2 (p. 26) "According to an embodiment, the principles for the synchronization process (between the Cloud-based transaction data generation system 106 to issuer 180) are as follows:

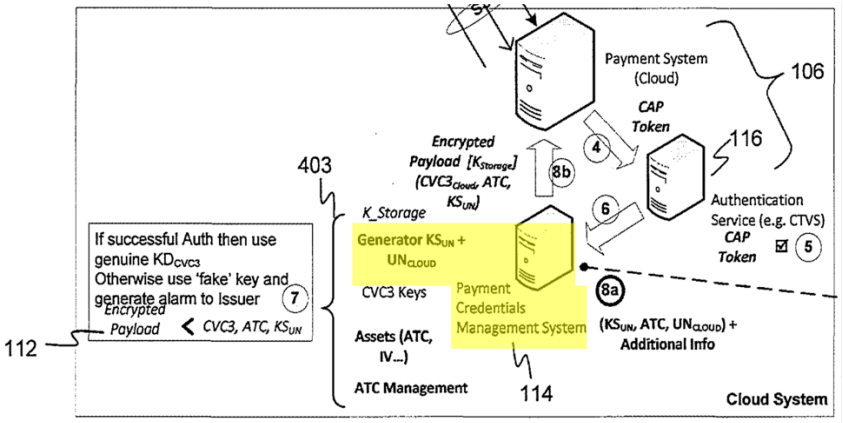
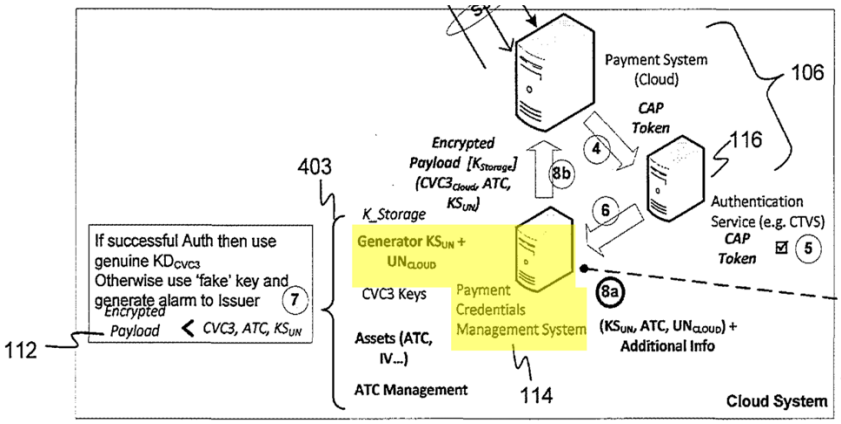
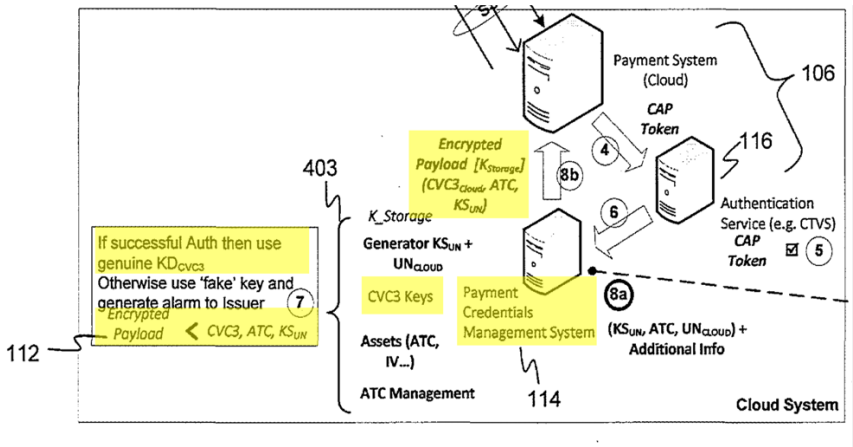
	1. The Cloud_CVC3$_{TRACK1/2}$ generation is managed in the Cloud-based transaction data generation system 106 ("the Cloud). This encompasses the generation of KS$_{UN}$ and UN$_{CLOUD}$, and the application transaction counter (ATC) management." '248 Provisional (Ex.1006), ¶0077; '095 Provisional (Ex.1005), ¶0056 (p.13)  '095 Provisional (Ex.1005), Fig. 1 (annotated excerpt); *see also* '095 Provisional (Ex.1005), Fig. 7
generating, by the processing device, a cloud unpredictable number (UN$_{CLOUD}$);	The Collinge Provisionals disclose a cloud-based payment system generating a cloud unpredictable number (UN$_{CLOUD}$). "According to an embodiment, the principles for the synchronization process (between the Cloud-based transaction data generation system 106 to issuer 180) are as follows: 1. The Cloud_CVC3$_{TRACK1/2}$ generation is managed in the Cloud-based transaction data generation system 106 ("the Cloud). This encompasses the generation of KS$_{UN}$ and UN$_{CLOUD}$, and the application transaction counter (ATC) management." '248 Provisional (Ex.1006), ¶0077; '095 Provisional (Ex.1005), ¶0056 (p.13) "A Glossary of terms and acronyms described above and depicted in Figures 3-8 is provided in Table 2 below:

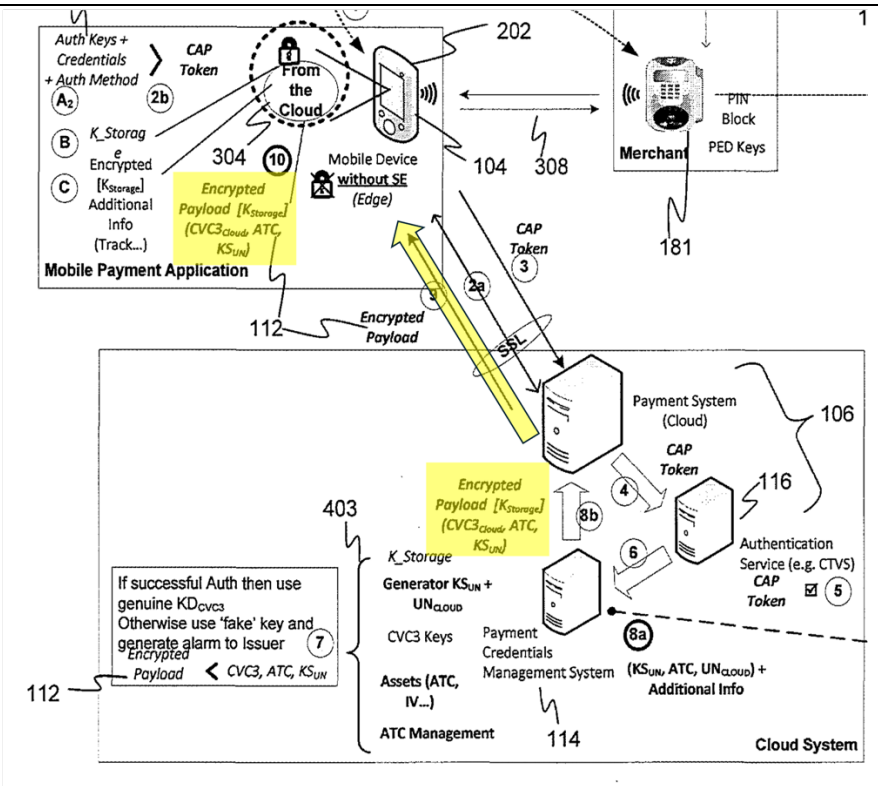
	Table 2 **Stage** **Description** *** **UN** Unpredictable Number '095 Provisional (Ex.1005), Table 2 (p. 25)  '095 Provisional (Ex.1005), Fig. 5 (annotated excerpt); '095 Provisional (Ex.1005), Fig. 4, 6-7
identifying, by the processing device, an encrypted payload based on a derived dynamic card validation code key (KD_{CVC3}), wherein the encrypted payload includes at least a dynamic card validation code key of the	The Collinge Provisionals disclose the cloud-based transaction data generation system identifying an encrypted payload, including a dynamic card validation code (CVC3), KS_{UN}, and an application transaction counter (ATC), based on a dynamic card validation code key (KD_{CVC3}). "4. If the validation of the CAP Token is successful, the cloud-based transaction data generation system 106 generates the CVC3 value using a genuine KD_{CVC3} and returns an encrypted payload to the Mobile Payment Application." '095 Provisional (Ex.1005), ¶0056 (p.13) **7** Upon successful authentication, a genuine KD_{CVC3} is used and (KS_{UN}, $Cloud\_CVC3_{TRACK1/2}$, ATC) is returned. '248 Provisional (Ex.1006), Table 1 (p. 16)

plurality of dynamic card validation code keys, the KS_{UN}, and the application transaction counter;	"Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below: *** ▸ Key derivation process in the Cloud (KD_{CVC3} + KD_{UN})" '095 Provisional (Ex.1005), ¶0068 (p.20)  '095 Provisional (Ex.1005), Fig. 5 (annotated excerpt); *see also* '095 Provisional (Ex.1005), Figs. 4, 6-8 "in response to determining that the authenticating was successful, including a genuine CVC3 derived key (KDcvc3) in the payment credentials and returning an encrypted payload to the mobile device including at least one of the KSUN, the Cloud_ CVC3TRACK1/o2r, the ATC" '095 Provisional (Ex.1005), Claim 1
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	The Collinge Provisionals disclose the cloud-based transaction data generation system transmitting the encrypted payload the mobile device for use in generating a dynamic card validation code for use in a financial transaction "The present disclosure is directed to a method and system providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in the mobile device using in part a

financial transaction; and	financial transaction card processing system or network as a part thereof." '095 Provisional (Ex.1005), ¶0001 "As shown in Figure 1 the encrypted payload 112 is provisioned to the mobile device 104 from the cloud-based transaction data generation system 106." '095 Provisional (Ex.1005), ¶0038 "The mobile payment application may generate a cryptogram. This cryptogram may be forwarded with the authorization request 168 to the acquirer 166. As shown in Figure 1, this can be further sent to the payment processing network 170. In an embodiment, the cryptogram 178 may be generated using key management services (i.e., through CVC3 validation, including dynamic CVC3 validation). The payment processor 103 then routes an authorization request 168 based on the payment credentials 174 and the cryptogram 178 to the issuer 180 and the issuer 180 responds to the authorization request 168 with the authorization response 172. In one embodiment, system 100 includes a connection 178 between the issuer 180 and a payment credentials management system 114. After receiving the authorization response 172, the payment processor 103 forwards the authorization response 172 to the acquirer 166, which in tum routes the authorization response 172 back to the POS terminal 181." '095 Provisional (Ex.1005), ¶¶0044-0047; '248 Provisional (Ex.1006), ¶¶0053-0055 **"Payment Process** The principles for the payment process (Mobile to Cloud) are: 1. The Mobile Payment Application must have retrieved at least one (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$, ATC) before the Tap.

	2. The dynamic values (CVC3 and ATC) are used as a first form factor to authenticate the payment transaction. The Online PIN can be used as a second form factor." '095 Provisional (Ex.1005), ¶0056. "► Delivery of Encrypted Payload [using $K_{Storage}$] (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$ and ATC) to Mobile Payment Application" '095 Provisional (Ex.1005), ¶0068. "4. If the validation of the CAP Token is successful, the cloud-based transaction data generation system 106 generates the CVC3 value using a genuine KD_{CVC3} and returns an encrypted payload to the Mobile Payment Application." '095 Provisional (Ex.1005), ¶0056. "Encrypted (using $K_{Storage}$) Payload sent to the Mobile Payment Application (Valid for one contactless payment transaction) ◊ Cloud_$CVC3_{TRACKl/2}$ ◊ ATC ◊ KSUN '095 Provisional (Ex.1005), p. 23 "Payload sent to the Issuer ◊ Identifier (PAN ...) ◊ UNCLOUD ◊ ATC ◊ Authentication Status Info+ Additional Generation Information (e.g. Validity) **$CVC3_{TRACKl/2}$** Mobile Payment Application to perform CVC3 generation using: ◊ Information from the Reader ◊ Stored Information ◊ Credentials previously retrieved from the Cloud

	CVC3 value to be included in Payment Authorization message (Track 2 (and Track 1) information). '095 Provisional (Ex.1005), p. 23 "Issuer Validation Process An exemplary validation process is described below wherein the Issuer 180 uses the information provided in the payment transaction: • Identifier - e.g. PAN Information • UN_{READER} (4 bytes) - Partial Information retrieved from Track data (Discretionary Information) • ATC (2 bytes)-Partial Information retrieved from Track data (Discretionary Information) • $CVC3_{TRACK1/2}$ Partial Information retrieved from Track data (Discretionary Information) *** The Issuer can validate the **$CVC3_{TRACK1/2}$**." '095 Provisional (Ex.1005), ¶¶0072-0074 "The dynamic values (CVC3 and ATC) are used as a first form factor to authenticate the payment transaction. The Online PIN can be used as a second form factor. This dynamic CVC3 value is generated by the mobile payment application using information from the payload provided by the cloud-based transaction data generation system 106 ('the Cloud')." '095 Provisional (Ex.1005), ¶0112

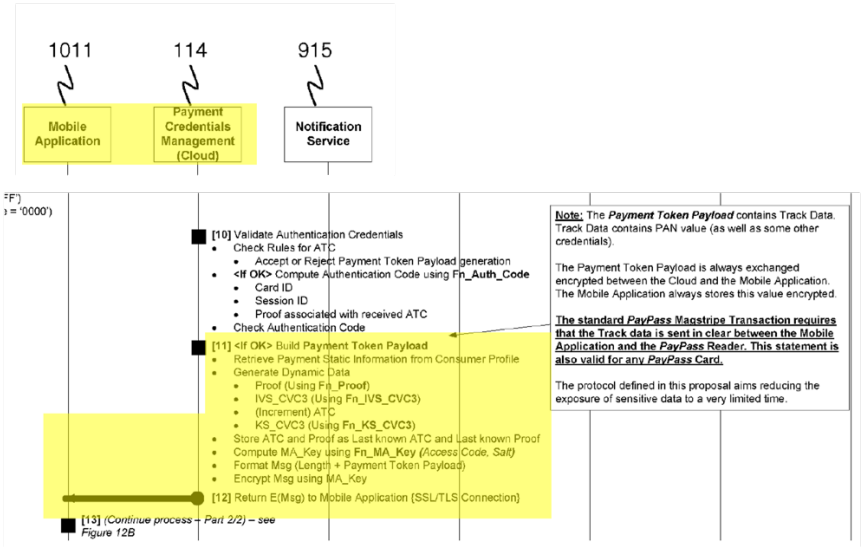
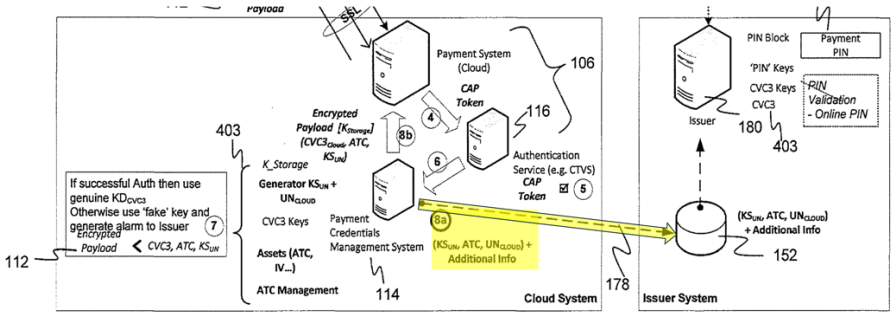


'095 Provisional (Ex.1005), Fig. 5 (annotated excerpt);
'095 Provisional (Ex.1005), Figs. 1, 6-8

"In stage [11], the payment token payload is built. In the exemplary embodiment of Figure 12A this stage includes retrieving payment static information from the consumer profile and generating dynamic data. Such dynamic data generation includes: the proof (using Fn_Proof), the IVS_CVC3 (using Fn_IVS_CVC3), incrementing the ATC, and the KS_CVC3 (Using Fn_KS_CVC3)."

'248 Provisional (Ex.1006), ¶0161

"Stage [11] continues with the computation of the MA_Key using Fn_MA_Key (Access Code, Salt), formatting of the message Msg (Length+ Payment Token Payload) and encryption of Msg using MA_Key before proceeding to stage [12] where the E(Msg) is returned to the mobile application 1011 over the SSL/TLS Connection."

	’248 Provisional (Ex.1006), ¶0166  ’248 Provisional (Ex.1006), Fig. 12A (annotated excerpt)
transmitting, by the transmitting device, at least the KS_{UN}, UN_{CLOUD}, 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 Collinge Provisionals disclose the cloud-based transaction data generation system transmitting KS_{UN}, UN_{CLOUD}, and application transaction counter to an issuer associated with the account for use in validating the generated dynamic card validation code used in the financial transaction. **8a** There is synchronization process between the Cloud and the Issuer. The synchronization process may include the definition of rules for the validity of the generated CVC3 values. ’095 Provisional (Ex.1005), Table 1 (p. 16)  ’095 Provisional (Ex.1005), Fig. 5 (annotated excerpt);

’095 Provisional (Ex.1005), Figs. 6-7

19a	The Issuer has a mean to identify transaction that requires additional processing for CVC3 validation when an embodiment using SE-less Mobile Contactless Payment is used. Using the ATC provided in the Payment Transaction, 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. Detection of unsuccessful authentication can also take place at this stage.
19b	A standard process applies for the CVC3 validation using the UN_{CLOUD} and KS_{UN} values.
20	The completion of the Payment transaction process remains unchanged.

’095 Provisional (Ex.1005), Table 1 (p. 17)

“Payload sent to the Issuer
◊ Identifier (PAN ...)
◊ UN_{CLOUD}
◊ ATC
◊ Authentication Status Info+ Additional Generation Information (e.g. Validity)”

’095 Provisional (Ex.1005), p. 23

“Issuer Validation Process
An exemplary validation process is described below wherein the Issuer 180 uses the information provided in the payment transaction:

- Identifier - e.g. PAN Information
- UN_{READER} (4 bytes) - Partial Information retrieved from Track data (Discretionary Information)
- ATC (2 bytes)-Partial Information retrieved from Track data (Discretionary Information)
- $CVC3_{TRACK1/2}$ Partial Information retrieved from Track data (Discretionary Information)

The Issuer system is able to compute Cloud_CVC3$_{TRACK1/2}$ using:

- IVCVC3$_{TRACK1/2}$ (2 bytes)
- UN$_{CLOUD}$ (4 bytes)
- ATC (2 bytes)

The Issuer system is able to compute CVC3$_{TRACK1/2}$ using:

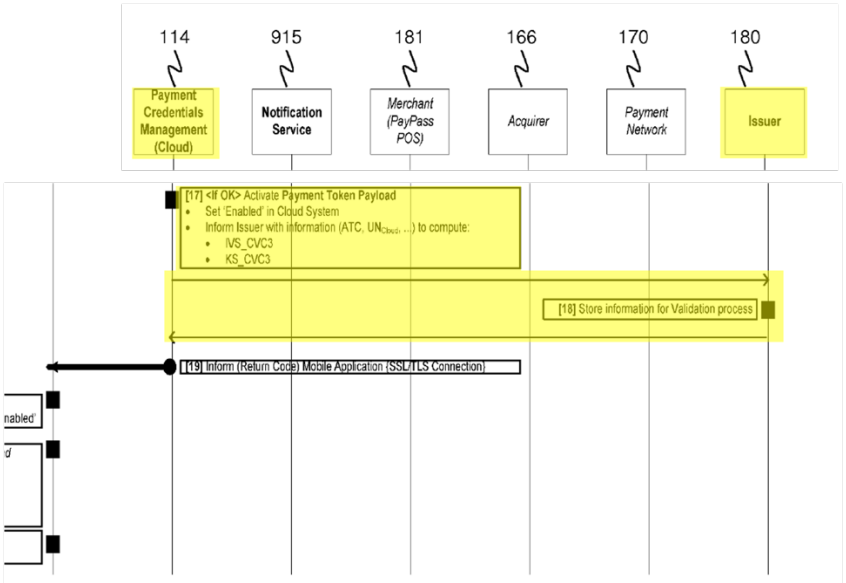
- Cloud_CVC3$_{TRACK1/2}$ (2 bytes)
- UN$_{READER}$ (4 bytes)
- ATC (2 bytes)

The Issuer can validate the CVC3$_{TRACK1/2}$"

'095 Provisional (Ex.1005), ¶¶0072-0074;
'248 Provisional (Ex.1006), ¶0226 (p. 54)

"In stage [17], the payment token payload is activated by setting 'Enabled' in the cloud-based transaction data generation system 106. Then, the issuer 180 is provided (informed) with information (ATC, UN$_{CLOUD}$, ...) needed to compute the IVS_CVC3 and KS_CVC3. In stage [18], this information is stored for a subsequent validation process."

'248 Provisional (Ex.1006), ¶0172



'248 Provisional (Ex.1006), Fig. 12A (annotated excerpt)

	"CVC3 Validation process (*Fn_ValCVC3*) by the Issuer using information provided by the Cloud at time of the synchronization process;" '248 Provisional (Ex.1006), ¶0184 Next, in stage [14], CVC3 validation is done using Fn_ValCVC3 before proceeding to stage [15], where the standard process for PayPass Magstripe Transaction is completed between the issuer 180, the payment processing network 170, the Acquirer 166, and the Merchant 181 (see reference number 14 in Figure 15). '248 Provisional (Ex.1006), ¶¶0203 "*UN_{CLOUD} is part of the payload exchanged between the Cloud and the Issuer during the Synchronization process*." '248 Provisional (Ex.1006), ¶0224. "**<u>Fn ValCVC3</u>** This function validates CVC3 values (Track 1 and Track 2) generated by the Mobile Payment Application using UN_{Reader} and the content of the Payment Token Payload. For the validation process, the Issuer uses the information provided in the payment transaction: ♦ Identifier - e.g. PAN Information retrieved from Track Data ♦ UN_{READER}(4 bytes) - Partial Information retrieved from Track data (Discretionary Information) ♦ ATC (2 bytes) - Partial Information retrieved from Track data (Discretionary Information) ♦ $CVC3_{TRACK1/2}$ - Partial Information retrieved from Track data (Discretionary Information) The Identifier and ATC values are used to retrieve the information provided by the cloud-based transaction data generation system 106 ("the Cloud system"):

	◊ Identifier (PAN, ...) ◊ UN_{CLOUD} ◊ ATC ◊ (Option) Additional Generation Information The issuer 180 system is able to compute IVS_CVC3 using: ◊ $IVCVC3_{TRACK112}$(2 bytes) ◊ UN_{CLOUD} (4 bytes) ◊ ATC (2 bytes) ◊ KD_{CVC3} The Issuer system is able to compute $CVC3_{TRACK1/2}$ using: ◊ IVS_CVC3 (2 bytes) ◊ UN_{READER}(4 bytes) ◊ ATC (2 bytes) ◊ KS_CVC3 The issuer 180 can validate the $CVC3_{TRACK1/2}$ value." '248 Provisional (Ex.1006), ¶¶0226 (p. 54) "Generate KS_{UN} using: UL:= DES3(KD_{UN})[(ATC II 'FO' II '00' II UN_{CLOUD})] UR:= DES3(KD_{UN})[(ATC II 'OF' II '00' II UN_{CLOUD})] KS_{UN} := (UL II UR) **KS_CVC3 := KS_{UN} generated in the Cloud**" '248 Provisional (Ex.1006), ¶¶0226 (p. 53)

3. Support for Collinge in Collinge Provisionals

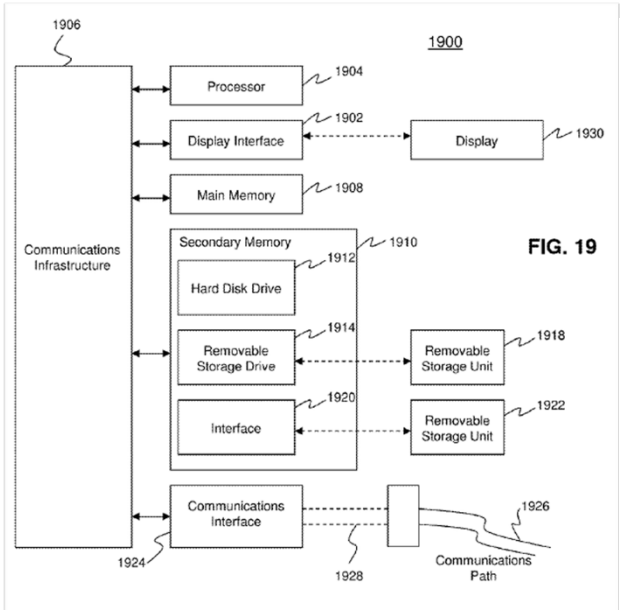
85. I have been informed that for Collinge to be §102(e) prior art as of the filing date of the Collinge Provisionals, the Collinge Provisionals must provide written description support for the subject matter relied upon in the petition. *See In*

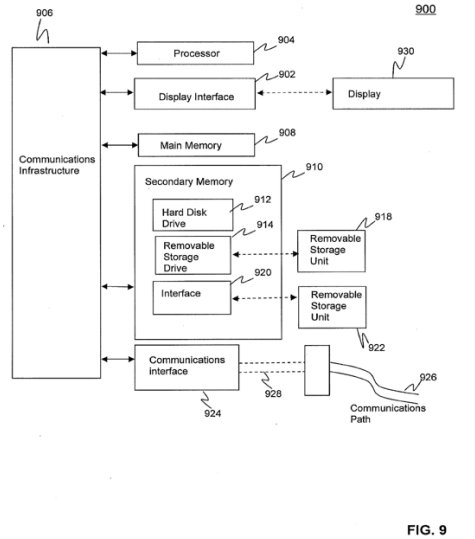
re Giacomini, 612 F.3d 1380, 1383 (Fed. Cir. 2010). "To satisfy the written description requirement, the claimed subject matter need not be described "in haec verba" in the original disclosure. *See In re Wright*, 866 F.2d 422, 425 (Fed. Cir. 1989). Rather, the test for determining compliance with the written description requirement is whether the original disclosure of the patent application reasonably conveys to a person of ordinary skill in the art that the inventor had possession of the claimed subject matter as of the filing date. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (*en banc*).

86. My opinion relies on many disclosures from Collinge, each of which a POSITA would have understood to be disclosed by the Collinge Provisionals.

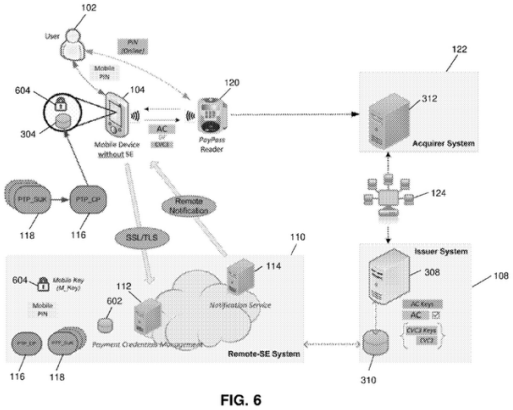
87. All portions of Collinge cited in the proposed ground below appear substantially identically in Collinge Provisionals. I have endeavored to include citations to corresponding disclosures in the Collinge Provisionals in the charts above. Accordingly, the disclosure relied on to meet challenged claim limitations is entitled to Collinge Provisionals' filing date. Further, Collinge's provisional applications are directed to the same invention. Figures, invention elements numbering, and invention descriptions substantially overlap, and a POSITA would recognize that the Provisionals provide additional implementation details relevant to Collinge's payment system. *Compare '098 Provisional (Ex.1008)*, Fig. 19 *with*

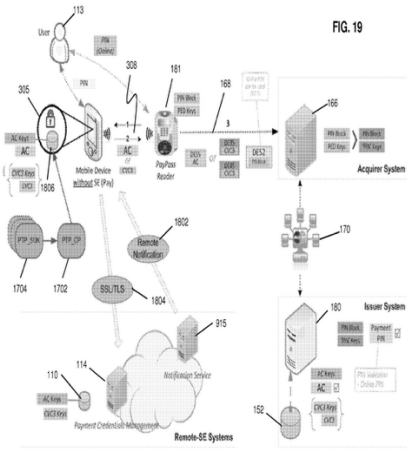
Collinge (Ex.1004), Fig. 6; *'095 Provisional (Ex.1005),* Fig. 9 *with Collinge (Ex.1004),* Fig. 19 and *'248 Provisional (Ex.1006),* Fig. 16.





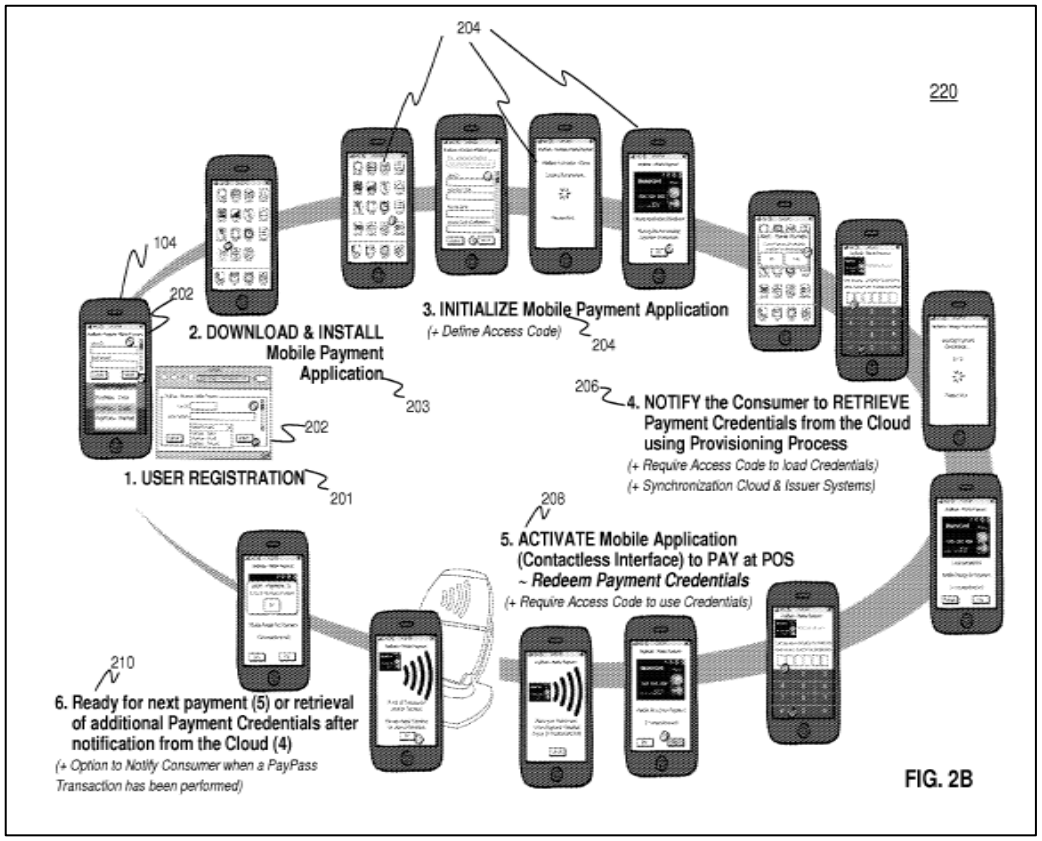
Collinge at Figure 19 (left); *'095 Provisional (Ex.1005),* Figure 9 (right).





Collinge at Figure 6 (left); *'095 Provisional (Ex.1005),* Figure 19 (right). Even if Collinge's Provisionals were directed to different payment system embodiments, it would have been obvious, and a POSITA would have been motivated to apply the

teachings in Collinge's Provisionals in Collinge's payment system. For example, Collinge's provisional applications provide additional detail about what is shown on the graphical user interface of Collinge's mobile device during user registration, user selection of a payment option, and an NFC transaction. *See e.g., '248 Provisional (Ex.1006),* Fig. 2A, 2B; *'098 Provisional (Ex.1008)*, p. 96-100; *Collinge (Ex.1004),* [0133].



'248 Provisional (Ex.1006), Fig. 2B. A POSITA would have found it obvious and would have been motivated to incorporate these disclosures into Collinge's payment system as examples of selectable softbuttons that could be used to implement the

invention. As another example, Collinge teaches use of a "CAP token" (*Collinge (Ex.1004),* [0144]) and the provisional applications provide examples of what controls on purchases may be represented by the token. *See '095 Provisional (Ex.1005),* Claims 9-10 (day of week, time of day, etc.). A POSITA looking to implement a CAP token would have been motivated to implement one or more of the examples of a CAP token in Collinge's Provisional application. In each case, a POSITA would have found a teaching, suggestion, or motivation in Collinge since the provisional was directed to the same mobile device used in Colline, that would have led them to apply the additional details in Collinge's Provisionals to Collinge's payment system and would have had a reasonable expectation of success.

B. Walker

88. I understand Walker teaches a "smart card" device that "generate[s] a single-use credit card number" that can be used to purchase goods or services. *Walker (Ex.1009),* [0043], [0046]. Walker's single use credit card number "is generated by the device cryptoprocessor 205, using a private key 601" by cryptographically combining the initialization variable, account number and encrypted nonce value. *Walker (Ex.1009),* [0060]-[0061]. When the single-use credit card number is used for payment, a card issuer "maps the single-use credit

card number onto a conventional credit card account" to authorize the transaction. *Walker (Ex.1009),* [0048]

89. I have been informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be "analogous art" to the claimed invention. I have been informed that a prior art reference is analogous to the claimed invention if the reference is from the same field of endeavor as the claimed invention or if it is reasonably pertinent to the particular problem that the inventor was trying to solve.

1. Walker is Analogous

90. A POSITA would have classified Walker within the same field of endeavor as the '820 Patent because both Walker and the '820 Patent relate to the generation and use of credentials for smart payment devices. For example, *Walker* like the '820 Patent discloses conducting secure payment transactions. *Compare '820 Patent (Ex.1001),* Abstract, 1:27-31, Fig. 1 *with Walker (Ex.1009),* [0001], [0022] ("secure electronic commerce…third party cannot misuse any credit card information"), [0021]. Thus, *Walker* is in the same field of endeavor as the '820 Patent.

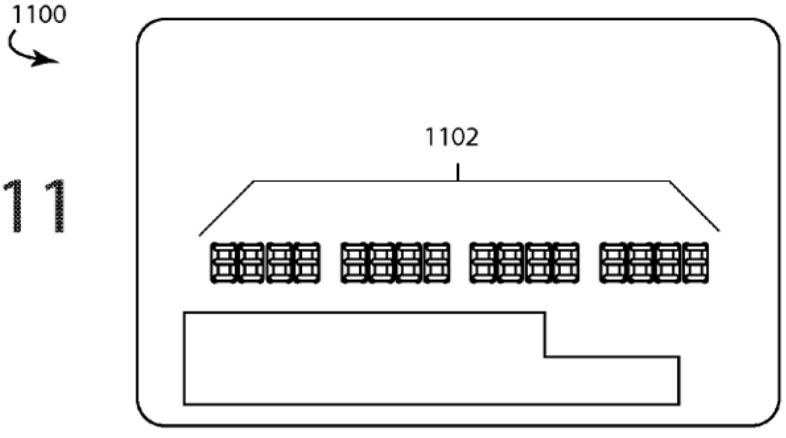
91. Additionally, a POSITA would have found Walker reasonably pertinent to the problem faced by the inventors of the '820 Patent because both

Walker and the ’820 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. *See ’820 Patent (Ex.1001),* 1:27-31, 1:66-2:7, 2:4-12. For example, Walker’s invention notes that current credit card systems have a “risk of fraudulent use” and lists examples of common ways that “credit card security is vulnerable.” *Walker (Ex.1009),* [0003], [0009]-[0013]. *See also, id,* [0002]-[0008], [0013]-[0021]. Therefore, a POSITA would have considered Walker analogous art to the ’820 Patent.

C. Brown

92. I understand Brown teaches a smart payment card that has a “full personal account number (PAN) [that] has been **implemented to be variable** on a visual display.” *Brown (Ex.1010),* [0200] (emphasis added).

Fig. 11



Brown, Fig. 12.

1. Brown is Analogous

93. Brown is analogous art to the ’820 Patent because it is from the same field of endeavor because both Brown and the ’820 Patent are directed towards conducting secure payment transactions. Like the ’820 Patent, Brown is concerned with conducting secure payment transactions. *See, e.g., Brown (Ex.1010),* [0004] (“the present invention relates to…methods for secure financial transactions with consumer payment cards”). *Compare ’820 Patent (Ex.1001)*, Abstract, 1:27-31, Fig. 1 *with Brown (Ex.1010),* Abstract, [0004].

94. Additionally, a POSITA would have found Brown reasonably pertinent to the problem faced by the inventors of the ’820 Patent because both Brown and the ’820 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. *Compare ’*820 *Patent (Ex.1001),* 1:27-31, 1:66-2:7, 2:4-12,*with Brown (Ex.1010)*, [0006]-[0021], [0024]-[0029].

D. Gauthier

95. I understand Gauthier teaches a secured account number, different than the user’s primary account number (PAN), that is **only** used for “wireless transactions” with a proximity reader, using “a contactless mode, infrared mode, RF mode (i.e. Radio Frequency), and the like[.]” *Gauthier (Ex.1011),* [0022], [0037], Fig. 1.

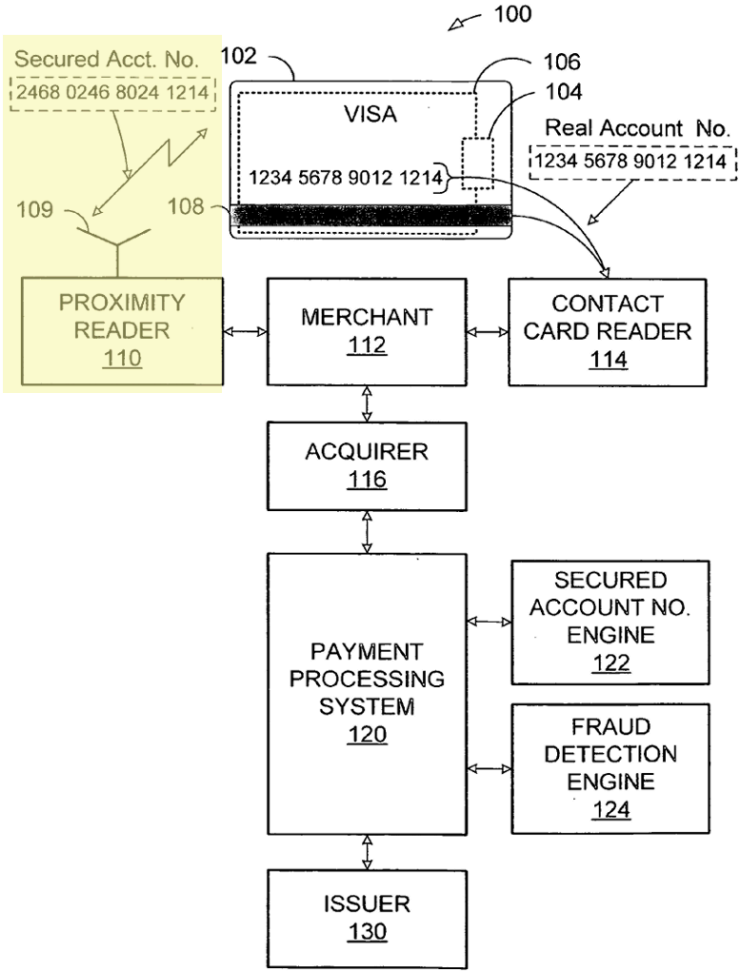


FIG. 1

Gauthier (Ex.1011) Fig. 1 (annotated).

1. Gauthier is Analogous

96. Gauthier is analogous art to the '820 Patent because it is from the same field of endeavor because both Gauthier and the '820 Patent are directed towards conducting secure payment transactions. *Compare '820 Patent (Ex.1001)*, Abstract, 1:27-31, Fig. 1 *with Gauthier (Ex.1011)* at [0009]-[0010], [0019], Fig. 1 (discussing "secured" account numbers).

97. Gauthier is also reasonably pertinent to at least one problem addressed by the '820 Patent. Like the '820 Patent, Gauthier is concerned with increasing security of payment transactions. *Compare '820 Patent,* 1:27-31, 1:66-2:7, 2:4-12, *with Gauthier (Ex.1011),* [0006]-[0008] ("Theft of sensitive information…is a major concern for consumers and business alike" and "many payment service providers have instigated safeguards…such safeguards have had limited success as they are generally expensive to implement, can be overcome, and have not been fully accepted by the credit card industry, merchants, payment processors, etc.").

E. Patel

98. I understand Patel teaches a "credit card, debit card, or other similar financial Instrument" and "temporary assignment of a dynamic CVV" to the card for increased card security." *Patel (Ex.1012),* Abstract. "The dynamic CVV is read, changed, and rewritten to the card with each transaction." *Id.* Patel teaches that the dynamic CVV is used "[t]o pay for the goods or services" through "a magnetic card reader 130[.]" *Patel (Ex.1012),* [0057].

99. The dynamic CVV is transmitted to the financial institution 150, which "authenticates the verification data, including the dynamic CVV 330, and transmits a verification code, including a new dynamic CVV 330 to the transaction device 130." *Patel (Ex.1012)*, [0059]. "The transaction device 130 reads the new dynamic

CVV 330, and writes the new CVV 330," which was received from the card issuer, "to the magnetic strip 220" of the payment card. *Patel (Ex.1012)*, [0060]. "The financial institution 150 may then update its database to expire the previous dynamic CVV 330, and enter the new dynamic CVV 330 as the valid dynamic CVV 330." *Patel (Ex.1012),* [0062]. "Once the new CVV 330 has been provided, the old CVV 330 expires and is no longer valid." *Patel (Ex.1012)*, [0065].

1. Patel is Analogous

100. Patel is analogous art to the '820 Patent because it is from the same field of endeavor. Like the '820 Patent, Patel is concerned with conducting secure payment transactions. *Compare '820 Patent (Ex.1001)*, Abstract, 1:27-31, Fig. 1 *with Patel (Ex.1011),* Abstract, [0003] ("This invention relates to financial transactions and more particularly, to novel systems and methods for security codes for transactional cards[.]"), [0007].

101. Patel is also reasonably pertinent to at least one problem addressed by the '820 Patent. Like the '820 Patent, Patel is concerned with increasing security of payment transactions. *Compare '820 Patent,* 1:27-31, 1:66-2:7, 2:4-12, *with Patel (Ex.1012),* [0005]-[0006].

F. Eng

102. I understand Eng teaches a card that has the following fixed payment information: (1***) a card-holder name***, (2) bank name (***a payment issuing logo***) among other items. *See Eng (Ex.1014),* [0020]-[0021].

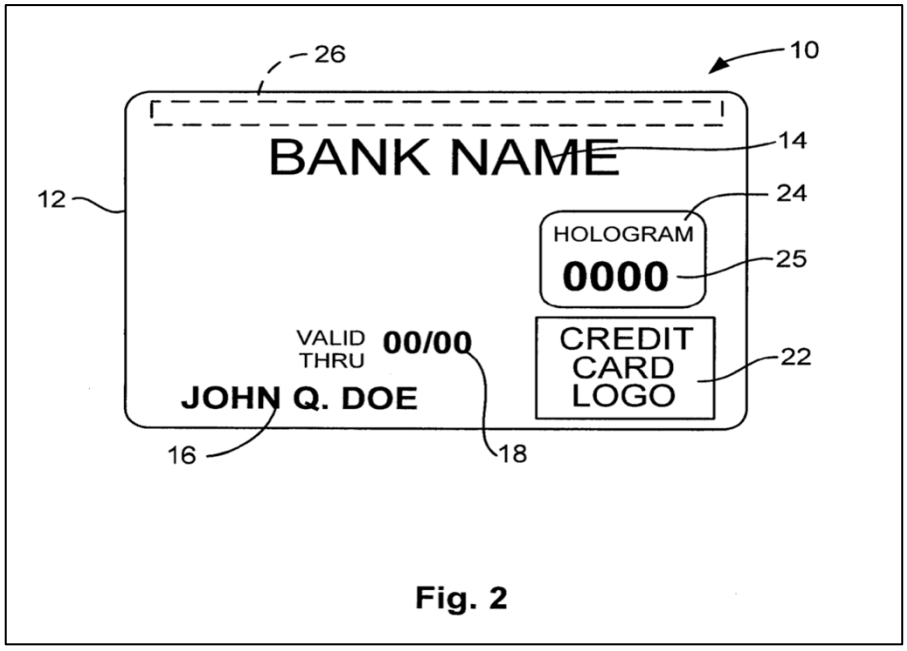


Fig. 2

Eng (Ex.1014), Fig. 2.

1. Eng is Analogous

103. Eng is analogous art to the '820 Patent because it is from the same field of endeavor. Like the '820 Patent, Eng is concerned with conducting secure payment transactions. *See, e.g., Eng (Ex.1014),* [0023] ("cards containing only partial credit card account information herein provides added security."); [0024] ("the partial account information appearing on the credit card is plainly visible and can be compared by a merchant to an authorization receipt or document."); Abstract

("systems and methods for protecting information related to credit card accounts and other kinds of information displayed on personal and identification cards."). *Compare '820 Patent (Ex.1001)*, Abstract, 1:27-31, Fig. 1 *with Eng (Ex.1014),* Abstract, [0024]-[0024], Fig. 2.

104. Eng is also reasonably pertinent to at least one problem addressed by the '820 Patent. Like the '820 Patent, Eng is concerned with increasing security of payment transactions. *See, e.g., Eng (Ex.1014),* [0023] ("cards containing only partial credit card account information herein provides added security."), Abstract ("systems and methods for protecting information related to credit card accounts and other kinds of information displayed on personal and identification cards."); *compare '820 Patent (Ex.1001),* 1:27-31, 1:66-2:7, 2:4-12 *with Eng (Ex.1014),* Abstract, [0023], Fig. 2.

G. Kranzley

105. Kranzley teaches that "[t]he payment application of the mobile device 12 converts the data (including the PAN, expiry, and dynamic data) into a bar code image 13." *Kranzley (Ex.1013),* [0028]. Kranzley teaches displaying "the static VPAN…in plain text on a display device 14 of the mobile device 12 along with an expiry date and dynamic data." *Kranzley (Ex.1013),* [0035]; [0033]-[0036].

1. Kranzley is Analogous

106. Kranzley is analogous art to the ’820 Patent because it is from the same field of endeavor. Like the ’820 Patent, Kranzley is concerned with conducting secure payment transactions. *See, e.g., Kranzley* at Abstract (“Systems, methods processes, computer program code and means for conducting a payment transaction which include…a dynamic verification code generated by the payment application[.]”), [0003] (“It would further be desirable to provide mobile payment transactions which are secure and in which the cardholder’s presence may be confirmed.”), [0010] (“…and means for conducting a payment transaction include…at least one of a payment account number, an expiry date of said payment account number, and a dynamic verification code generated by said payment application[.]”). *Compare ’820 Patent (Ex.1001)*, Abstract, 1:27-31, Fig. 1 *with Kranzley (Ex.1013),* Abstract, [0010], Fig. 1.

107. Kranzley is also reasonably pertinent to at least one problem addressed by the ’820 Patent. Like the ’820 Patent, Kranzley is concerned with increasing security of payment transactions. *See, e.g., Kranzley* at [0003] (“It would further be desirable to provide mobile payment transactions which are secure and in which the cardholder’s presence may be confirmed.”), [0065] (“As a specific example, for VPANs processed over the payment network operated by MasterCard International Incorporated, VPANs are 16 digit numeric codes in which the first 6 digits are used

to identify the VPAN as a VPAN to be routed to a payment provider 110 for processing."), [0067] ("The shared secret key may be used to encrypt a dynamic value transmitted from the mobile device. The payment provider 110 may use the shared secret key, in conjunction with the counter 508, to decrypt the dynamic value from the mobile device 102 to ascertain the authenticity of the transaction request."). *Compare '820 Patent (Ex.1001),* 1:27-31, 1:66-2:7, 2:4-12 *with Kranzley (Ex.1013),* [0003], [0065].

IX. SUMMARY OF UNPATENTABILITY

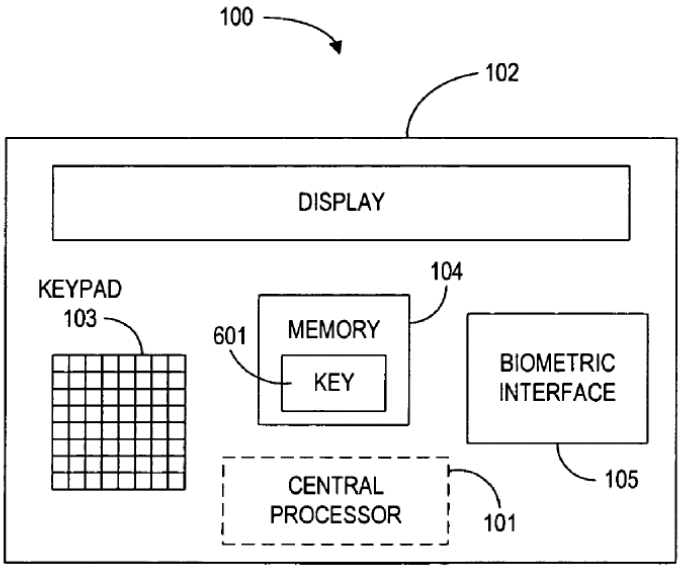
108. I have reproduced the Proposed Grounds of Unpatentability from the Petition for ease of reference:

Ground	Claim(s)	References
1	1, 8, 10	Walker (Ex.1009) and Brown (Ex.1010)
2	2	Walker, Brown, and Eng (Ex.1014)
3	4-7, 9	Walker, Brown and Gauthier (Ex.1011)
4	3	Walker, Brown, and Patel (Ex.1012)
5	11, 13-15, and 17-20	Collinge (Ex.1004), Kranzley (Ex.1013), and Brown
6	12, 16	Collinge, Kranzley, Brown, and Eng

X. OPINIONS REGARDING GROUND 1: CLAIMS 1, 8, AND 10 ARE OBVIOUS OVER *WALKER* AND *BROWN*.

A. 1(Pre): A payment system comprising:

109. Walker teaches *a payment device*[2], device 100, which is preferably a "smart card." *Walker (Ex.1009),* [0043]. Walker's device 100 "generate[s] a single-use credit card number" that can be used to purchase goods or services. *Walker (Ex.1009),* [0043], [0046].



Walker (Ex.1009), Fig. 1.

B. 1(a): a thin shaped body having no fixed payment numbers disposed thereon

1. Patentable Weight

[2] Claim language identified with *italics* and underline.

110. The limitation "having no fixed payment numbers disposed thereon" is directed to printed matter which I understand has no patentable weight if it has no functional or structural relationship to the claimed card device.

111. A POSITA would have understood that, at the time, it was common for a payment card (such as a credit or debit card) to have fixed payment numbers such as a PAN (primary account number), expiration date, and CVC numbers.

PayPass (Ex.1025), 1.

112. The PAN, expiration date, and CVC/CVV shown on the face(s) of a traditional payment card are useful to the card-holder because they provide the card-holder with information that may be used to make payments online, by mail, over the phone, or in other circumstances where card-reader equipment such as a magnetic stripe reader or smart card reader is unavailable. In such cases for online, by mail, or over the phone payments, the medium that the payment information is

provided on—for example, the plastic of the payment card itself—is irrelevant to conducting the payment transaction. The plastic card is merely how the payment information is stored for later reference by the user. I was asked to consider whether a POSITA at the time of the '820 Patent would have understood the PAN, expiration date, CVC, and other payment information on the face of a common payment card to have a functional relationship with the material (e.g., plastic) of the payment card itself. I was unable to identify any such functional relationship. The physical payment card simply serves as the medium on which the information is attached, the same way paper may serve as the medium when a payment card number is printed on a receipt.

113. I was also asked to consider whether the limitation "having no fixed payment numbers disposed thereon" has any relationship to any other element of the claims that might impact my opinion. I observed that there were no further references to fixed payment numbers in the remainder of claim 1. None of the other limitations of the claims of the '820 Patent impact my opinion that payment numbers do not have a functional relationship to physical (e.g., plastic or metal) payment cards.

114. Nevertheless, a POSITA would have understood that the combination of Walker and Brown renders this limitation obvious.

2. Walker's Teachings

115. Walker's payment device 100 is a "hand-held **smart card** device" with a *thin shaped body*, as shown in Fig. 1. *Walker (Ex.1009),* [0028] (emphasis added), [0043] ("device is preferably a **smart card**") (emphasis added), Fig. 1. A POSITA would have been well-familiar with the term "smart card" by the Critical Date and would have understood that in the context of Walker's disclosures a "smart card" resembles a credit card in size and shape, but contains additional hardware such as an embedded processor.*'820 Patent*, 1:45-51 (smart cards are "credit cards [that] have a built in microprocessor with cryptographic capabilities"). As discussed in Section VII.A.2, smart cards with integrated microprocessors were used in the 1990s for debit card transactions. Bona describes such an NFC-enabled companion card 900 that "takes the shape of a standard plastic magnetic stripe card" and includes "display 204," an "internal power source 212" a "smart card controller 216" and a "magnetic stripe emulator 214." *Bona (Ex.1019),* [0045]-[0047], [0011]. The companion card can be used in "a traditional magnetic stripe reader" *Bona (Ex.1019),* [0125].

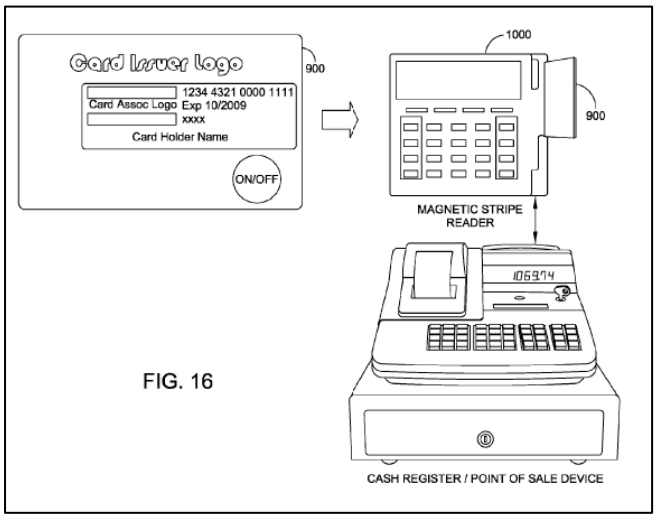


FIG. 16

Bona (Ex.1019), Fig. 16.

116. Likewise, Eng describes a credit card having a partial credit card number and magnetic data strip and separate sheath portion. *Eng (Ex.1014),* [0021]-[0025], Figs. 2-3. The portions together are thin enough to "slide into or through electronic/magnetic card apparatus." *Eng (Ex.1014),* [0031].

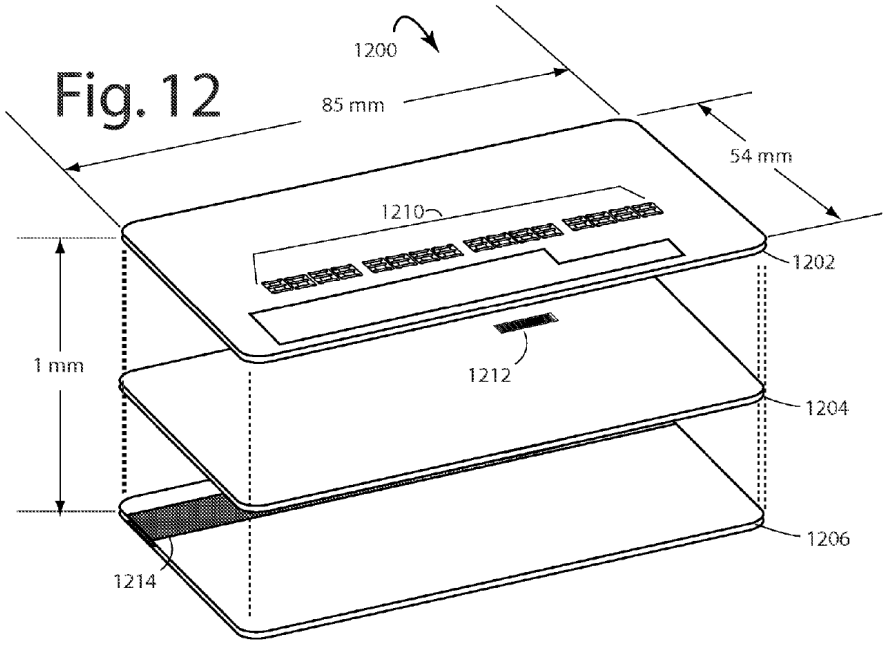
117. U.S. Patent No. 7,793,851 to Mullen also describes a "dynamic credit card" having a "secret/hidden credit card number" that provides a "dynamic credit card number." *Mullen '851 (Ex.1044)*, Abstract, Fig. 1. The dynamic number may be written to a magnetic stripe "such that the number may be processed by traditional credit card merchants (e.g., swiped)." *Mullen '851 (Ex.1044)*, Abstract, 10:23-29.

118. Walker's payment device 100 "generate[s] a single-use credit card number" that can be used to purchase goods or services. *Walker (Ex.1009),* [0043], [0046]. Walker's "single-use credit card number" is "unique for the specific input

variables set by the cardholder or by the device" and "may also be unique to the specific date and time to avoid so-called 'replay,' attacks for that card at that merchant with that exact purchase amount." *Walker (Ex.1009),* [0047]. There is no fixed account number to be displayed on device 100 because (1) Walker does not display any payment numbers until the time-and-date-specific payment number is generated and (2) when Walker does display a payment number, it is single use, not fixed. Thus, Walker's payment device 100 has no *fixed payment numbers disposed thereon*.

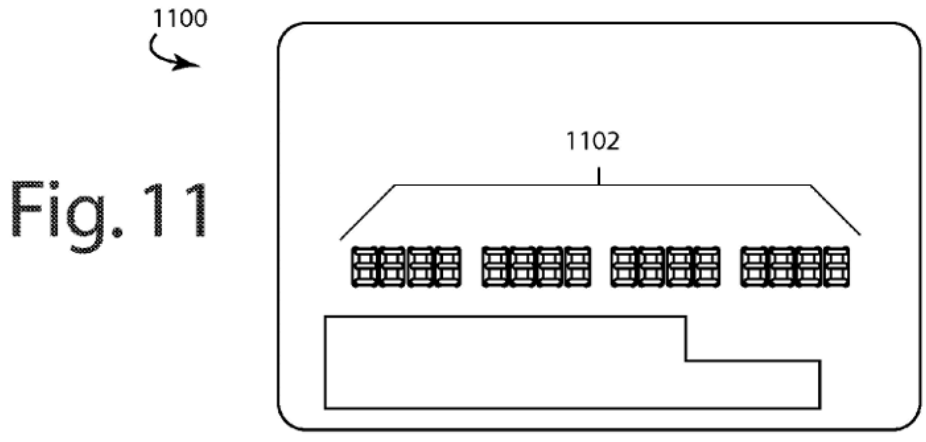
3. Brown's Teachings

119. Brown similarly teaches a smart payment card that is "1mm" in thickness and therefore has a *thin shaped body*. *Brown (Ex.1010),* [0091] (citing payment card thickness standards), [0200] (describing a "smart card" as "1mm" in thickness); *see also,* [0067]-[0069], [0084] (describing the payment card as a "credit card format" that can be used with "legacy magnetic stripe card readers").



Brown (Ex.1010), Fig. 12.

120. Brown's payment card has a "full personal account number (PAN) [that] has been **implemented to be variable** on a visual display." *Brown (Ex.1010),* [0200] (emphasis added).



Brown (Ex.1010), Fig. 12 (showing variable account number).

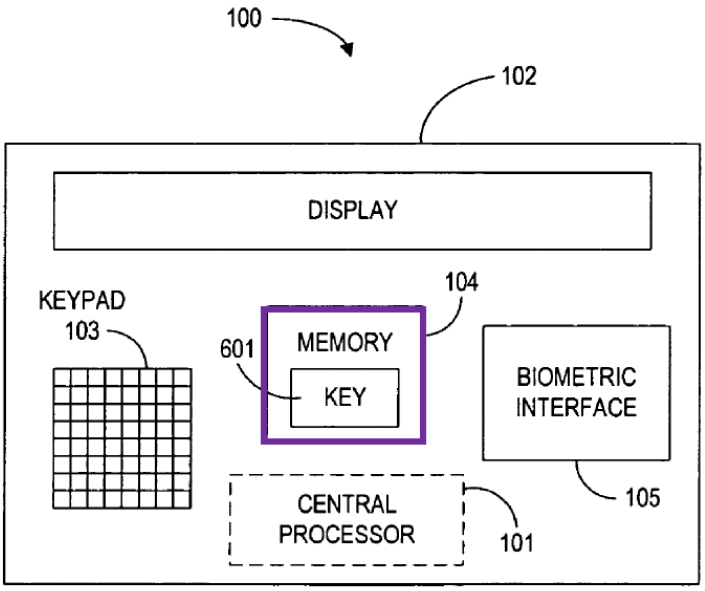
121. Brown teaches displaying a wholly variable payment account number therefore there are no fixed account numbers displayed on Brown's payment card.

4. Motivation to Combine

122. To the extent Walker does not expressly teach a thin-shaped body, it would have been obvious, and a POSITA would have been motivated to implement Walker's payment device 100 with a *thin-shaped body*. Smart cards had long been known in the art; the EMV specifications standardized smart card processing in 1994. *See* VII.A.2. Further, smart cards having bodies similar to typical credit card such that they are able to be swiped through existing card readers were well-known. *Id.; Brown (Ex.1010),* [0091]. This would be desirable so that the card could be used with legacy readers, in addition to more modern-day chip and contactless readers. Further, a POSITA would have found it obvious and would have been motivated to implement Walker's payment device to "resemble a typical payment or bank/ATM card" conforming to relevant form-favor standards "so as to allow rapid assimilation into the payment card system and its use by consumers" as explicitly taught by Brown. *Brown (Ex.1010),* [0091]. A POSITA would have had a reasonable chance of success in making the modification because at the time it was already common for smart cards to be thin, resembling a typical payment card.

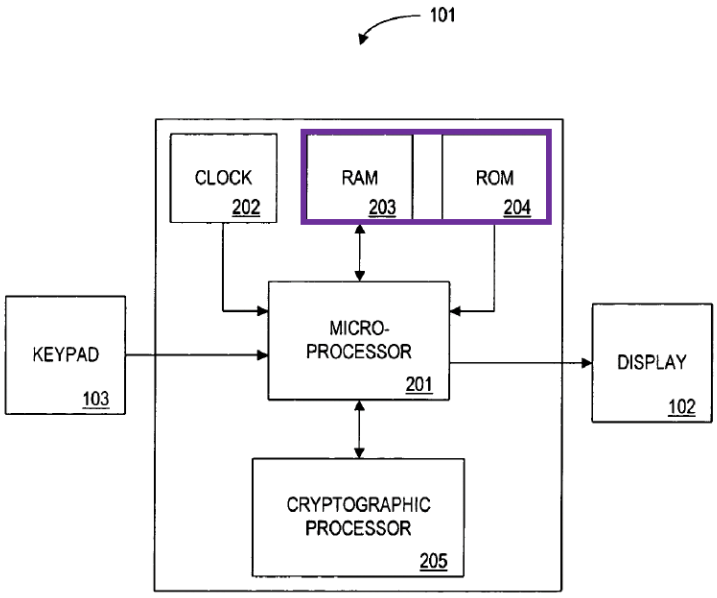
C. 1(b): a memory

123. Walker's "device includes *a memory* device connected to the processing unit" which is "memory 104." *Walker (Ex.1009),* [0024], [0043], [Abstract].



Walker (Ex.1009), Fig. 1 (annotated).

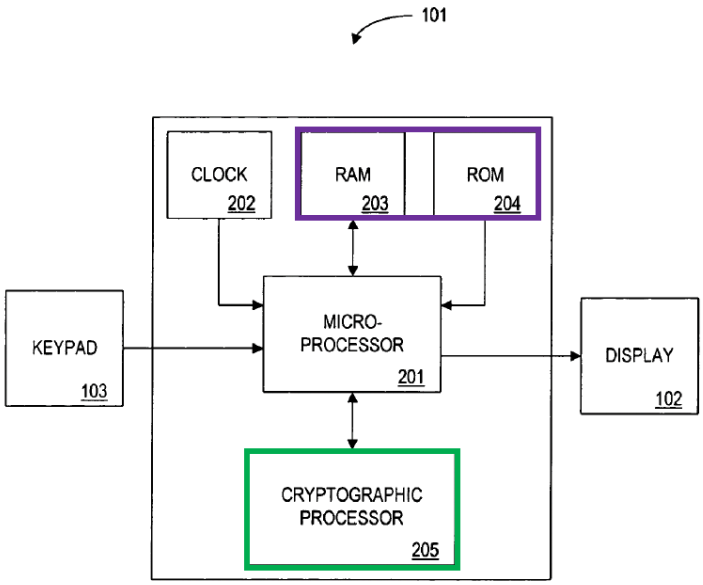
124. The central processor 101 includes a microprocessor 201 which "is connected to a clock 202, **a random-access memory (RAM) 203, a read-only memory (ROM) 204**, and a cryptographic processor 205.)." *Walker (Ex.1009),* [0044] (emphasis added).



Walker (Ex.1009), Fig. 2 (annotated).

D. 1(c) a cryptographic processor coupled to the memory; and

125. Walker's device 100 also includes a "*cryptographic processor* 205." *Walker (Ex.1009),* [0044], Fig. 2.



Walker (Ex.1009), Fig. 2 (annotated).

126. Walker's "single-use credit card number is generated by the device **cryptoprocessor 205,** using a private key 601 stored in the device **memory 104 (preferably the ROM 204)."** *Walker (Ex.1009),* [0050] (emphasis added). A POSITA would understand that Walker's cryptographic processor 205 is coupled to and accesses the memory during use. *Walker (Ex.1009),* [0044], [0050], Fig. 2.

E. 1(d) a reader interface, including at least one interface selected from a set comprising: a magnetic-stripe, a smart card reader interface, a magstripe inductor interface, an RF interface, an NFC interface, and a wireless interface, and

1. Walker's Teachings

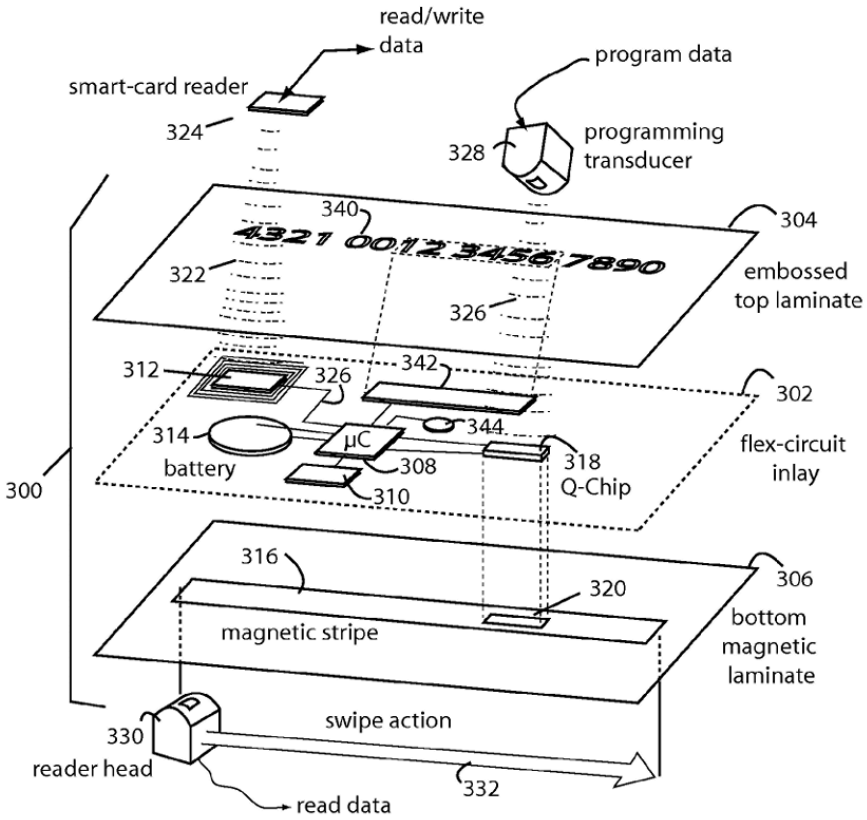
127. Walker teaches that the cardholder "**transmits** the single-use credit card number 300 to the merchant" who then "transmits" the number to a credit card issuer. *Walker (Ex.1009),* [0045] (emphasis added), [0048]. Walker teaches that the cardholder may purchase goods "in person, via telephone, or via the internet." *Walker (Ex.1009),* [0046].

128. Walker does not provide specificity regarding how the device transmits limited-use payment information to the merchant, instead only noting that the single-use credit card number is "read, shown or otherwise transmitted to the merchant." *Walker (Ex.1009),* [0063]. Walker notes that there is a risk of "incorrect keying" if the number is manually entered. *Walker (Ex.1009),* [0048].

2. Brown's Teachings

129. In related art, Brown's smart card device includes a "dynamic magnetic stripe" (i.e., *a magnetic*-stripe) and an "internal dynamic account number generator [] able to reprogram some of the magnetic bits encoded in the magnetic stripe to reflect the latest virtual account number." *Brown (Ex.1010),* [0022], Abstract, [0041], [0066]-[0067], [0070].

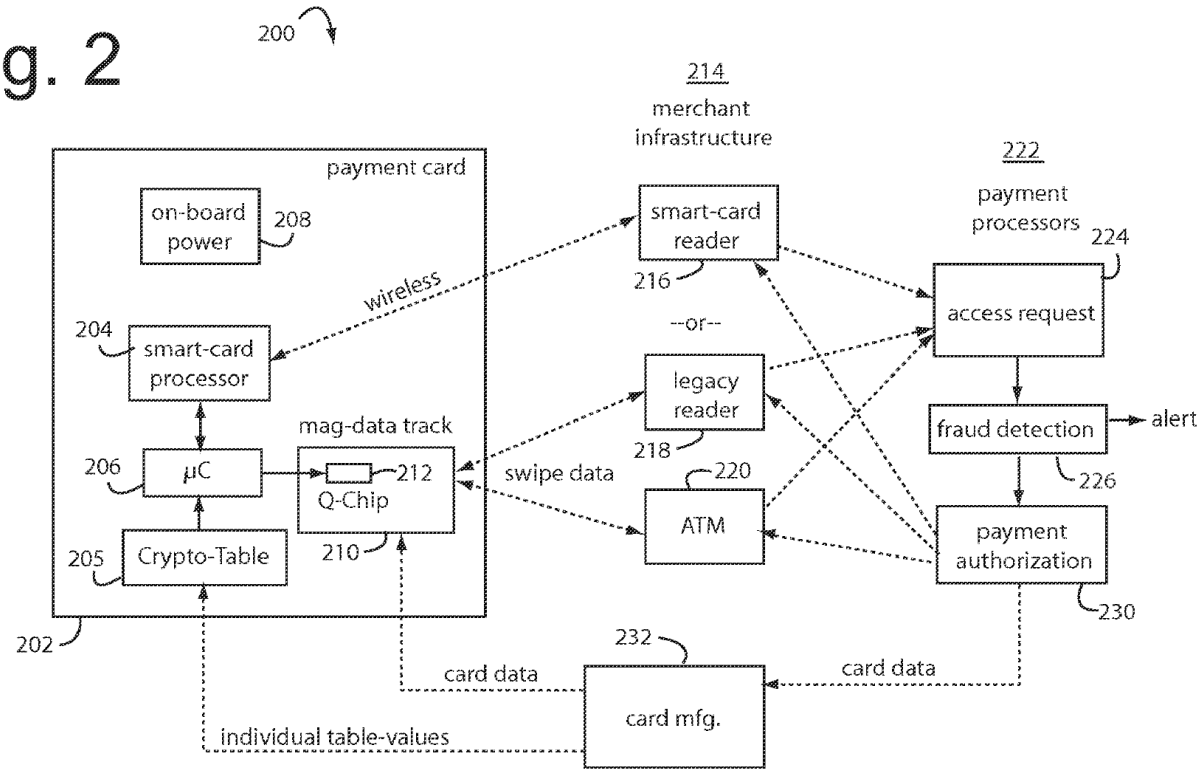
130. Brown's smart card device further includes a "contact/contactless programing inducer 312" and an "inductive or wireless coupling communication channel 326" that may be used "with *Near Field Communication* or similar *wireless communications*." *Brown (Ex.1010),* [0094] (emphasis added). Brown explains that the "contact/contactless reader 324 (FIG. 3)" is "conventional" and "already typically deployed throughout the world." *Brown (Ex.1010),* [0112].



Brown (Ex.1010), Fig. 3.

131. Brown teaches that it is advantageous for its smart card to work with both magnetic stripe readers and contact/contactless readers and demonstrates "how magnetic stripe and contact/contactless financial network infrastructures can be simultaneously supported." *Brown (Ex.1010),* [0066]-[0069], [0112], Fig. 2.

Fig. 2



Brown (Ex.1010), Fig. 2.

132. Brown's payment card further includes an "industry-standard contact/contactless smart-card processor" (smart-card processor 204) coupled to the reader interface. *Brown*, [0067], Fig. 2. For example, Brown teaches that the card dimensions, materials, magnetics, recordings, and data formats … are dictated by industry 'ISO' standards," including ISO 14443, which defines characteristics of proximity cards, such as RFID cards and their interfaces with readers. *Brown (Ex.1010),* [0070].

133. Brown, therefore, teaches a smart card that includes *interfaces* for legacy and smart card *readers*.

3. Motivation to Combine

134. Based on the teachings of Brown, it would have been obvious, and a POSITA would have been motivated to configure Walker's device to include a reader interface comprising a dynamic magnetic stripe and/or NFC interface so that Walker's single-use credit card number can be transmitted to a merchant with conventional POS infrastructure. These types of interfaces on smart cards were well-known at the time. For example, Bona's companion card include a smart-chip interface for contact and contactless transactions. *Bona (Ex.1019)*, [0045], [0047] (describing magnetic stripe reader interface), [0054], [0057] (describing smart-chip for magnetic stripe emulator), [0110] (describing NFC interface), Figs. 2A-B, 13B. Mullen '851 similarly describes a smart card having a magnetic stripe interface for interacting with a magnetic stripe reader. *Mullen '851*, 10:23-26, 12:40-44, 14:19-59, Figs. 2, 6-7.

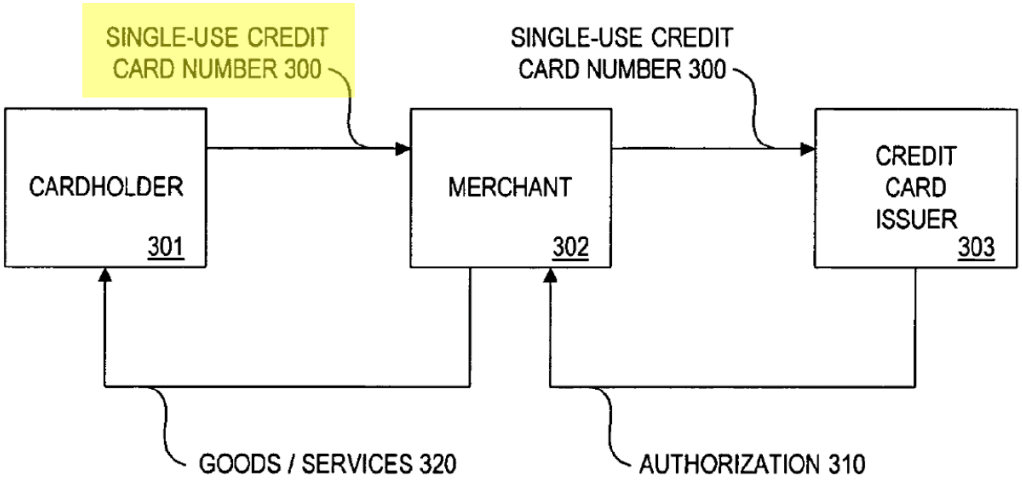
135. A POSITA would have been motivated to combine the prior art elements of Walker's smart card with Brown's dynamic magnetic stripe and NFC interfaces according to known methods to yield the predictable result of allowing Walker's smart card to communicate the single-use credit card number with a merchant POS terminal during a transaction. A POSITA would have recognized that without a reader interface, Walker's payment information would have to be

manually input by the user or cashier even where a merchant POS terminal is available, increasing the time to complete the transaction, holding up the line for other customers, and increasing the chance of error should an incorrect payment number be input manually. Consumers likely would not have found any such outcomes to be desirable. A POSITA further have found it obvious and been motivated to couple a reader interface comprising a dynamic magnetic stripe and/or NFC interface to Walker's processor 201 to allow the reader interfaces to send and receive the necessary data to complete a transaction, as taught by Brown.

136. Brown recognizes and a POSITA would have understood that magnetic stripe and NFC interfaces were already well-known and conventional (and, in fact, standardized) well-prior to the Critical Date. *See Brown (Ex.1010),* [0067], [0070], [0090]-[0091]. I discuss these technologies in Section VII.A-B. Given the ubiquity of magnetic stripe and NFC payment cards technology, there would have been a reasonable expectation of success configuring Walker's smart card device to include a dynamic magnetic stripe and NFC interface, per Brown, to yield a payment card for contact and contactless transactions and conforming to industry standards.

F. 1(e): wherein payment information for a transaction is operable to be conveyed via the reader interface and comprises limited-use payment information, and

137. Walker teaches transmitting a single use credit card number to a merchant. *Walker (Ex.1009),* [0045], Fig. 3A. Because Walker's single-use credit card number is "is different for each transaction" and "is preferably a 16-digit number that can be recognized as a conventional credit card number," it is *limited-use payment information*. *Walker (Ex.1009),* [0050]-[0051], [0047]-[0048].



Walker (Ex.1009), Fig. 3A.

138. For the reasons discussed above, it would have been obvious to a POSITA to configure Walker's smart card device to transmit *payment information*, including the single-use credit card number to the merchant terminal via a dynamic magnetic stripe or NFC interface (i.e., *the reader interface*). *See* Claim 1(d).

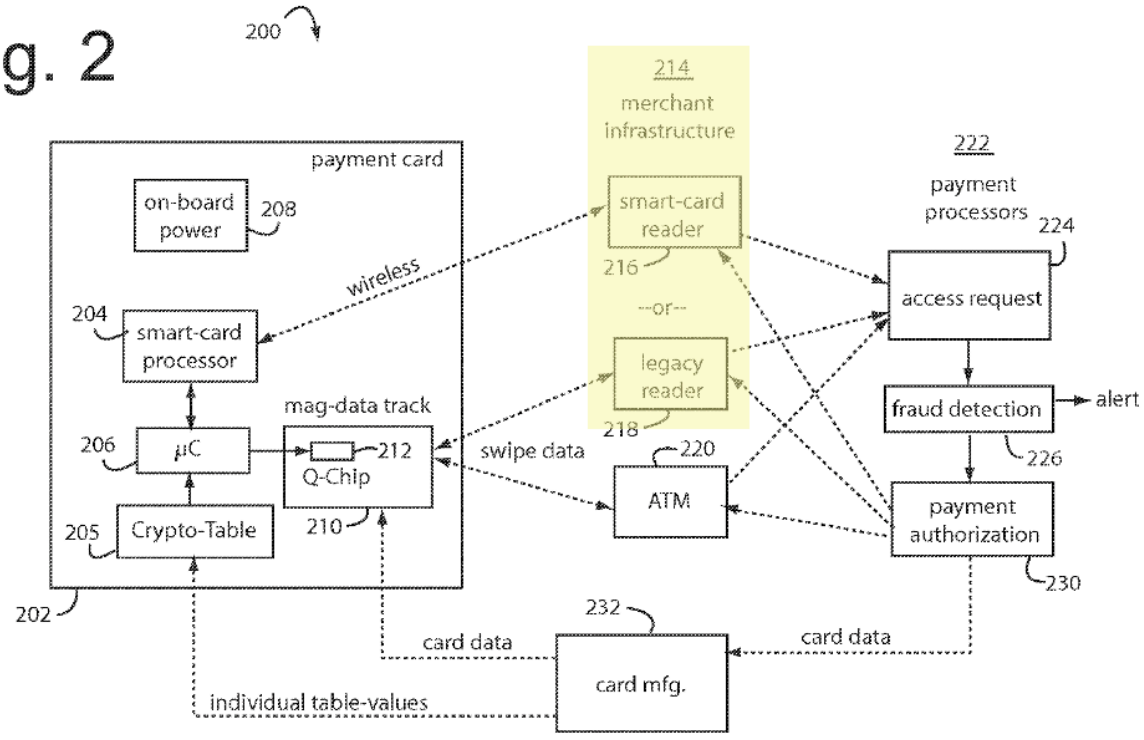
G. 1(f): wherein further the limited-use payment information is to be used in place of card issuer payment information for payment transactions by said device at payment card reader facilities.

139. Walker's single-use credit card number (i.e., *the limited use payment information*) *is to be used in place of* a conventional credit card number (i.e., *card issuer payment information*). *Walker (Ex.1009),* [0048], Fig. 3A. Walker teaches that "[a] cardholder 301, wishing to purchase goods or services from a merchant 302 … transmits a single-use credit card number 300 to the merchant" and "[t]he merchant 302 transmits the single-use credit card number 300 to a credit card issuer 303." *Walker (Ex.1009),* [0045], Fig. 3A. "The credit card issuer 303 returns an authorization 310 to the merchant, based on which the merchant delivers the desired goods or services 320 to the cardholder." *Id.* Specifically, the card issuer "**maps the single-use credit card number onto a conventional credit card account** and determines whether the transaction is authorized (step 380); if so, the central system returns an authorization code for display on the merchant's authorization terminal." *Walker (Ex.1009),* [0048] (emphasis added). Thus, Walker's single-use credit card number is used *for payment transactions* at the merchant's authorization terminal (i.e., *payment card reader facilities*).

140. To the extent that Walker does not specifically teach that the merchant's payment terminal includes a *payment card reader,* Brown teaches that the merchant

infrastructure at the time included magnetic stripe readers 218 and contact/contactless smart-card readers 216, and it would have been obvious to convey Walker's limited-use payment information through these payment card readers for the reasons discussed above at Claim 1(d). *Brown (Ex.1010),* [0066]-[0069], [0112], Fig. 2.

Fig. 2



Brown (Ex.1010), Fig. 2.

H. Claim 8(a): The device of claim 1, wherein the reader interface is operable to wirelessly receive cardholder transaction information and to identify a valid user through at least one user-validation action, selected from a set of [sic]comprising:… a device user interface receiving a user entered a valid PIN or Key-Code; […] a device biometric recognition of a valid user…

1. Walker

141. Walker teaches that the payment device 100 "may be activated through the input of a unique cardholder identifier such as a personal identification number (*PIN*)" or "a suitable *biometric* record such as the cardholder's fingerprint." *Walker (Ex.1009),* [0043] (emphasis added), [0046] (before a "transaction-specific, single-use credit card number" is generated, the cardholder "first inputs *his PIN* or *biometric* data to access the device (step 351).") (emphasis added).

142. Walker's "single-use credit card number is generated by the device cryptoprocessor 205 using a private key 601 stored in the device memory" as well as a nonce value, initialization variable, and account number. *Walker (Ex.1009),* [0050], [0056], [0060]-[0063]. However, Walker does not teach how the values required for generating the single-use credit card number come to be stored in the device memory nor discuss specific messages exchanged with a point of sale merchant during a transaction.

2. Brown

143. Brown teaches that during "initial card personalization" a "stream of [personalization] data" is sent "over inductive or wireless interface 326" to appropriate memory locations in the card. *Brown (Ex.1010),* [0094]-[0095]. For example, a "table of cryptographic values associated with the PAN [Payment Account Number]" may be stored and then used in financial transactions. *Brown (Ex.1010),* Abstract, [0048]-[0049], [0134]. Brown further teaches "maintaining this channel for use with Near Field Communication or similar wireless communications." *Id.*, [0094], [0110] (describing "data receptors" on the card, such as a "Near field Communication device," that provide the card with "initial programming and personalization data" that is stored in the card's non-volatile memory). Therefore, Brown teaches that a payment account number (*cardholder transaction information* that will be used to complete a transaction) is received via the card's NFC interface (*the reader interface*).

144. Notably, the "data formats" of Brown's payment card 202 are dictated by industry standards including ISO and EMV standards. *Brown (Ex.1010),* [0070]. Brown explains that the components of the card "all must fit within these constraints" meaning the constraints of industry standards. *Id.* A POSITA would have understood that at the time, the relevant standards included EMV Version 4.3, dated November, 2001. Ex.1034 (*EMV4.3 Book 3)*. That standard identifies

transaction-related data that is sent to the card during the payment process, which includes *cardholder transaction information*. Ex.1034 at 54-56. For example, section 6.5.5 of the standard describes the transaction-related data that is sent to the card during a payment (i.e. "Transaction-related data" which is *cardholder transaction information*). As discussed further below, POSITA would have understood that, per the teachings of Brown, this data would be wirelessly received by Brown's card via Brown's NFC interface (the *reader interface*).

3. Motivation to Combine

145. In the combination, the NFC interface (reader interface) wirelessly receives *cardholder transaction information* first when account information is wirelessly provisioned to the card and second, during a transaction from the POS (point-of-sale) reader in accordance with EMV standards.

146. As discussed above at Claim 1(d), it would have been obvious and a POSITA would have been motivated to include an NFC reader interface on Walker's card as taught by Brown. A POSITA would have been further motivated to use that interface to transfer *cardholder transaction information* including Walker's account number and nonce values to the memory of Walker's payment card. A POSITA would have recognized the benefit of using an existing card communications channel to load required payment information to memory, rather than including additional

hardware in Walker's payment card for that purpose. The use of wireless technologies in this way would have been desirable to, for example, providing such information over a wired connection that would require additional hardware and time to physically connect each card before providing such information. A POSITA would have had a reasonable expectation of success in transferring transaction information to the memory of Walker's payment card using NFC because NFC technology was well-known and standardized by the Critical Date (as discussed above at Section VII.A-B; *Brown (Ex.1010),* [0067], [0070], [0090]-[0091]), and a POSITA would have been familiar with how to implement NFC to transfer data to a card memory, as taught by Brown.

147. In addition, a POSITA would have been motivated to use the NFC interface to receive *cardholder transaction information* from the POS terminal during the transaction based on the teachings of Brown, and based on a POSITA's understanding of EMV standard requirements at the time. A POSITA would have understood that security is enhanced when transaction-specific data (such as merchant specific data provided by the POS terminal) is available to the payment card and available to be used when generating a cryptogram. A POSITA would have understood that it was well-known and standardized for a POS terminal to send such information to a payment card at the time. *Ex.1034* (*EMV4.3)* at 54-56. A POSITA

would have been motivated to make a payment card that is compliant with industry standards—including EMV standards—so that the payment card will already be compatible with existing POS terminals and with payment processing systems, as specifically taught by Brown. *Brown (Ex.1010),* [0070]. Because the relevant feature—receiving cardholder transaction information wirelessly—from a POS terminal was standardized, a POSITA also would have had a reasonable expectation of success in making the proposed combination.

I. 8(b): wherein a display of the device is operable to display transaction information through a user interface, and wherein transaction information includes at least one of a set comprising: a transaction time; a transaction amount; transaction merchant information; a transaction location; a transaction facility; card information; a partial card number; graphical card images; and

148. Walker's device includes a "display for prompting the user or displaying information." *Walker (Ex.1009),* [0044], Figs. 1-2. The device also "quer[ies] the cardholder on display 102 whether it should generate a single-use credit card number" and further asks the user to enter "the amount of the purchase" (*a transaction amount*) and "a merchant code" (*transaction merchant information*) through a keypad 103 to be shown on display 102 (*user interface*). *Walker (Ex.1009),* [0046], [0043], Fig. 3B. A POSITA would understand that the amount and merchant code would be displayed in order to ensure that the information was correctly entered by the user.

J. 8(c): wherein upon validating the user, the user-interface is operable to receive a valid user input, of at least one user action selected from a set comprising: a payment approval authorization; a payment denial; and an adjustment of a transaction payment.

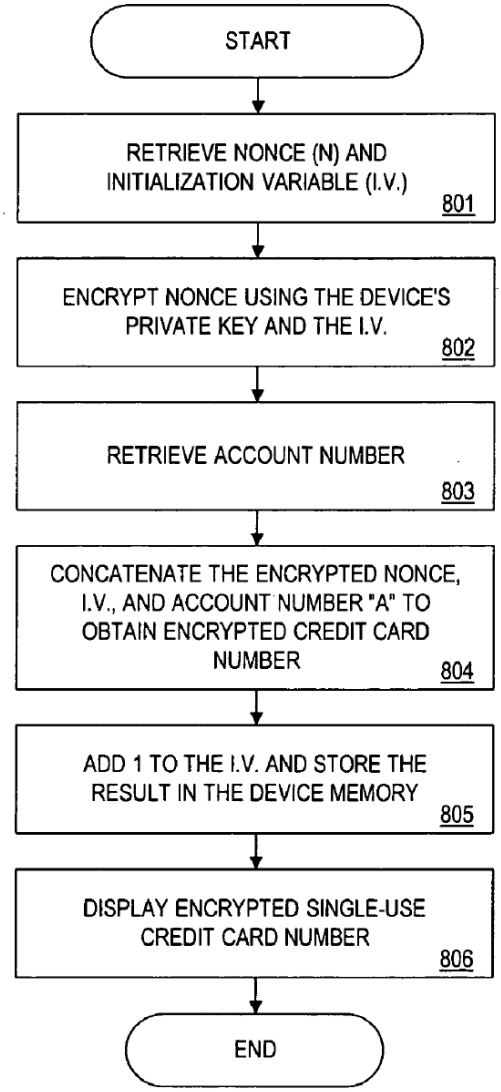
149. Walker teaches that "if access is granted" after the cardholder inputs his PIN or biometric data (*validating the user*), the device "quer[ies] the cardholder on display 102 whether it should generate a single-use credit card number" and "[t]he cardholder responds by requesting generation of a credit card number (for example, by keying 'YES')," which is a *payment approval authorization*. *Walker (Ex.1009),* [0046].

K. 10(a): The device of claim 1, wherein the processor cryptographically dynamically generates a one-time limited-use number based on combination of a card device transaction sequence count, and

150. Walker teaches that the cryptographic processor dynamically generates the single-use credit card number (i.e., *a one-time limited-use number*) based in part on an "initialization variable" that "is set at 0 (zero) when the card is newly issued, and is incremented each time a single-use credit card number is generated." *Walker (Ex.1009),* [0056], [0050], [0079] ("Each time the credit card is used the IV increments by 1."). Because the initialization variable is initially set at zero and then incremented each time a single-use credit card number is generated, it qualifies as *a card device transaction sequence count*.

151. Walker shows the steps for "generating an encrypted single-use credit card number" in Figure 8. *Walker (Ex.1009),* [0060]. First, in step 801 "the device central processor 101 retrieves the nonce 602 **and the initialization variable 704** from the device memory 104." Then "[i]n step 802, the nonce is **encrypted using** the user's private key K and **the IV**" as represented by the equation "C=E k(N, IV)." *Walker (Ex.1009),* [0060].

152. Ultimately, "the encrypted nonce C, the initialization variable IV, and account number A are concatenated to form an encrypted, single-use credit card number CCN: CCN=C_IV_A, where _ denotes concatenation." *Walker (Ex.1009),* [0061]. The IV is then incremented and the result is stored. *Walker (Ex.1009),* [0062].



Walker (Ex.1009), Fig. 8.

153. Because Walker's single-use credit card number is generated at the time of each transaction through encrypting various pieces of information, including the IV, Walker's device processor *cryptographically dynamically generates a one-time limited-use number based on combination of a card device transaction sequence count*.

L. 10(b): at least one of a set of information including:…a user card account number; a device account number; device secret keys; card issuer keys; … an account information; …

154. Walker's single use credit card number "is generated by the device cryptoprocessor 205, using a private key 601" (*device secret keys* or *card issuer keys*) by cryptographically combining the initialization variable with the account number (i.e., *a user card account number)* and the encrypted nonce value (*account information*), which is itself a cryptographic combination of the user's private key, the nonce (device secret key) and the IV. *Walker (Ex.1009),* [0060]-[0061].

M. 10(c): wherein the processor increments the card device transaction sequence count on each transaction.

155. Walker teaches that *the processor increments* the initialization variable (i.e., *the card device transaction sequence count*) each time a single-use credit card is generated for a transaction (i.e., *on each transaction*). *Walker (Ex.1009),* [0056], [0062] ("The initialization variable is incremented and the result is stored in the device memory 104 (step 805): IV=IV+1"), [0079].

XI. GROUND 2: CLAIMS 4-7 AND 9 ARE OBVIOUS OVER WALKER, BROWN, AND GAUTHIER

A. Claim 4: The device of claim 1, wherein said limited-use payment information is provided by a card issuing authority for use by the payment device and wherein the card processing authority rejects as invalid, any use of said limited-use payment information obtained via any means other than: a payment card reader reading said limited-use payment information from the reader interface.

1. Walker

156. Walker's "limited-use payment information" comprises Walker's account number, which is limited-use payment information provided by the issuer. *See* Claim 9(b).

2. Gauthier

157. Gauthier teaches a secured account number, different than the user's primary account number (PAN), that is **only** used for "wireless transactions" with a proximity reader, using "a contactless mode, infrared mode, RF mode (i.e. Radio Frequency), and the like[.]" *Gauthier (Ex.1011),* [0022], [0037], Fig. 1. Gauthier teaches that if a user "enters the secured account number onto a Web form to conduct a transaction, the transaction is not authorized by the issuer[.]" *Gauthier (Ex.1011),* [0023]. If the secured account number is entered into a web form by a thief that "surreptitiously intercepts the secured account number during a contactless purchase transaction," because it "is configured to resemble a real account number, it will deceive the unauthorized user into believing that it is an operable account number"

that can be used for web transactions. *Id.* Since the limited use account number is not usable for online transactions, it will "prevent the transaction that the thief tries to conduct from being authorized." *Id.* Therefore, use of the secured account number in an online (card-not-present) transaction is rejected by the card processing authority as not valid. *Id.*

158. In contrast, "[i]f the secured account number is valid and if the transaction is identified as a wireless transaction," the secured account number is converted to the user's real account number and transmitted for payment authorization. *Gauthier (Ex.1011),* [0043], [0054]-[0059], Figs. 3-4. Thus, if the secured account number is used in a card-present transaction with a proximity reader with a valid transaction identifier, it is approved as valid by the card processing authority. *Walker (Ex.1009),* [0057] ("the transaction is authorized…the transaction is cleared and settled"), [0058]-[0059].

159. Gauthier teaches a "smart card." *Gauthier (Ex.1011),* [0019], [0034]. The "secured account number may be stored in a database…preferably accessible to at least one of the payment processing system 120 and/or the issuer 130, since the issuer 130 authorizes or does not authorize the user's transaction." *Gauthier (Ex.1011),* [0039]. A POSITA would have understood that the card issuer and the card processing authority may be the same entity (as in the case of American Express

or Discover). Therefore, Gauthier teaches or renders obvious that the *card processing authority* rejects the transaction as invalid since it has access to the secured account number database. *Gauthier (Ex.1011),* [0029], [0035].

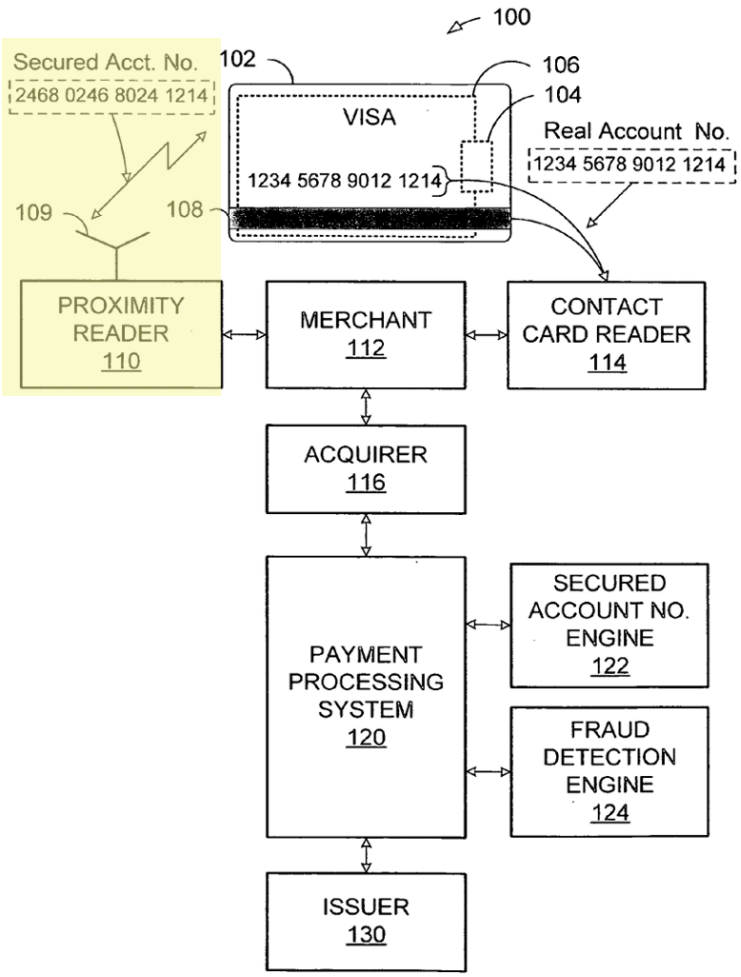


FIG. 1

Gauthier (Ex.1011), Fig. 1 (annotated).

160. Gauthier further teaches "a POS [point-of-sale] transaction type identifier" that indicates "that the transaction was a wireless type of proximity transaction." *Gauthier (Ex.1011),* [0042]. If a secured account number is received

by the payment processing system 120 but there is no identifier "indicating a proximity transaction" then the "fraud detection engine 124" associated with the payment processing system 120 (*card processing authority*) may "deny the transaction." *Gauthier (Ex.1011),* [0047], [0058]-[0059].

161. Gauthier teaches or renders obvious that the secured account number is *provided by the issuer*. Specifically, Gauthier teaches that the secured account number may be generated "when generating real account numbers" and "preloaded" on the consumer's device. *Gauthier (Ex.1011),* [0040]-[0041]. A POSITA would have understood the role of card issuing authorities in generating and assigning credit card account numbers. *See* VII.A, VII.C. Further, it would have been desirable for the real account number to be generated by a card issuing authority because, ultimately, the real account number is what is used to determine whether the transaction can be completed (e.g., to determine whether there are sufficient funds or credit in the account). *Gauthier (Ex.1011),* [0039].

162. Gauthier teaches that the secured account number changes when "the user's real account number expires" and it is therefore *limited use payment information*. *Gauthier (Ex.1011),* [0020].

3. Motivation to Combine

163. It would have been obvious and a POSITA would have been motivated to use an issuer-supplied secured account number in place of Walker's account number when making NFC payments, as expressly taught by Gauthier. In the Walker-Brown combination, the payment information transmitted via NFC to a merchant for payment includes an account number—an unchanging identifier for the cardholder. *Walker (Ex.1009),* [0048]-[0049], [0051]; *see* Claim 1(d). Walker's account number may resemble a traditional 16-digit card number and, if intercepted, a thief may attempt to use that number for an online payment transaction. *Walker (Ex.1009),* Fig. 6.

164. Gauthier teaches and a POSITA would have recognized that proximity-type wireless financial transactions may be intercepted, which was "a major concern for consumers and businesses alike." *Gauthier (Ex.1011),* [0005]-[0006]. Further, a consumer may not immediately know when their information has been intercepted, making enforcement efforts against bad actors challenging. *Gauthier (Ex.1011),* [0006] ("it is often too late to discover where the theft took place."). Gauthier teaches that if the secured account number is intercepted, and the thief attempts to use it for an online transaction, not only will the transaction be denied, but further "a fraud protocol" is initiated and the authorities may be alerted. *Gauthier (Ex.1011),* [0047], [0058]. A POSITA would have understood and would have been motivated to

implement a system that prevents unauthorized transactions and allows fraudulent transaction attempts to be immediately reported, recognizing the greater security of such a system. Long-running schemes where the malicious use of payment credentials goes undetected for long periods of time can be some of the most difficult because by the time the fraud is discovered the bad actor is more likely to have covered their tracks or gotten away with the ill-gotten funds.

165. A POSITA would have had a reasonable expectation of success in implementing an NFC-specific account number into Walker's payment card as it would merely change one issuer-provided (generally 16-digit) account number for another issuer-provided account number. Moreover, Walker, Brown and Gauthier teach similar smart card devices, so necessary modifications to the Walker-Brown combination would be minimal and implemented primarily through programmatic changes because the smart card already includes memory, a processor, and wireless interfaces. *Walker (Ex.1009),* Figs.1-2; *Brown (Ex.1010),* Fig. 1; *Gauthier (Ex.1011),* Figs. 1-2. In the combination, the payment card proximity interface (e.g., NFC) would transmit the secure account number to proximity reader, and the transaction would be deemed invalid if not also received with a valid POS transaction type identifier (e.g., "POS entry code 91"). *Gauthier (Ex.1011),* [0043]. Further, in the combination, the secured account number would continue to have an

expiration date, as taught by both Walker (*Walker (Ex.1009),* [0083]) and Gauthier (*Gauthier (Ex.1011),* [0020]). Notably, Gauthier cites an earlier patent in the Walker patent family (U.S. Patent No. 6,163,771), further confirming the relatedness of the references' teachings.

B. 5(a): The device of claim 1, wherein a request for payment includes at least one of a set comprising: payment information, transaction information, merchant information, and payment card reader information, and

1. Walker's Teachings

166. Walker's smart card device asks the cardholder "whether it should generate a single-use credit card number" and the cardholder responds "YES" and enters "the amount of the purchase in step 356 or a merchant code provided by the merchant" (transaction information and merchant information). Walker (Ex.1009), [0046].

167. Walker then teaches that the single-use credit card number is sent to the credit card issuer for authorization (as part of a <u>*request for payment*</u>). *Walker (Ex.1009),* [0045], Fig. 3A, [0048], Fig. 3B. The credit card issuer stores information associated with a transaction, including the transaction amount and merchant identification number, in a database. *Walker (Ex.1009),* [0055], Fig. 7. Thus, Walker teaches that the issuer knows the transaction amount and the merchant because it ultimately stores this information in a database.

168. Walker does not specify how the transaction and merchant information is used in the payment authorization process or what information is sent to the issuer during the authorization process other than the single-use credit card number. Walker does teach that issuers may chose not to "approve purchases that exceed available credit," indicating that the issuer is also sent the transaction amount (*transaction information*) at this time. *Walker (Ex.1009),* [0069].

2. Gauthier's Teachings

169. Gauthier teaches that an "authorization request message" (*request for payment*) can include "an account holder's payment account number" (*payment information*), "sale amount" (*transaction information*), "merchant transaction stamp" (*merchant information*), "POS transaction number [and] POS transaction type" (*payment card reader information*). *Gauthier (Ex.1011),* [0030]. *See '820 Patent*, 19:30-34 (identifying "amounts" as "credit card transaction information"). Gauthier teaches that the "authorization request message for a transaction is created after a customer purchases a good or service at a POS terminal" and is "sent from the POS terminal located at a merchant to the merchant's acquirer, to a payment processing system, and then to an issuer." *Gauthier (Ex.1011),* [0027], [0042]-[0043].

3. Motivation to Combine

170. It would have been obvious and a POSITA would have been motivated to include a purchase amount and merchant information in Walker's request for payment sent to the card issuer for authorization, as taught by Gauthier. Walker already teaches that a request for authorization is sent to the issuer which may deny authorization if the purchase "exceed[s] available credit[,]" which requires the issuer to know the transaction amount. *Walker (Ex.1009),* [0069]. Therefore, a POSITA would have understood and been motivated to include the purchase amount in the request for payment sent to the issuer. Likewise, a POSITA would have understood that including a merchant information in the payment authorization would provide the issuer with a record of where fraud has occurred, in the case that Walker's card was stolen and used improperly, and to also provide a history of a user's transactions. The merchant identification information could also be used to limit the types of transactions conducted with a specific card that have been defined by the user or issuer. *See Ex.1015* (*Patterson*) at 6:28-46 (discussing blocking criteria, including a list of merchants not allowed). Indeed, a POSITA would have understood that the issuer database including the merchant identifier and transaction amount for each transaction would first need to receive this information before storing it in the database. *Walker (Ex.1009),* [0055], Fig. 7. A POSITA would have had a reasonable chance of success in making the proposed combination because merchant

information and transaction information was already commonly received by and processed by issuers by the Critical Date and transmitting this additional information with other account information during a transaction would not be overly burdensome. *See Ex.1023* at 88 (EMV 4.3 Book 2 recommends using the amount authorized in an application cryptogram, for example). Moreover, it would be expected that the issuer receives this information in order to keep accurate records of transactions and account balances.

C. 5(b): wherein a card-present transaction is one including the limited-use payment information, and valid payment card reader information, and wherein a card-not-present transaction is one including at least a portion of said limited-use card payment information, and not including valid payment card reader information; and,

1. Gauthier's Teachings

171. *See* Claim 4. Gauthier further teaches that a secured account number is transmitted to a proximity reader device 110 (*payment card reader*) and further that "a POS [point-of-sale] transaction type identifier (indicative that the transaction was a wireless type of proximity transaction) (*valid payment card reader information*) is received by the merchant 112 and is transmitted to the acquirer 116" and further to the "payment processing system 120[.]" *Gauthier (Ex.1011),* [0042]; *see also* [0058]-[0059], Fig. 4.

172. Gauthier further teaches that someone may attempt to use the secured account number online (in a *card-not-present* transaction). *Gauthier (Ex.1011),* [0023]. In that case, the "authorization request message…does not have the transaction type identifier (e.g., POS 90), or other indicator, indicating a proximity transaction." *Gauthier (Ex.1011),* [0047], [0058], Fig. 4. In such a case, the transaction can be denied. *Gauthier (Ex.1011),* [0047], [0058]. Thus, Gauthier teaches there would be no *valid payment card reader information* if the secured account number is entered on a Web form as there is no payment card reader involved in the transaction. *Id.*

2. Motivation to Combine

173. It would have been obvious and a POSITA would have been motivated to include payment card reader information in Walker-Brown's request for payment sent to the card issuer for authorization, as taught by Gauthier, as discussed in Claim 4. A POSITA would have recognized that it was conventional in the credit card industry to include transaction type identifiers in transactions as Gauthier, a VISA-owned patent application, explains. *Gauthier (Ex.1011),* [0043] (identifying "a conventional number used in the credit card industry" as "POS entry code 91" and further recognizing "international standards organization (ISO) indicator[s]"). Further, a POSITA would have recognized that different payment methods have

different risk profiles, and that it may be easier to surreptitiously obtain payment credentials via contactless payment methods versus through a mag-stripe reader. *Gauthier (Ex.1011),* [0006]; A POSITA would further have understood the benefits of including a merchant identifier, as discussed above at Claim 5(a). A POSITA would have had a reasonable chance of success in making the proposed combination because the use of merchant identifiers was known to a POSITA and the subject of standards.

D. 5(c): wherein a processing authority is operable to approve as valid, a card-present payment transaction; and,

174. *See* Claim 4.

E. 5(d): wherein said card processing authority is operable to reject, as not valid, a use of the limited-use card payment information in a card-not-present payment transaction; and

175. *See* Claim 4.

F. 5(e): wherein a card issuing authority receiving said request for payment is operable to decline a transaction not involving a valid card-present use of a limited-use card payment information portion used in place of card issuer supplied payment information.

176. *See* Claims 4, 5(d).

G. 6: The device of claim 1, wherein a card processing authority is operable to reject as invalid, a use of the limited-use payment information provided via the reader interface, in online payment transactions.

177. *See* Claims 4, 5(b)-(c).

H. 7(Pre): The device of claim 1, wherein a card issuer providing the limited-use payment information, for use by the payment device, limits valid approval of said limited-use payment information to performing a card-present payment transaction by the card device, and wherein said card issuer declines as invalid a use of said limited-use payment information in transactions other than wherein the payment device is present, and

178. *See* Claims 4, 5(b)-(c).

I. 7(a): wherein a card issuer limits said card payment information to use for a finite amount of time, and declines as invalid use when said amount of time has expired, and

179. Walker's account number expires when Walker's payment card expires. *Walker (Ex.1009),* [0083]-[0084]. Walker also teaches that the single-use credit card number may be unique to the specific data and time to avoid so-called 'replay attacks.'" *Walker (Ex.1009),* [0047], [0085]. Gauthier likewise teaches that the secured account number changes when "the user's real account number expires." *Gauthier (Ex.1011),* [0020]. A POSITA would have understood or found obvious that an expiration date is a *finite amount of time* for which the payment information is valid for use, after which attempts to use the payment information will be declined. A POSITA therefore would have found it obvious and would have been motivated to implement a secured account number (per Gauthier) that expires on Walker's payment card for the reasons discussed in Claim 4. A POSITA would have also been motivated to include Walker's timestamp in the payment information such that if the time falls outside of time window, it would not be considered valid. This was

commonplace at the time in order to prevent replay attacks, which were a well-known source of fraud.

J. 7(b): wherein a card issuer limits use to payment for transactions with the user approving, and declines as invalid use when the card user is denying an approval, and

180. *See* Claim 5(a). Walker teaches that the account number assigned to Walker's device cannot be used for payment alone but rather must be used to generate a single-use credit card number. *Walker (Ex.1009),* [0050] ("knowledge of the account number does not allow an attacker to generate a valid single-use credit card number"), [0072]. Walker further teaches that the single-use credit card number can only be generated with user approval for the transaction. *Walker (Ex.1009),* [0046] (cardholder responds "YES" and enters "the amount of the purchase in step 356 or a merchant code provided by the merchant"). Therefore, Walker teaches that the issuer limits use of the account number for *transactions with the user approving* where the account number is invalid when used on its own, i.e. *when the card user is denying an approval* and therefore a single-use credit card number is not generated. *Walker (Ex.1009),* [0046], [0050].

181. It would have been obvious and a POSITA would have been motivated to implement Gauthier's secured account number on Walker's payment device in place of Walker's account number such that the secured account number cannot be

used for payment alone, but rather as part of a single-use credit card number generated when the user approves the transaction—as taught by Walker—for the reasons discussed in Claim 4.

K. 7(c): wherein a card issuer limits to use in place of card issuer information for payments by the payment device.

182. Walker's account number is assigned to Walker's payment device for use by the payment device and cannot also be assigned to another device unless Walker's card expires. *Walker (Ex.1009),* [0083]-[0084]. Even after Walker's card expires, any new card provided with the same account number must be assigned a "different nonce and private key" so that "any credit card numbers generated with the old credit card will not match any new credit card numbers[.]" *Walker (Ex.1009),* [0084]-[0085].

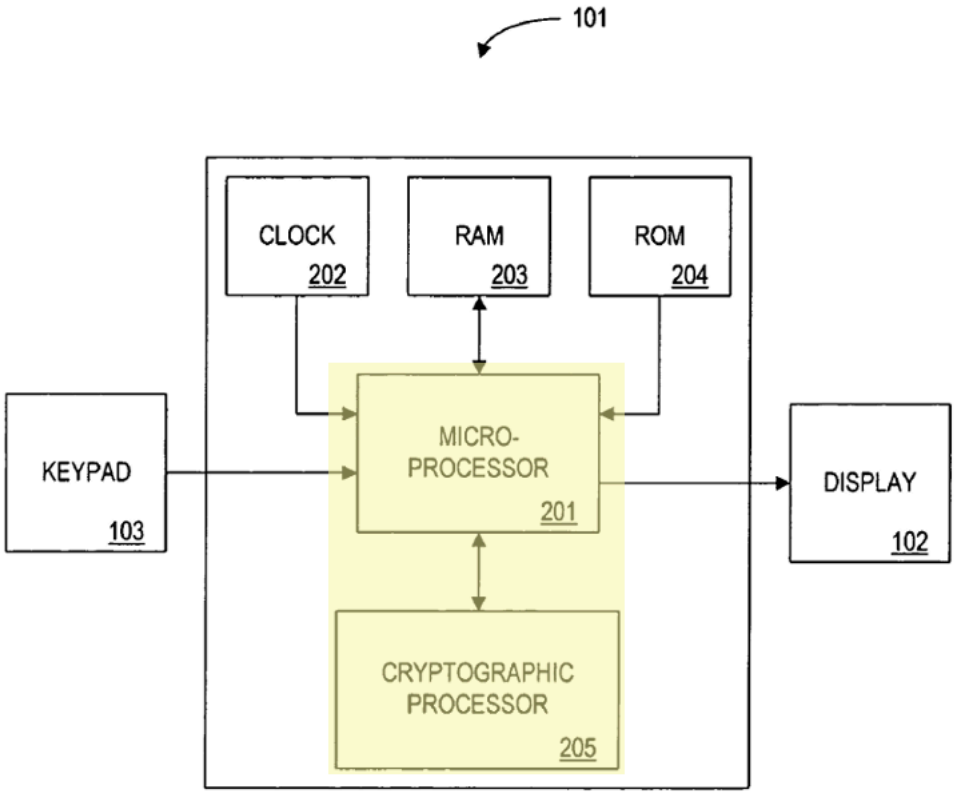
183. Gauthier's secured account number likewise is assigned to a particular payment device (*Gauthier (Ex.1011),* [0019], [0021], [0040]) and likewise must be converted to the user's real account number (is used *in place of card issuer information*). *Gauthier,* [0055].

184. Therefore it would have been obvious and a POSITA would have been motivated to implement Gauthier's secured account number on Walker's payment device to (1) be limited to use by Walker's payment device and (2) be used in place of card issuer information for the reasons discussed in Claim 4.

L. 9(a): The device of claim 1, wherein a dynamically-generated one-time limited-use payment information portion is generated by said processor when coupled to a reader interface accessible to said processor, and

185. Walker teaches a single-use credit card number that is *dynamically-generated* by the cryptoprocessor of Walker's payment card. Walker (Ex.1009), [0050], [0056].

186. As discussed above at Claim 1(d), in the combination, Walker's payment card includes a reader interface comprising a dynamic magnetic stripe and/or NFC interface coupled to Walker's micro-processor. In the combination, the reader interface *is accessible* to Walker's cryptographic processor through Walker's microprocessor to generate the single-use credit card number (*one-time limited-use payment information*).



Walker (Ex.1009), Fig. 2.

M. 9(b): wherein the payment information conveyed to a payment card reader, at the time of transaction, includes at least one of a portion of: a static limited-use portion; and a dynamically-generated limited-use portion, and

187. Walker's one-time use credit card number is a concatenation of "the encrypted nonce C, initialization variable IV, and account number A… CCN: CCN=C_IV_A." *Walker (Ex.1009),* [0061]. In combination with Gauthier (*see* Claim 4), it would have been obvious and a POSITA would have been motivated to use an issuer-supplied secured account number in place of Walker's account number.

Therefore, Walker's credit card number includes a *static limited-use portion* (secured account number) and an encrypted nonce generated from the private key and incremented IV (*dynamically-generated limited-use portion*). *Walker (Ex.1009),* [0060].

188. Walker's account number is *limited-use* because it expires or is limited in time. *Walker (Ex.1009),* [0059], [0084] ("After a cardholder's card expires, his account number can be reused."), [0085]. Further, the number of times the account number can be used is limited by the size of the initialization variable (IV) allowed, with a limit of 512 uses with a 9-bit initialization variable. Walker (Ex.1009), [0058]-[0059]. In the combination, the secured account number would likewise expire, as taught by both Walker and Gauthier. *Gauthier (Ex.1011)* [0020] ("The term 'static' means that the secured account number does not have to change between transactions, but may change when…the user's real account number expires.").

189. The encrypted nonce is also *limited-use* because it can only be used for the transaction with the associated IV. *Walker (Ex.1009),* [0065]-[0067].

N. 9(c): wherein said static limited-use payment information is provided by a card issuing authority for use in place of a card issuer payment information.

190. In the combination, Gauthier's secured account number is used by Walker in place of the assigned conventional credit card account number. *See* Claim 4; *Gauthier (Ex.1011)* [0020], [0043], [0054]-[0059], Figs. 3-4 (describing conversion of secured account number to a user's real account number in payment processing). Gauthier's secured account number, like Walker's conventional credit card number, would still be assigned by the card issuing authority. *Walker (Ex.1009),* [0049]; *Gauthier (Ex.1011)* [0029] (issuer issues credit cards with credit card numbers); [0040] (secured account number generated when real account numbers are generated).

XII. GROUND 3: CLAIM 2 IS OBVIOUS OVER WALKER, BROWN, AND ENG

A. Claim 2: The device of claim 1, wherein the body comprises fixed payment information disposed thereon and wherein the fixed payment information includes only: a card-holder name; a payment issuing logo; and a card payment network logo, and wherein further, the body is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.

1. Printed Subject Matter

191. The limitation "comprises fixed payment information disposed thereon" is directed to printed matter which I understand has no patentable weight if it has no functional or structural relationship to the claimed card device.

192. As I discuss in Claim 1(a), a POSITA would have understood that, at the time, it was common for a payment card (such as a credit or debit card) to have fixed payment numbers such as a PAN (primary account number), expiration date, CVC, account holder name, and various logos. However, this printed information is not relevant to conducting the claimed payment transaction. The plastic card is merely how the payment information is stored for later reference by the user. I was asked to consider whether a POSITA at the time of the '820 Patent would have understood the card-holder name, a payment issuing logo, and a card payment network logo on the face of a common payment card to have a functional relationship with the material (e.g., plastic) of the payment card itself. I was unable to identify any such functional relationship. The physical payment card simply serves as the medium on which the information is attached, the same way paper may serve as the medium when a payment card number is printed on a receipt.

193. I was also asked to consider whether the limitation "having fixed payment information disposed thereon" has any relationship to any other element of

the claims that might impact my opinion. I did not see any such claim language. The same is true of the lack of certain information on the physical card.

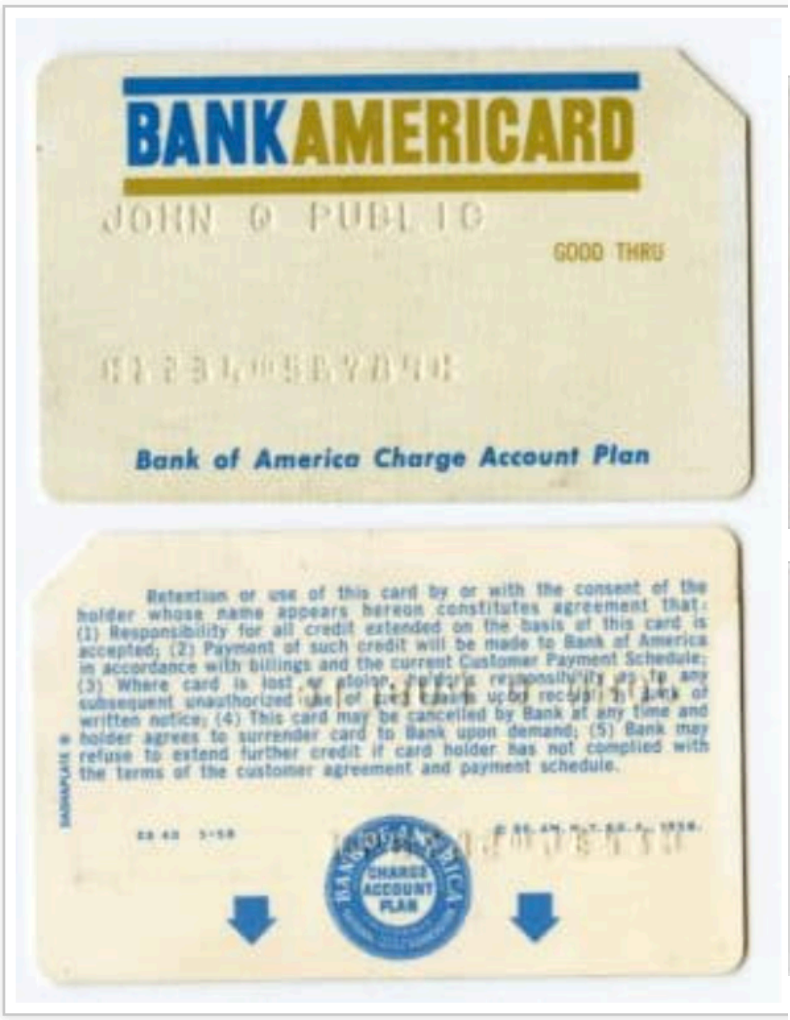
194. To the extent this limitation is entitled to patentable weight, it is taught by Walker and Brown in view of Eng.

2. Walker's Teachings

195. Walker teaches a card with a card body free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon. See Claim 1(a).

3. Eng's Teachings

196. In related art, Eng teaches a card that has: (1) a card-holder name, (2) credit card logo (card payment *network logo*), and a (3) Bank Name (*payment issuing logo)*. *Eng*, [0020]-[0021], [0042]. Notably, when a traditional credit card includes a bank name on the front, the name is typically stylized, i.e., the bank's logo with the bank's chosen font, capitalization scheme, etc. This began with Bank of America's BankAmericard in the 1950's (*Banker & Tradesman (Ex.1017))* (below on the left) and continued through the early 2000's to today *(Colnect (Ex.1018))* (below on the right):



Front and back of a sample of the card used in the 1958 Fresno Drop. National Numismatic Collection, National Museum of American History, Smithsonian Institution | CC0

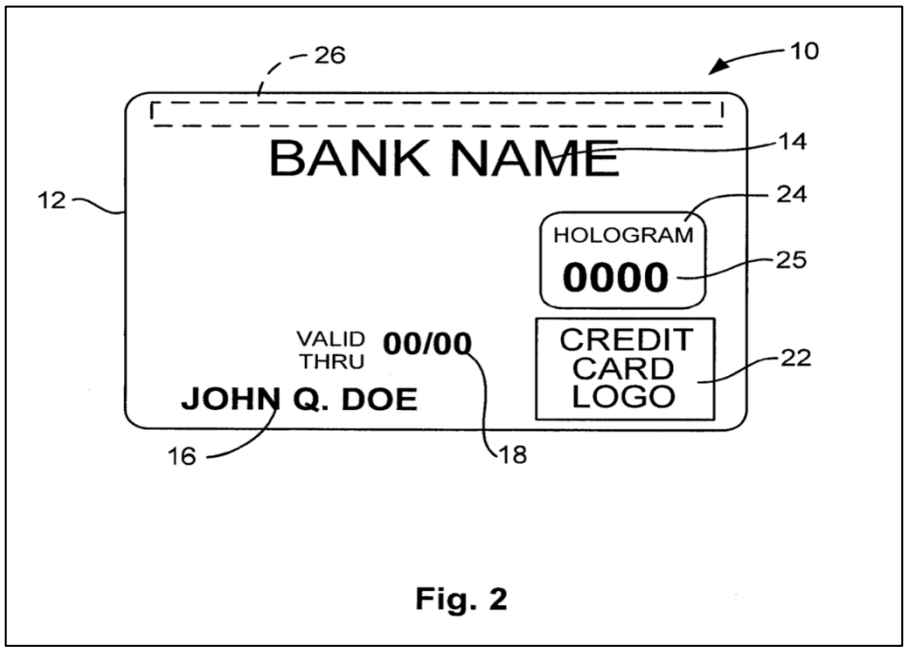


Fig. 2

Eng, Fig. 2.

197. To the extent embodiments of Eng's card also includes an expiration date and a portion of a PAN, a POSITA would have no reason to include those pieces of information on Walker's smart card device, since the payment credentials used by Walker's smart card constantly change and are one-time use. *See* Claim 1(e); *Walker (Ex.1009),* [0043], [0046].

4. Motivation to Combine

198. It would have been obvious and a POSITA would have been motivated to modify Walker's smart card to include a fixed card-holder name, payment issuing logo, and card payment network logo, as taught by Eng. A POSITA would have understood that a user would have found it valuable to distinguish their cards from each other (for example, with a payment issuing logo (e.g., Chase Bank logo) and

card payment network logo (e.g., VISA)) and from similar cards that others in their household might have (e.g., with a cardholder name). This information prevents a user from using a card that was not intended to be used for a transaction. Each of these pieces of information was well-known to a POSITA and common on payment cards prior to the '820 Patent, therefore, a POSITA would have had a reasonable expectation of success in making this combination of known elements without undue experimentation.

XIII. GROUND 4: CLAIM 3 IS OBVIOUS OVER WALKER, BROWN AND PATEL

A. Claim 3(a): The device of claim 1, wherein the limited-use payment information is conveyed via the magnetic stripe and is unique to the payment device and to the magnetic stripe, and

1. Walker-Brown

199. As discussed in Claim 1(d), in the Walker-Brown combination, Walker's payment card is provided with a dynamic magnetic stripe, as taught by Brown. In the combination, Walker's magnetic stripe would be "reprogramed to reflect the latest" one-time use payment information, per Brown's teachings. *Brown (Ex.1010),* [0022]. The magnetic stripe would further include the information required by standards to be present in mag-stripe track data to ensure that Walker's payment card is usable in conventional POS infrastructure, including a CVC value. *Brown (Ex.1010),* [0023], [0045], Fig. 2, [0069] (218, "legacy reader"); *see also*

Section VII.A.1. Brown further teaches preferably varying just the CVV and leaving the account number unmodified. *Brown (Ex.1010),* [0043] ("The PAN, expiration date, or the CVV2/4DBC could all be varied, but **most initial implementations are likely to vary only one of them, e.g., the CVV2**/4DBC.").

2. Patel's Teachings

200. Patel teaches assigning a payment card a "dynamic CVV" that "is read, changed, and rewritten to the card with each transaction." *Patel (Ex.1012),* Abstract. Patel's dynamic CVV is coded to the magnetic stripe "[t]o pay for the goods or services" through "a magnetic card reader 130" or RFID interface. *Patel (Ex.1012),* [0055]-[0057]. The dynamic CVV is transmitted to the financial institution 150 (card issuer) which "authenticates the verification data, including the dynamic CVV 330, and transmits a verification code, including a new dynamic CVV 330 to the transaction device 130." *Patel (Ex.1012),* [0059]. "The transaction device 130 reads the new dynamic CVV 330, and writes the new CVV 330," which was received from the card issuer, "to the magnetic strip 220" of the payment card. *Patel (Ex.1012),* [0060]. The new dynamic CVV can then be used by magnetic strip in a subsequent transaction to help prevent fraud. *Patel (Ex.1012),* [0064].

201. Patel teaches that "a static CVV may also be provided for manual entry" to "facilitate online transactions." *Patel (Ex.1012),* Abstract, [0007]. [0072] ("[A]

static CVV 230 is printed on the card and it is retained as perpetually valid only for purchases where card data are input manually."). Therefore, Patel teaches that the dynamic CVV code is *limited-use payment information* that is *conveyed via the magnetic-strip*. It is further *unique to the payment device and to the magnetic stripe*, as Patel teaches that the dynamic CVV is assigned by the financial institution to a specific payment card (*payment device*).

3. Motivation to Combine

202. A POSITA would have been motivated and would have found it obvious to implement Patel's dynamic CVV techniques in the Walker-Brown payment device for use in mag-stripe payments. A POSITA would have understood that in magstripe payment transactions, track data is transferred to the merchant, including a verification code. *Brown (Ex.1010),* [0109] (citing ISO/IEC Standards 7810, 7811-1-6, and 7813). Typically, the discretionary data segment includes the card verification code. For example, as discussed in Section VII.A.1, typical track 1 data includes a discretionary data field in which the CVV or CVC can be included. Bona similarly describes ISO 7813 as including the CVV or CVC in the discretionary data field. *Bona (Ex.1019)*, [0102]. Replacing the static CVV in the magnetic stripe data with a dynamic alternative would have increased the security of the payment system as another barrier for an unauthorized user to use the payment

credentials, which a POSITA would have been motivated to implement. Indeed, the use of dynamic CVVs was well-known at the time. *See* Section VII.C.2. For example, MasterCard and Visa were already replacing a CVC/CVV with dynamically generated CVC3/dCVVs inserted into the Track 1 and Track 2 data to be used with traditional POS readers. *See Yeager (Ex.1029)*, [0049]-[0051], [0162].

203. A POSITA would have found it obvious to modify the Walker-Brown combination based on Patel's teachings because a dynamic CVV value was a known solution and it would have improved Walker's similar system in the same way, allowing the POSITA to obtain the predictable result described in Patel, namely increased security. Specifically, the use of a dynamic CVV "prevents a malicious actor from successfully completing several transactions by transmitting the old CVV 330[.]" *Patel (Ex.1012),* [0063]; *see also*, [0066]-[0070]. A POSITA would have had a reasonable chance of success in implementing a dynamic CVC into the Walker-Brown payment device because the Walker-Brown payment device already includes a programmable magstripe to provide data in a Track 1/2 format and because Brown already contemplates a dynamic CVV value being programmed to the magstripe. *Brown (Ex.1010),* [0043], [0079].

B. 3(b): wherein the limited-use payment information is limited to use by the payment device and is operable for conveying payment information to a magnetic-stripe payment card reader, and

204. Patel's dynamic CVV and the complete limited-use payment information in the combination provided to the merchant through the magnetic stripe are *both limited to use by the payment device* (i.e., credit card) and would be conveyed *to the magnetic-stripe payment card reader* in the combination. *See* Claims 1(d)-(e), 3(a).

C. 3(c): wherein said limited-use payment information has a limited period of valid use, and

205. Patel's dynamic CVV and the complete limited-use payment information are both one-time use information. *See* Claims 1(e), 3(a); *see also Walker (Ex.1009),* [0050] ("different for each transaction"); *Patel (Ex.1012),* [0007] ("dynamic CVV is rewritten to the card with each transaction"). Further, Walker teaches limiting the validity of payment credentials to a set time period (e.g., 5 minutes) for increased security. *Walker (Ex.1009),* [0102]-[0103]. ("Repeated power switch presses will re-display the same number until the display timer elapses, typically 1-5 minutes. Once the timer elapses, pressing the power switch again will restart the display timer and yield a new display number.").

D. 3(d): wherein said limited-use payment information is not valid when used other than through a magnetic stripe payment card reader.

206. Patel teaches that the dynamic CVV is coded to the magnetic stripe, and further that "a static CVV may also be provided for manual entry" to "facilitate online transactions." *Patel (Ex.1012),* Abstract, [0007]. Therefore, a POSITA would have understood that Patel teaches the dynamic CVV coded to the magnetic stripe is only used in card present transactions and would not be valid for online transactions (where the static CVV must be used). In the combination, the complete limited-use payment information encoded on the magnetic stripe of Walker's payment card is only used for magnetic stripe payments with a magnetic stripe payment card reader. A POSITA would have understood that a magnetic stripe must be read by a magnetic stripe payment card reader and specifically cannot be read by an NFC reader. Further, information used in a magnetic stripe transaction and an NFC-based payment differs, as discussed above at VII.A.

XIV. GROUND 5: CLAIMS 11, 13-15, AND 17-20 ARE OBVIOUS OVER COLLINGE, KRANZLEY AND BROWN

A. 11(pre): An online payment system, the system comprising:

1. Collinge's Teachings

207. Collinge teaches *a payment system* that includes generating and "provisioning payment credentials to a mobile device" for "use in mobile payment transactions." *Collinge (Ex.1004), Abstract,* [0006], [0039].

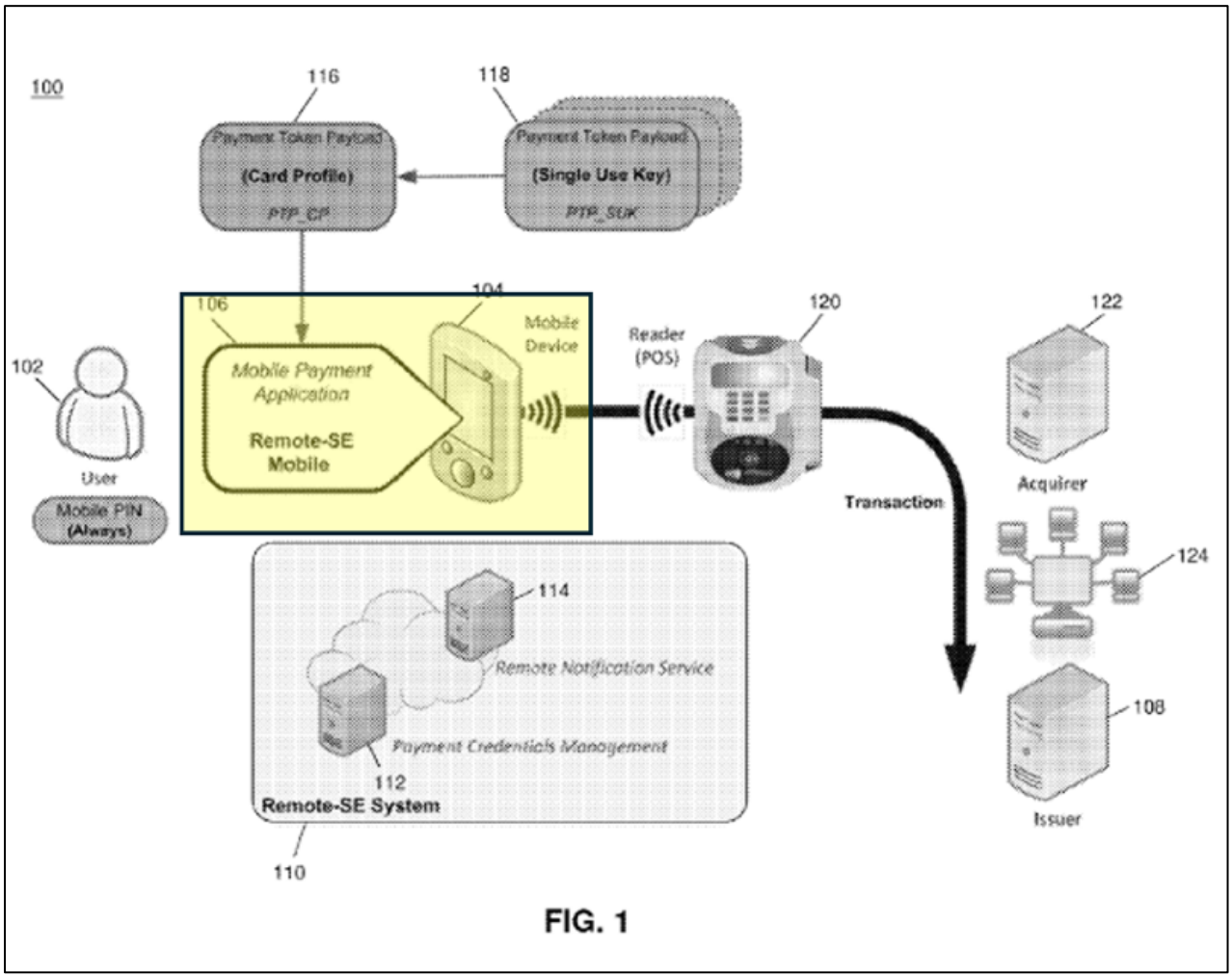
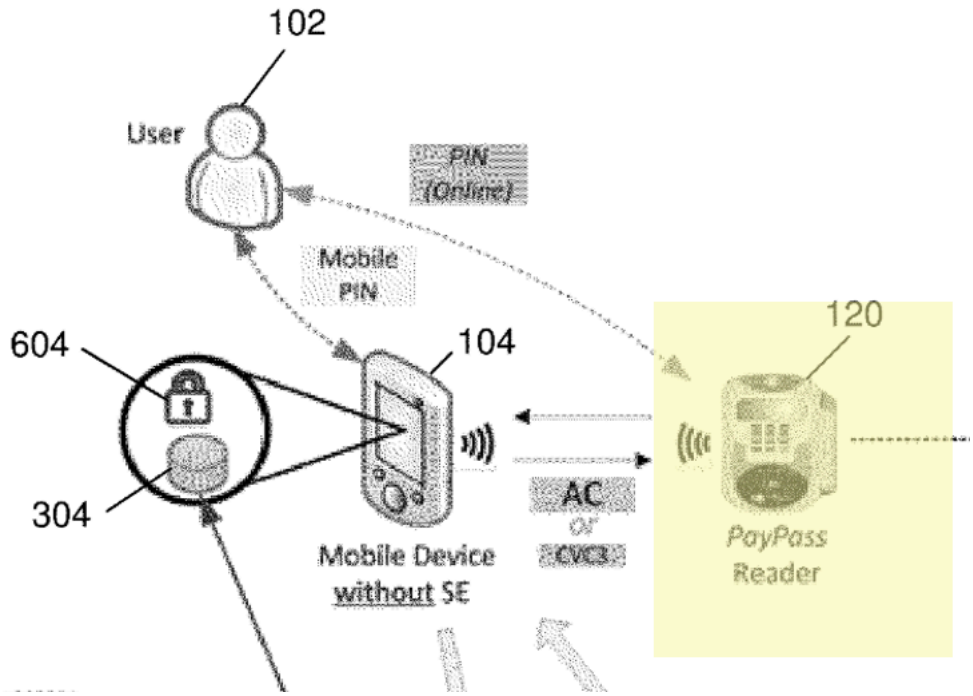


FIG. 1

Collinge (Ex.1004), Fig. 1. (annotated)

208. One motivation for Collinge's invention was to allow a user to "conduct PayPass® transactions at PayPass®-enabled merchants with a mobile device." *'095 provisional 9* [0003].



Collinge (Ex.1004), Fig. 6 (excerpted, annotated).

209. Collinge teaches that a virtual primary account number (VPAN) can be used as an alternative to the card PAN. *'248 Provisional (Ex.1008),* 159-160. Collinge teaches that using a VPAN is safer and can "mitigate the risk of any misuse of a PAN value" but provides limited implementation details.*'248 Provisional (Ex.1008),* 159-160. I note that a POSITA would have been well-familiar with the use and benefits of a PAN alternative such as a VPAN at the Critical Date, as I discuss in detail above at VII.C.1.

210. I further note that Collinge does not specifically teach how Collinge's payment credentials would be used to make purchases from a website, though a

POSITA certainly would have recognized that online commerce was common at the time.

2. Kranzley

211. In related art, Kranzley teaches a mobile device 102 which includes a mobile payment application that may be used at "a physical storefront or **electronic commerce merchant**." *Kranzley,* [0038] (emphasis added). Kranzley teaches that the payment application may be "configured to operate in accordance with the PayPass standard[.]" *Kranzley,* [0020].

212. Kranzley teaches a "static virtual payment account number (or 'VPAN')" is used as an "alternative" to the issued PAN. *Kranzley,* [0036]. "An authorized user of the payment application may access the VPAN and use it to make a purchase transaction…along with its expiry date, and a dynamic code (generated by the payment application) to the merchant." *Kranzley,* [0036]. Then, "[t]he payment provider uses the VPAN to look-up an actual PAN associated with a payment account of the customer[.] *Kranzley,* [0037]. The VPAN "may have its own virtual expiry date." *Kranzley*, [0036]. Use of the VPAN "ensure[s] that merchants are not made aware of the actual payment card information as they are only exposed to the VPAN information." *Kranzley,* [0049].

213. Kranzley teaches "in electronic commerce environments, the customer may cause the payment application in the mobile device to display a VPAN, expiration date and dynamic account validation code" on the mobile device's display so that "[t]he customer may read the information from the display device and then key in that data into a Web page on a computer to complete the ecommerce transaction." *Kranzley,* [0040].

3. Motivation to Combine

214. To the extent the preamble is limiting, it would have been obvious and a POSITA would have been motivated to modify Collinge's mobile device to display payment credentials to complete an online payment transaction, as taught by Kranzley.

215. At the time, mobile wallets were well-known, as I discuss above at VII.B.6. Kranzley demonstrated the feasibility of using a particular mobile wallet—PayPass—in an online system. *Kranzley,* [0036]. A POSITA would have appreciated the benefits of performing an online transaction using Collinge's secure payment credentials and convenient mobile payment application. Specifically, one of the benefits of a mobile wallet application is that a user would no longer be required to carry multiple payment options—therefore there would be a desire for the mobile wallets payment credentials to be accepted in the most places possible. While a

POSITA would have recognized that there are a few options for how to use mobile wallet crediential online, a POSITA would have recognized that simply displaying payment credentials on the screen of Collinge's mobile device would have beneficially allowed the credentials to be used for online transactions without requiring any additional hardware (for example, a separate computer with an NFC reader) or separate online systems (such as, for example, requiring the website seeking to accept mobile wallet payment credentials to send the user to a separate specialized payment application).

216. A POSITA would have had a reasonable chance of success in making the combination and would have recognized that (1) both Kranzley and Collinge teach compliance with PayPass standards when generating payment information, meaning they already have considered standard MasterCard payment requirements and (2) the primary modification is simply displaying payment information that Collinge's mobile device already has on Collinge's touchscreen display (that Collinge's mobile device already has), which would have been well-within the skill level of a POSITA. Therefore, use of Collinge's payment credentials for online payment would have combined known elements to predictably allow display of payment credentials on the screen of Collinge's mobile device.

217. A POSITA would have further been motivated to assign a VPAN to payment cards registered with Collinge's payment system, as taught by both Collinge and Kranzley, and to use the VPAN in place of a PAN for increased security. *'248 Provisional (Ex.1008),* 159-160; *Kranzley,* [0049]. A POSITA would have recognized the risk that payment credentials could be intercepted in online transactions (such as if a user inadvertently find themselves on a fraudulent webpage online that asks for payment credentials). Therefore, a POSITA would have appreciated the security benefits of using an alternative to a credit card number (PAN) for online payments.

218. In addition, it is more convenient for a user to obtain a replacement VPAN rather than to have to update their PAN. If a VPAN is stolen, only the VPAN will need to be replaced, and the user will not be required to get a new physical card or to update automatic payments that use the PAN. *Grigg (Ex.1047),* [0074], Fig. 6. But if the user's PAN is entered and stolen, the user will require a new payment card with a new account number, and they will have to re-setup any existing automatic payments.

219. In the combination, Collinge's mobile device would receive the VPAN, in place of PAN information in Collinge's payment credentials provisioned to the Collinge's mobile payment application as part of card profile 116. *Collinge*

(Ex.1004), [0048], Fig. 6, [0104] (card profile (PTP_CP)); *'098 Provisional (Ex.1008)*, [0101] ("Payment Token Payload – Card Profile (PTP_CP_ contains the Payment Credentials required to perform a [MasterCard] *PayPass* transaction" including "data elements such as: **PAN,** PSN + Track Data."); [0049] ("The common payment credentials "may include all data elements common to any type of payment transactions, such as both mag stripe and m/chip payment transactions. Such data elements may include payment account number, tracking data, and card layout description data."). Kranzley already teaches that a VPAN would be provisioned to the mobile device in place of a PAN. For example, in Figure 5 "[t]he table includes entries identifying VPANs that have been issued or assigned by the payment provider 110."

500

VPAN 502	PAN 504	STATIC CARD VERIFICATION CODE 506	COUNTER 508	VPAN EXPIRY 510
5555-5555-5555-5555	5422-4343-2324-1332	432	0	04/01/2009
5555-5457-4381-3243	5489-2382-1818-4343	312	4	04/30/2009
5555-5929-3453-1242	5982-2381-2848-1281	647	9	05/4/2009
5555-2438-3422-4629	5898-2428-5421-0938	321	0	03/28/2009

FIG. 5

Kranzley (Ex.1013), Fig. 5.

220. The VPAN would then be stored in Collinge's storage 304 within the card profile as a replacement for Collinge's PAN and in the same manner that Collinge's PAN was stored. *Collinge (Ex.1004),* [0068]; *Kranzley (Ex.1013),* [0036] (The "payment application of the mobile device may also store at least one static virtual payment accountment account number (or 'VPAN')").

221. Therefore, Collinge's mobile device would not be required to store the PAN, which is a sensitive financial number. It was well known in the art that storing sensitive information such as a PAN in fewer locations can lessen the risks of the sensitive information being compromised. For example, PCI SSC teaches that "[s]toring tokens instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment[.]" *PCI SSC (Ex.1031),* 3. PCI SSC also teaches that "[o]ne of the primary goals of tokenization solution should be to replace sensitive PAN values with non-sensitive token values." *PCI SSC (Ex.1031),*

222. It was also well known in the art that a device without a secure element (SE), such as Collinge's mobile device, could be vulnerable to malicious attacks and therefore, storing Kranzley's VPAN instead of the PAN on Collinge's mobile device would have increased security for the user's account. *See Ghosh (Ex.1048),* 51 ("Without a secure infrastructure for computing on the device, achieving secure m-

commerce may not be possible."); *Collinge (Ex.1004),* [0003]-[0004]. ("mobile phones with secure element hardware (e.g., a Secure Element chip) are used to securely store payment account credentials, such as credit card credentials. However, not all mobile devices have secure elements."). A POSITA would have understood that it is valuable to remove all traditional payment device account numbers from a user device so that if the device were stolen, the thief would have access only to VPANs. *Grigg (Ex.1047),* [0074].

223. Ultimately, Collinge's payment application would use the VPAN instead of a PAN when generating payment credentials; nothing else about how Collinge generates payment information would change. The simple substitution of Collinge's PAN with a VPAN is a substitution of one known element (a PAN) for another (a VPAN) and a POSITA would have understood that the substitution would have predictably increased the security of Collinge's payment system and protected the user's sensitive PAN information for all of the reasons discussed above. Since Colline already teaches using a VPAN, the issuer would have already been equipped to process and verify transactions when an alternate to the PAN was used. *'098 Provisional (Ex.1008)*, 159-160.

B. 11(a): a payment device comprising no fixed payment numbers visible thereon; and

224. For the reasons I previously discussed, the limitation that the payment card be "free of any fixed payment numbers visible thereon" is directed to printed matter that has no functional or structural relationship to the claimed card device and is entitled to no patentable weight. In any event, this limitation is obvious based on Brown's teachings.

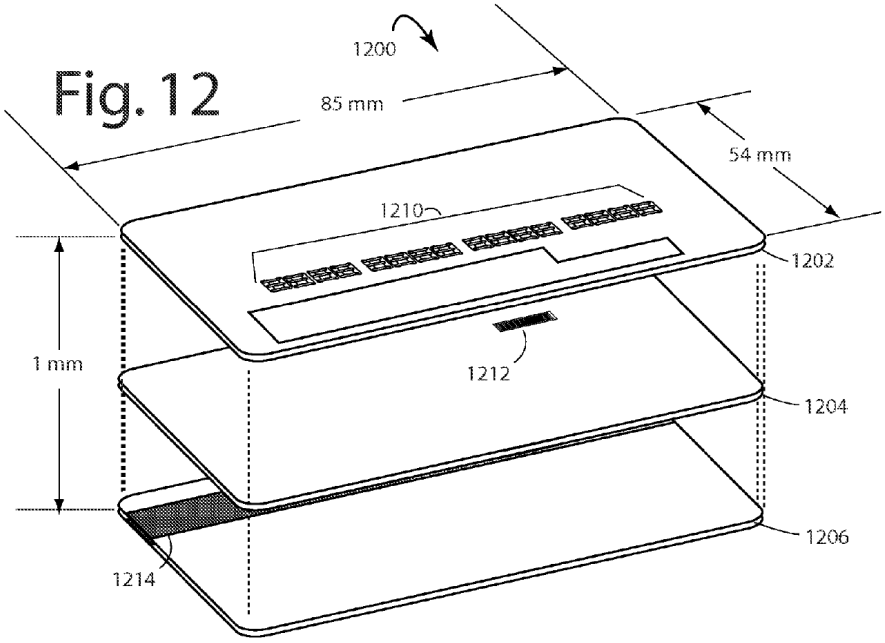
1. Collinge's Teachings

Collinge teaches a mobile payment system wherein a user may register a mobile device to be connected to a payment account (such as a credit card account) so that Collinge's mobile device may be used instead of the physical payment card to complete payment transactions. Per Collinge, "[a] payment card may be a physical card that may be provided to a merchant, or may be data representing the associated payment account (e.g., as stored in a communication device, such as a smart phone or computer)." *Collinge (Ex.1004),* [0038]. Collinge teaches that the authentication credentials provisioned to Collinge's mobile device are "associated with a payment card." *'095 Provisional (Ex.1005),* [0051], Fig. 2.

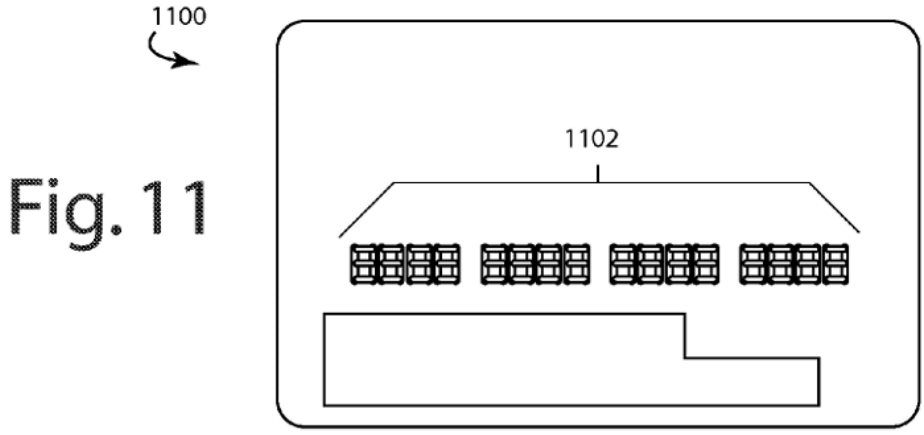
2. Brown's Teachings

225. Brown teaches a smart payment card (*payment card device*) that is "1mm" in thickness and therefore is a thin card-shaped device. *Brown (Ex.1010),*

[0091] (citing payment card thickness standards), [0200] (describing a "smart card" as "1mm" in thickness)



Brown (Ex.1010), Fig. 12. Brown's payment card has a "full personal account number (PAN) [that] has been **implemented to be variable** on a visual display." *Brown (Ex.1010),* [0200] (emphasis added).



Brown (Ex.1010), Fig. 11 (showing variable account number). Accordingly, Brown teaches a wholly variable payment account number and therefore there are *no fixed account* numbers visible on Brown's payment card.

226. Brown's smart card includes a "dynamic magnetic stripe." *Brown (Ex.1010),* [0022], Abstract, [0041], [0066]-[0067], [0070].

3. *Motivation to Combine*

227. A POSITA would have found it obvious and would have been motivated to use Brown's payment card device free of any fixed payment numbers visible thereon with Collinge's NFC-enabled computing device (i.e., cell phone) and payment system.

228. It was well-known that many point-of-sale terminals only accepted a physical magstripe payment method. A POSITA would have understood, that at the time "the predominate point of sale reader technology deployed worldwide" continued to be "magnetic stripe." *See Bona (Ex.1019),* [0008]. At thie time, it was estimated that there were "20,000,000 magnetic stripe readers in the field." *Id.,* [0036], [0080]. A 2013 study by the Federal Reserve confirmed the prevalence of magnetic stripe transactions, estimating that only 74 out of every 100,000 card-present credit card transactions were initiated with a chip while the remainder were initiated with a traditional swipe of a magnetic stripe. *Study Summary (Ex.1036),* 17.

229. Further, at the time it was well-known that many point-of-sale terminals still ***only*** accepted a physical magstripe payment method. The same 2013 Federal Reserve study noted that chip cards and chip terminals were "not widely adopted" though their availability was "growing." *Study (Ex.1037)*, 63 n.46. Notably, in a further survey reported in December 2015, it was reported that three-quarters of the major retailers surveyed had installed checkout terminals able to read smart cards, but had not yet enabled the terminals to accept chip payments, meaning swipers were still required to swipe their card's magnetic strip to make a payment. *ConsumerWorld Survey (Ex.1038)*. A POSITA therefore would have been motivated to modify Collinge's payment system to take advantage of Collinge's more secure payment system while also having the flexibility to make payments on point-of-sale terminals that only accepted magstripe transactions.

230. A POSITA would have understood that, at that time "existing contactless transaction enabled cell phones cannot be used for magnetic stripe transactions, which is the dominant technology presently in use." *See Bona (Ex.1009),* [0109]. A POSITA would have understood that Collinge's mobile phone does not have a physical magstripe that is able to be swiped in a reader, and therefore Collinge's mobile phone would not be suitable for performing magnetic stripe transactions where only a physical reader is available. A POSITA would have

understood that providing the user with both payment options would expand the number of POS terminals where Collinge's payment credentials could be used, and provide the user with additional payment options if an NFC-enabled point-of-sale terminal was broken, not enabled, or not present.

231. A POSITA would have recognized that given the state of point-of-sale terminals at the time, a user would have found it valuable to have access to a variety of methods for completing a payment transaction. In addition, a user of Collinge's payment system would have benefited from having back-up payment options in the event that point-of-sale equipment (such as an NFC-enabled point of sale terminal) was broken, mobile payment features of the terminal were not enabled by the merchant, or a merchant was only able to accept magnetic stripe payments. A POSITA would have been motivated to combine Collinge with Brown to allow the flexibility to make contactless payments using Collinge's payment application on Collinge's cell phone, and also make payments at point-of-sale terminals that still only accepted a physical swipe of a magstripe card.

232. A POSITA would have had a reasonable expectation of success in combining Brown's smart card with Collinge's payment system as a combination of known elements (e.g., a mobile device with a mobile payment application and a payment card device with a variable display), would have recognized that in the

combined system, the functionality of Collinge and Brown would not change, and would have predictably created a system that provides a user with access to a greater variety of payment methods.

233. A POSITA considering what payment cards would be compatible with Collinge's payment system would also have been motivated to look to Brown's payment card because both were designed with reference to the same well-known industry standards. *Brown (Ex.1010),* [0110] (discussing ISO/IEC/IEC Specifications), [0173] (discussing the format of a PAN on a typical credic card, including MasterCard specific numbers); '*095 Provisional (Ex.1005),* [0064] ("Track 2 Data (DE 35) comprises information encoded on track 2 of a payment card's magnetic stripe as defined in ISO 7813" and "Track 1 Data (DE 45) includes information encoded on track 1 of a bankcard's magnetic stripe as defined in ISO 7813."). ISO/IEC 7813 is an international standard that defines the structure and content of magnetic tracks 1 and 2 on financial transaction cards. *See MagTek (Ex.1022)*.

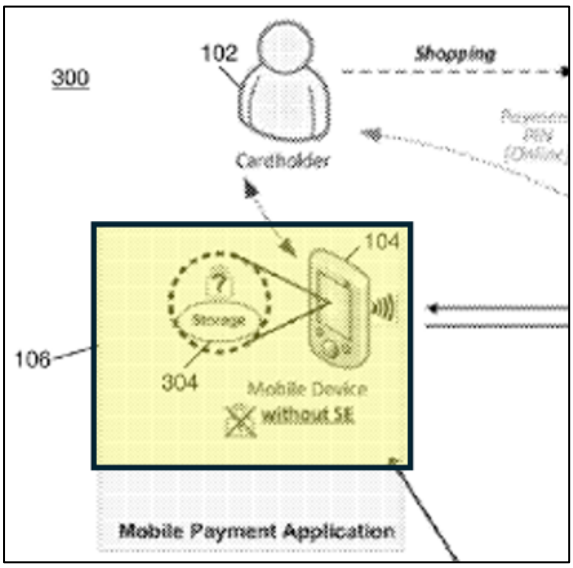
234. In the combination, Brown's payment card would be assigned a VPAN, just like any other payment card registered in Collinge's payment system. *See* Claim 11(pre).

C. 11(c): a processor;

235. Collinge's mobile device includes "an application program stored in data storage of the mobile device" that is "executed by *a processor* included in the mobile device[.]" *Collinge (Ex.1004),* [0041] (emphasis added), [0147] ("at least one processor device… may be used to implement the above described embodiments"). Collinge teaches and a POSITA would have found it obvious that Collinge's mobile device 104 would be implemented as the computer system 1900 as discussed at claim 11(g).

D. 11(d): a memory;

236. Collinge's mobile device includes *a memory* for storing a payment card information accessible to the processor. Collinge teaches "an application program stored in **data storage** of the mobile device and executed by a processor included in the mobile device 104." *Collinge (Ex.1004),* [0041], [0147] ("at least one processor device and *a memory*") (emphasis added). Collinge's memory includes storage 304, which may include a "local encrypted database." *Collinge (Ex.1004),* [0067], [0147]. Storage 304 stores "received payment credentials[.]" *Collinge (Ex.1004),* [0063], [0048]-[0049] (describing payment credentials contents).



Collinge (Ex.1004), Fig. 3 (annotated excerpt).

E. 11(e): a wireless interface;

237. Collinge's mobile device includes a *wireless interface* (NFC interface). Collinge's mobile device can "conduct payment transactions via near field communication[.]" *Collinge (Ex.1004),* [0041]. Collinge repeatedly recognizes that a POSITA would have been familiar with methods for performing contactless payments via NFC technology. *Collinge (Ex.1004),* [0044] ("Suitable methods and protocols for the secure transmission of information via NFC will be apparent to persons having skill in the relevant art."). [0070] ("Methods for transmitting payment credentials and a payment cryptogram to a point-of-sale terminal 120 via NFC will be apparent to persons having skill in the relevant art."); [0120] ("Methods for executing transmission of payment credentials from a mobile device to a point-of-sale terminal will be apparent to persons having skill in the relevant art.").

238. A POSITA would have understood that "Near Field Communications (NFC) is a short-range wireless technology that allows mobile devices to actively interact with passive physical objects and other active mobile devices, connecting the physical world to mobile services in ways that empower and benefit users." *Cavoukian (Ex.1039),* 1. NFC is an open platform technology. *Paus (Ex.1040),* 3. A POSITA at the time would have been familiar with NFC communication and methods of executing standard NFC payment transactions, including those set out in ISO/IEC 18092:2013 and ECMA-340 (Near Field Communication – Interface and Protocol (NFCIP-1), 2nd Edition, December 2004. *Id.* These standards specify capabilities such as transfer speeds, bit encoding schemes, modulation, frame architecture, and transport protocol, as well as operating modes, and provide the information necessary for a POSITA to implement NFC communication on a mobile device. *Id.*

239. A POSITA would have understood that Collinge teaches that mobile phone 104 has an NFC interface that allows Collinge's mobile phone 104 to "conduct payment transactions via near field communication[.]" *Collinge (Ex.1004),* [0041]. It was well known that an NFC interface is the combination of hardware and software that enables an NFC-enabled device to communicate with another NFC-enabled device over a short distance (typically less than 4 cm). For example, it was

known that communication using an NFC device "may occur within a range of approximately 2 to 4 cm." *Lin (Ex.1045),* 19:26-27.

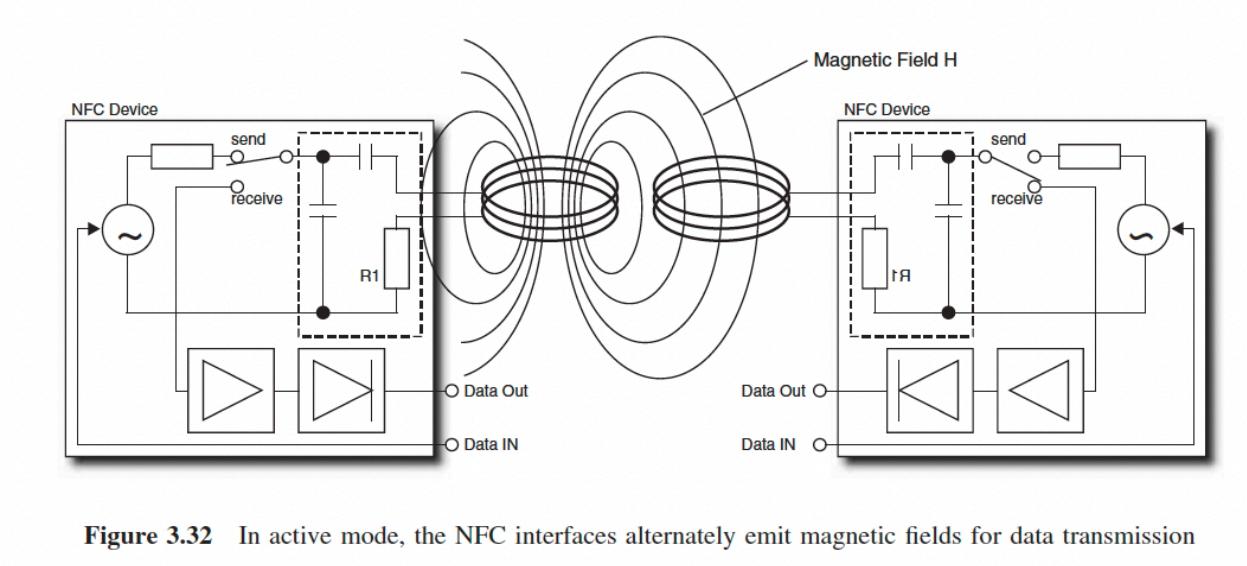


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (Ex.1024), 58.

240. Collinge teaches an NFC interface, as shown in Fig. 1 below. In addition, a POSITA would recognize that an NFC interface is necessarily present in Collinge's mobile device 104 because an NFC interface is required to "conduct payment transactions via near field communication[.]" *Collinge (Ex.1004),* [0041]; *'248 Provisional (Ex.1005),* [0067] (**NFC interface of the mobile device 104**…"), [0184]; Accordingly, a POSITA would have understood that Collinge teaches that mobile device 104 has an NFC interface that allows it to communicate with other NFC-enabled devices.

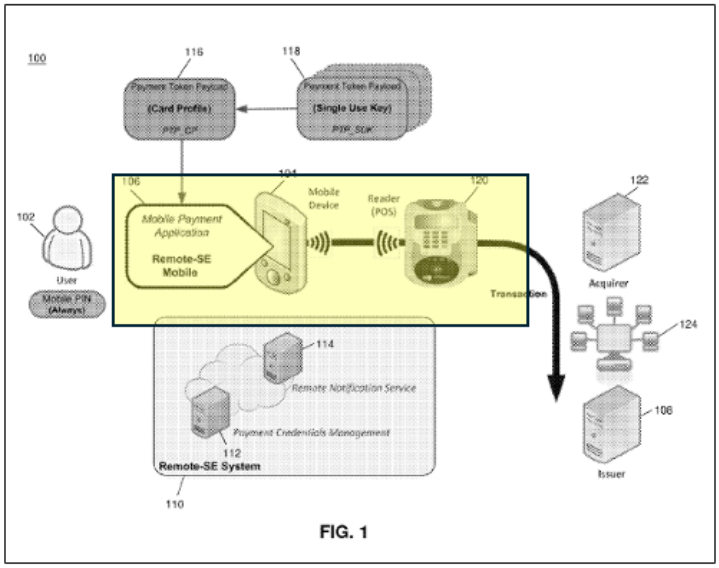


FIG. 1

Collinge (Ex.1004), Fig. 1 (annotated excerpt).

241. In addition, a POSITA would have understood that an NFC interface is a *wireless interface*. Near-field communication is "short-range wireless technology[.]" *Cavoukian (Ex.1039),* 1. NFC-enabled devices are able to communicate with other NFC-enabled devices over a short distance (typically less than 10 cm). *Paus (Ex.1040),* 5. Further, the processor of Collinge's mobile device is connected to a network, such as "a wireless network (e.g., WiFi), a mobile communication network, a satellite network, [or] the Internet[.]" *Collinge (Ex.1004),* [0150]. A POSITA would have understood that these are further teachings of a *wireless interface* of Collinge's mobile device because WiFi, the internet, mobile

communications networks (2G, 3G, etc.), and satellite networks are all wireless networks.

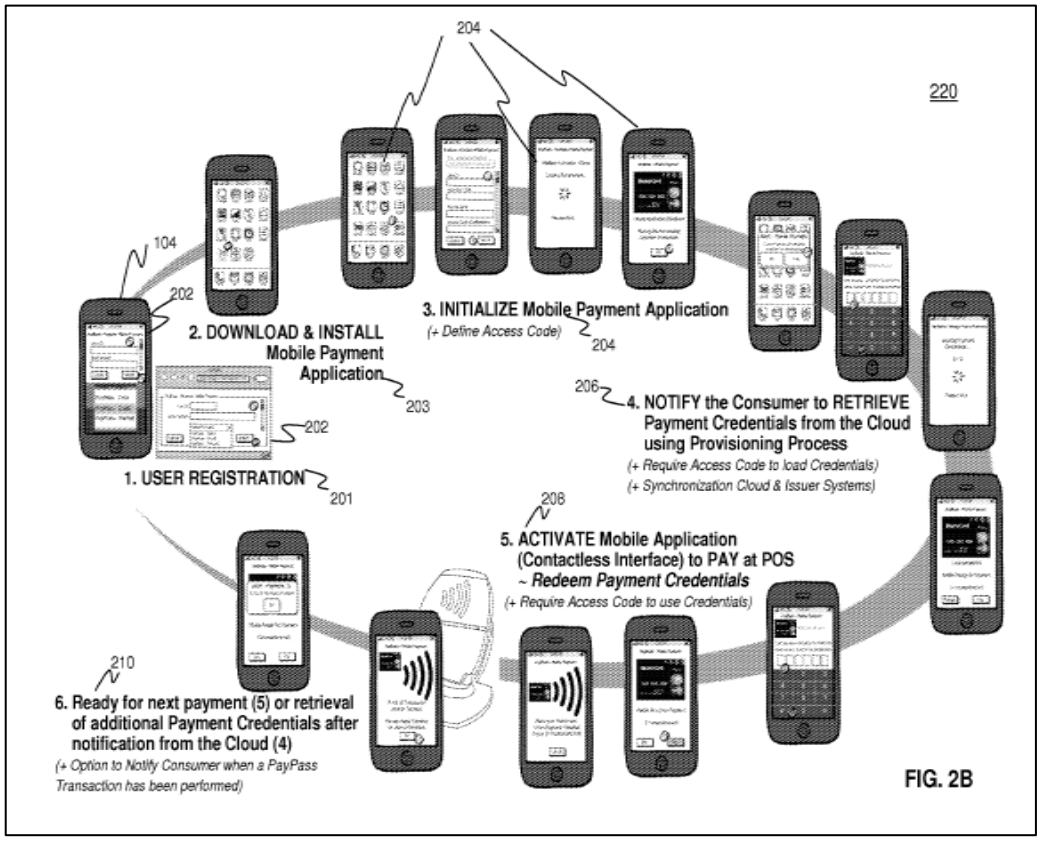
F. 11(f): a display operable to provide a visual user-interface operable for performing online transactions; and

1. Collinge's Teachings

242. Collinge's mobile device includes a touch-screen *display* which is a *visual user-interface*. *Collinge (Ex.1004),* [0133] ("a touch screen" of "the mobile device 104"). Collinge teaches that "a touch screen" of "the mobile device 104" provides a visual user-interface for user payment interactions. *Collinge (Ex.1004),* [0133]. For example, Collinge's touch screen receives a user's input of a "mobile personal identification number (PIN)" prior to generation of a payment cryptogram. *Collinge (Ex.1004),* [0133].

243. A POSITA would have understood that Collinge's touch screen (i.e., user-input device) would have physical hardware components and software components (e.g., a visual GUI component). *Mahapatra (Ex.1041)*, 37 ("[a] basic touch screen…is made up of 3 basic elements, a sensor, a controller and a software driver."). A POSITA would have understood that Collinge's touch screen includes a visual GUI component (for example, the GUI depicted in *'248 Provisional (Ex.1006),* Fig. 2B below) that corresponds to the claimed "touch-screen user interface."

244. Collinge's '248 Provisional application (which I understand is incorporated by reference into Collinge) provides further examples of user interaction with the touch screen during the user registration and payment process. In the below image, Collinge teaches that the user interacts with the user-interface on the touch screen of the device to download and install the mobile payment application, input access codes (e.g., PIN numbers), and make payment selections, for example:



'248 Provisional (Ex.1006), Fig. 2B.

2. Kranzley

245. Kranzley teaches that the payment application may display the payment information required for an online transaction, and the customer "may read the information from the display device and then key in that data into a Web page on a computer[.] *Kranzley,* [0040]. Kranzley's display of online-usable payment information is a *visual user-interface operable for performing online transactions*. Further, a POSITA would have understood that a mobile device (e.g., a smart phone) is a computer—a programable electronic device that stores, processes, and retrieves data. Ex.1016 (a computer is "a programmable electronic device that can store, retrieve and process data"). Therefore a POSITA would have understood (and it would have been obvious that) Kranzley teaches entering payment data into a Web page on the display of Kranzley's mobile device. *Kranzley,* [0040] ("key in that data into a Web page on a computer." Notably, the display of Kranzley's mobile device is likewise a *visual user-interface operable for performing online transactions*, as Kranzley explicitly teaches causing "the payment application in the mobile device to display a VPAN, expiration date and dynamic account validation code on a display device of the mobile device 102" so that a user can "key in that data into a Web page[.]"

3. Motivation to Combine

246. As discussed above at 11(pre), in combination with Kranzley, Collinge's display would be *operable for performing online transactions*. In the combination, the touch-screen display of Collinge's mobile device would continue to be used by the user to select the payment method for the POS transaction and enter an authentication PIN. *Collinge (Ex.1004),* [0038] ("[p]ayment cards may include credit cards, debit cards…"); *'248 Provisional (Ex.1008),* 96 (showing selection of Debit, Credit, or Prepaid) on Collinge's touch screen display; *'248 Provisional (Ex.1006),* Fig. 2A-2B (same); *Collinge (Ex.1004),* [0133] (touch screen receives a mobile PIN). Further, it would have been obvious and a POSITA would have been motivated to display payment credentials on Collinge's screen so that a user can input those credentials into a Web page on the display of Collinge's mobile device and complete an online transaction. *See* 11(pre).

G. 11(g): a user-interface coupled to the processor, and

247. I understand that Collinge teaches the touch-screen display (*user-interface*) of Collinge's mobile device is *coupled to* Collinge's mobile device's *processor*. Collinge teaches that "at least one processor device" is used to implement the payment system taught by Collinge. *Collinge (Ex.1004),* [0147]. The touch screen of Collinge's mobile device 104 is *coupled to the processor* so that user input can be received and acted upon by mobile device 104. For example, the touch screen

"receives a user's input of a "mobile personal identification number (PIN)" during generation of a payment cryptogram. *Collinge (Ex.1004),* [0133]. Collinge teaches and a POSITA would have understood that for the touch screen in Collinge's mobile device 104 to display information and receive and act on user input as taught by Collinge, the touch screen must be coupled to a processor. *Collinge (Ex.1004),* [0147].

248. Collinge's payment system comprises a display interface and display that is "coupled" to the processor via the communication interface:

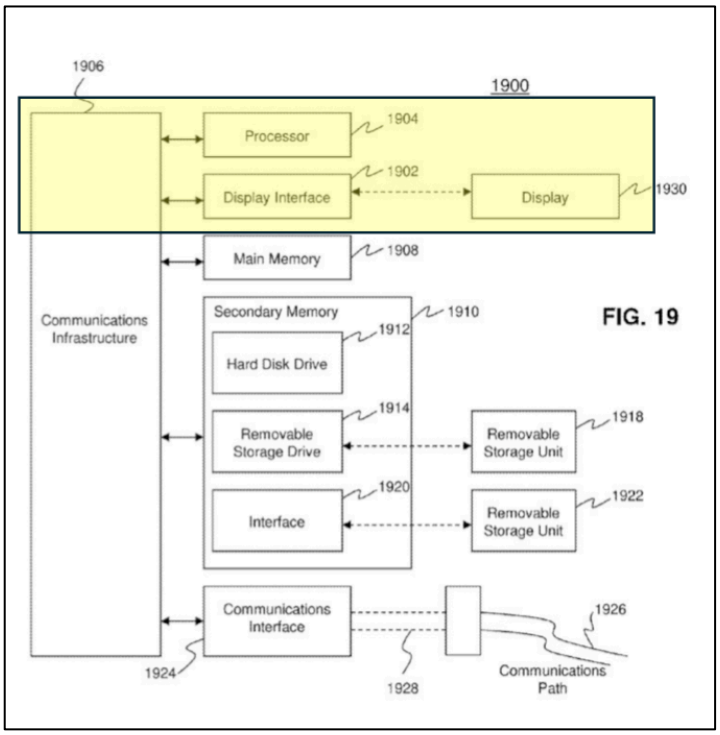
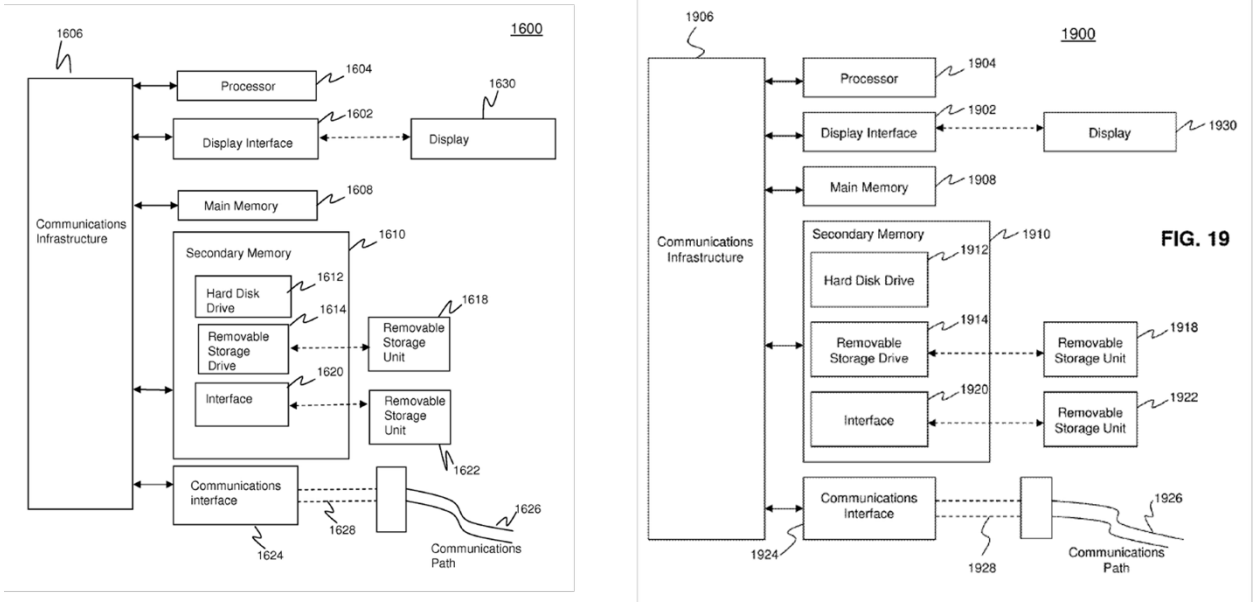


FIG. 19

Collinge (Ex.1004), Fig. 19 (annotated). *Collinge (Ex.1004),* [0150] (the communications infrastructure may be a "bus, message queue, network, multi-core message-passing scheme, etc.").

249. A POSITA would have understood or found obvious that Collinge's mobile device 104 would be implemented as the computer system 1900. For example, in the '248 Provisional (Ex.1006), which I understand is incorporated by reference into Collinge, the computer system of Figure 16 (which corresponds to Figure 19 in Collinge) is taught as corresponding to the mobile device.



'248 Provisional (Ex.1006) at Figure 16 (left); *Collinge* at Figure 19 (right). Specifically, the '248 Provisional (Ex.1006), regarding Figure 16, teaches "the computer programs, when executed, enable the processor 1604 to implement the processes of the present disclosure, such as the methods illustrated by Figures 2A and

2B[.]" *'248 Provisional (Ex.1006)* at [0246] (emphasis added). Figures 2A and 2B are "storyboards depicting provisioning processes for downloading, installing, provisioning, activation and using a mobile payment application with a mobile computing device[.]" *'248 Provisional (Ex.1006)* at [0017]. Further, Figures 2A and 2B are expressly taught as being carried out by "mobile device 104[.]" *'248 Provisional (Ex.1006)* at [0048].

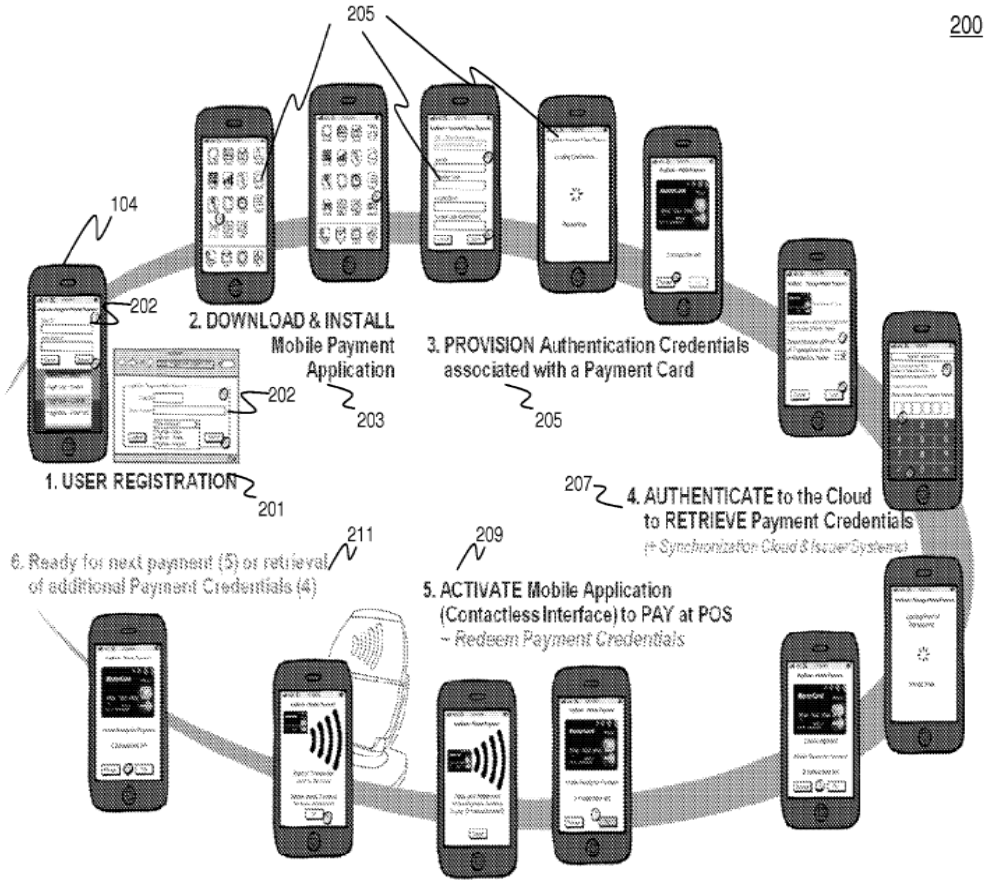


FIG. 2A

'248 Provisional (Ex.1006) at Figure 2A. Because Figure 16 of the '248 Provisional (Ex.1006) corresponds to Figure 19 of Collinge, and because the processor 1604 is taught as implementing the methods of Figures 2A and 2B, which are done by mobile device 104, a POSITA would have understood that processor 1904 in Figure 19 of Collinge is that of mobile device 104. In other words, because processor 1604/1904 in the '248 Provisional (Ex.1006) implements computer programs on mobile device 104, a POSITA would understand that Figure 19 of Collinge represents mobile device 104 (the *electronic device*).

250. It was well known that displays and processors are coupled in mobile devices. As one example, U.S. Patent Appl. No. 2006/0097991 to Hotelling et. al. ("Hotelling") teaches that "[t]he computer system 50 also includes a touch screen70 that is operatively coupled to the processor 56." *Hotelling (Ex.1042),* [0052].

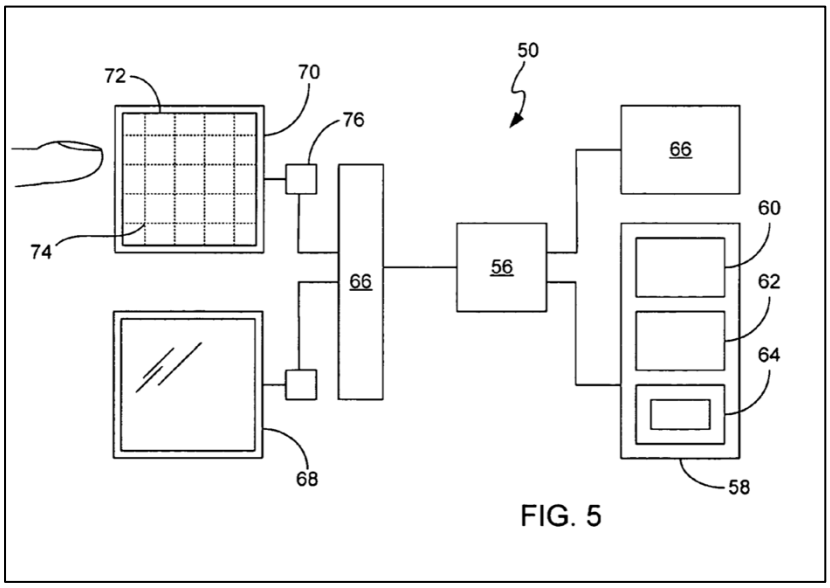


FIG. 5

Hotelling (Ex.1042), Fig. 5. Hotelling teaches that "[t]he touch screen also includes a sensing circuit that acquires data from the sensing device and that supplies the acquired data to the processor." *Hotelling (Ex.1042),* [0013]. The sensing device detects "multiple touches or near touches[.]" *Hotelling (Ex.1042),* Abstract.

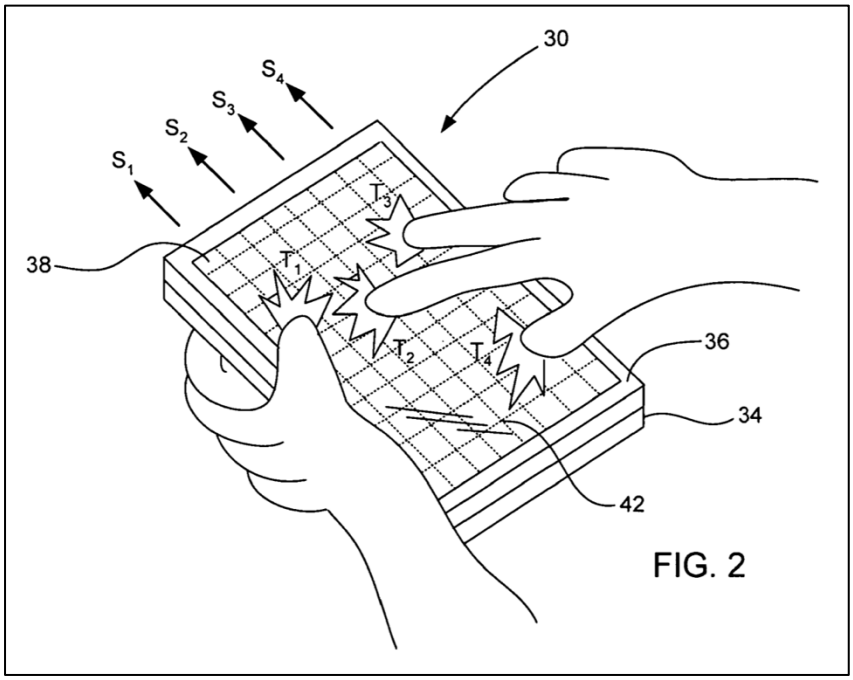


FIG. 2

Hotelling (Ex.1042), Fig. 2.

251. As another example, Jobs describes "peripherals interface 118 couples the input and output peripherals of the device to the CPU 120 and memory 102. The one or more processors 120 run or execute various software programs and/or sets of instructions stored in memory 102 to perform various functions for the device 100 and to process data." *Jobs (Ex.1043),* [0098]

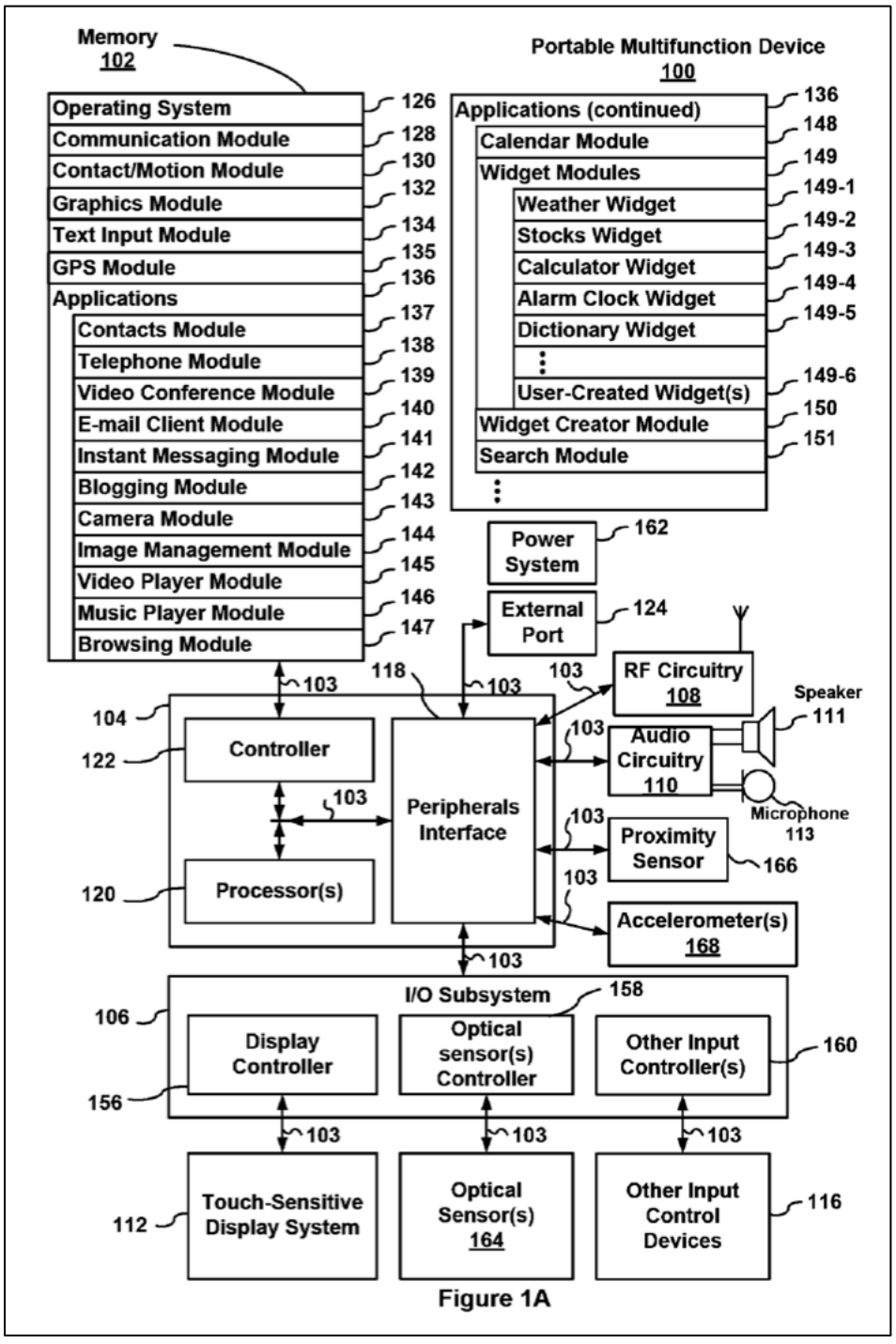


Figure 1A

Jobs (Ex.1043), Fig. 1A.

252. A POSITA would have understood that Collinge teaches a touch screen coupled to a processor because Collinge teaches that its touch screen is operable to provide a visual user-interface and accept and act on user input received at the touch screen. *Collinge (Ex.1004),* [0133] ("an input device (e.g., of the mobile device 104, such as a touch screen) may receive a mobile personal identification number (PIN) input by a user (e.g., the user 102) of the mobile device 104.") A POSITA would have understood that for the touch screen in Collinge's mobile device 104 to operate as described by Collinge, the touch screen must necessarily be coupled to a processor, similar to Hotelling. Therefore, a POSITA would have understood that for the touch screen in Collinge's mobile device 104 to operate as described by Collinge, the touch screen must necessarily be coupled to a processor.

H. 11(h): wherein the wireless interface is operable to wirelessly obtain card device payment account information, and

253. Collinge and Kranzley both teach that card device payment account information is *wirelessly obtained*.

254. Collinge teaches "the payment token payload [is] provisioned to the mobile device 104[.]" *Collinge (Ex.1004),* [0047]. The payload includes a "card profile 116 and the single use key 118" and the card profile 116 further includes "payment credentials provisioned to the mobile payment application 106 by the remote-SE system for use in conducting payment transactions." *Collinge (Ex.1004),*

[0048], [0150] (Collinge's mobile device is connected to a network, such as "a wireless network (e.g., WiFi), a mobile communication network, a satellite network, [or] the Internet[.]"). Collinge teaches and a POSITA would have found it obvious that when Collinge receives payment credentials from the remote-SE system, they are received *wirelessly*, (including because Collinge's mobile device would have been connected to wireless networks, as discussed above 11(e)) however, Collinge does not specify which wireless method is used.

255. Kranzley (like Collinge) teaches that to use the payment application on Kranzley's mobile device "a cardholder must first register a payment card" and "install (or activate a payment application on a mobile device[.]" *Kranzley,* [0050]. During registration, "the payment provider 110 creates a VPAN" and "delivers the VPAN to the cardholder's mobile device…**using over the air ('OTA') techniques."** *Kranzley,* [0054]. A POSITA would have been familiar with "OTA" or "Over the Air" techniques, which provides for the wireless delivery of software, firmware, or other data to mobile devices such as over WiFi or a cellular network. *Fjellheim (Ex.1035)* (discussing techniques for "Over-the-air (OTA) delivery of applications" to "enable[] easy deployment and upgrades to applications" and reduce "the disrupting effect which installations may have on mobile users.").

256. It would have been obvious and a POSITA would have been motivated to send card device payment account information (including a VPAN and CVC associated with Brown's card), to Collinge's mobile device wirelessly over WiFi or a cellular network as taught by Collinge and Kranzley. A POSITA would have recognized that for Collinge's mobile device to function as a ***mobile*** device, it must not be required to connect to wires to function (make phone calls, etc), but rather must have a wireless communication interface. It was well-known that mobile devices at the time could connect to WiFi and cellular networks through wireless connections. A POSITA would have had a reasonable chance of success in using the known methods of WiFi or a cellular network to provision payment credentials to Collinge's mobile device as taught by Kranzley, particularly since that was the common way for mobile devices to receive information already.

I. 11(i): wherein the processor is operable to generate limited-use payment information based on the card device payment account information, and

Collinge teaches a processor operable to dynamically *generate limited-use payment information* (a payment cryptogram).

In the Collinge-Brown combination, Collinge's mobile payment application is provisioned with payment credentials (including a VPAN and CVC3) associated

with Brown's card (*see* Claim 11(pre)) and Collinge generates limited-use payment information based on Brown's *payment account information*.

1. Brown

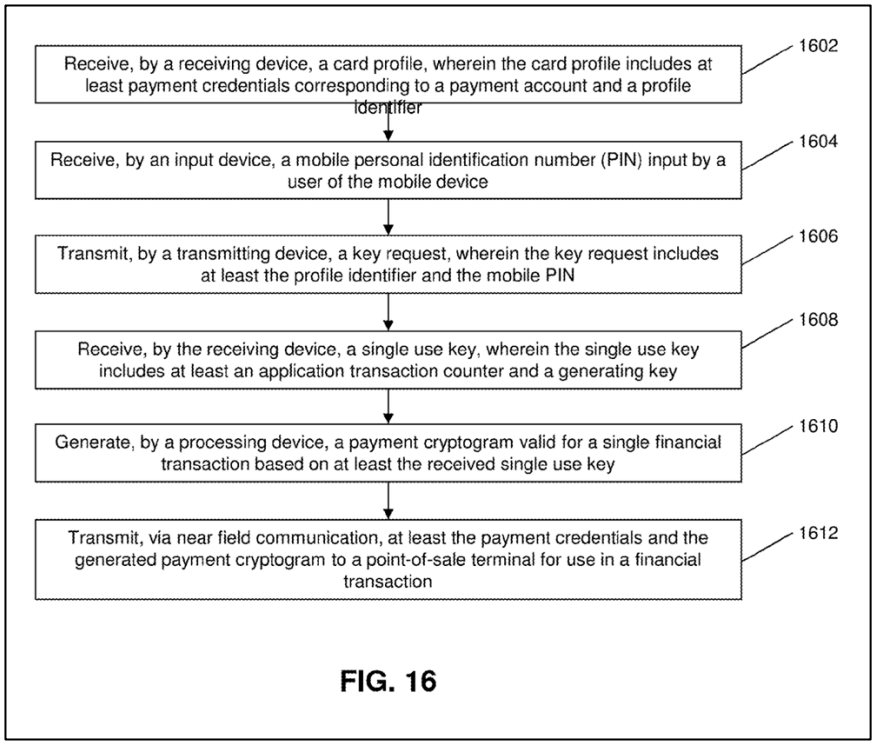
Brown teaches "use of a card-holders real personal account number (PAN) such that an issuing bank can authorize all transactions without support from a third party." *Brown (Ex.1010),* [0040]. Brown further teaches that the PAN will be assigned an "expiration date." *Id.* Brown teaches that "account numbers" and "expiration dates" are assigned before the user receives their card. *Brown (Ex.1010),* [0048], [0052]-[0053]. While embodiments of Brown discuss a variable payment account number displayed on Brown's card, as discussed above at claim 11(pre), Brown teaches and a POSITA would understand that those virtual account numbers must be correlated to the user's assigned real personal account number for payment to be processed. *Brown (Ex.1010),* [0040]. The purpose of a virtual account number is to serve as a stand-in for "real" account information, such as an issuer PAN, and (as taught by Kranzley (*Ex.1013*), Grigg (*Ex.1047*) and many other VPAN references at the time, when a VPAN is used for payment it will be correlated during payment processing with a payment account from which the payment amount will ultimately be deducted *Kranzley* (*Ex.1013*) at [0011] ("After the secured account number is received by the server computer, the real account number is determined"),

[0026], [0039]; *Grigg* (*Ex.1047*) at Fig. 4, [0083]-[0084]. A CVC is also assigned to each payment account. *Brown (Ex.1010),* [0177]

2. Collinge

257. Collinge's mobile payment application is "stored in data storage of the mobile device 104 and **executed by a processor** included in the mobile device 104." *Collinge (Ex.1004),* [0041].

258. The processor executing the mobile payment application of Collinge's mobile device generates a **payment cryptogram** which "may be, for example, an application cryptogram or a dynamic card validation code (CVC3)." *Collinge (Ex.1004),* [0077]. Collinge teaches the payment cryptogram is single-use, "valid for a single financial transaction." *Collinge (Ex.1004),* [Abstract], [0128], Fig. 16. The payment cryptogram is generated "using the generating key included in the single use key" that was previously provisioned to the mobile device. *Collinge (Ex.1004),* [0077], [0043]. Collinge teaches generating a CVC3 based on: "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge (Ex.1004),* [0145].



Collinge (Ex.1004), Fig. 16.

3. Motivation to Combine

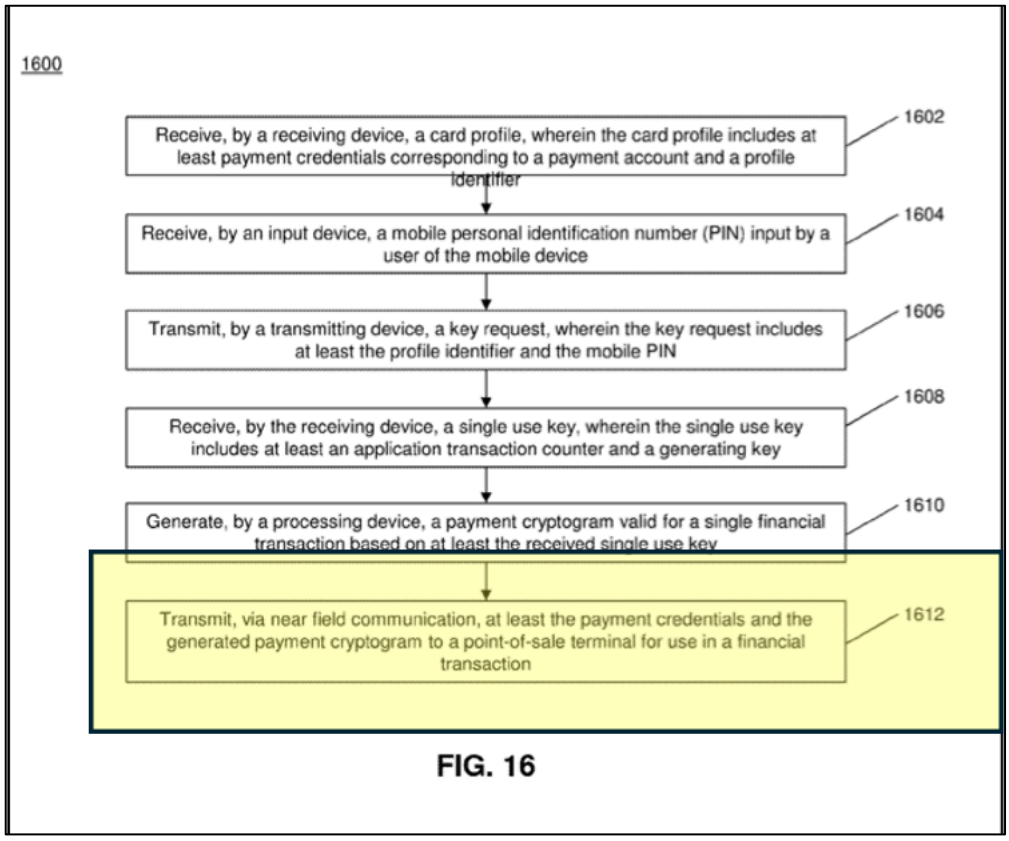
259. *See* claim 11(pre), (a).

J. 11(j): wherein the personal computing device is operable to generate complete payment information, including the limited-use payment information, and to convey said complete payment information via at least one interface of a set comprising: said display; and the wireless interface, and

260. Collinge teaches generating *complete payment information* and Collinge in light of Kranzley further teaches conveying the complete payment information via Collinge's *display*.

261. Collinge teaches generating *limited-use payment information* (a payment cryptogram). *See* Claim 11(i). Collinge further teaches sending the

dynamically generated payment cryptogram combined with payment credentials (which includes a Payment Account Number (PAN) or VPAN) to a point-of-sale terminal in a payment transaction. *Collinge (Ex.1004),* [0048]-[0049], [0070], [0077], [0135], Fig. 16. The payment cryptogram and payment credentials are *complete payment information* because they include the information required to process payment.



Collinge (Ex.1004), Fig. 16. (annotated), [0048], Fig. 6, [0104] (card profile (PTP_CP)); *'248 Provisional (Ex.1008),* [0101] ("Payment Token Payload – Card Profile (PTP_CP_ contains the Payment Credentials required to perform a

[MasterCard] *PayPass* transaction" including "data elements such as: **PAN,** PSN + Track Data.").

262. As discussed above at Claim 11(pre), it would have been obvious and a POSITA would have been motivated to convey complete payment information on Collinge's display, including (in the combination) a VPAN and a dynamic CVC (payment cryptogram).

K. 11(k): wherein the limited-use payment information is configured to be used in place of a card issuer payment information.

263. Collinge teaches that the payment cryptogram (*limited-use* payment information) is a "dynamic card validation code (CVC3)" that is used in place of a static card CVC, which, in the combination, is the CVC assigned to Brown's payment card by the card issuer. *Collinge (Ex.1004),* [0050], [0077]. *See* Claim 11(a).

L. Claim 13(a): The system of claim 11 wherein the personal computing device is configured for presenting on the display a limited-use card security code number for use in payments in place of card issuer payment information, and

264. Collinge teaches generating a *limited-use card security code number* (payment cryptogram) used in place of a card-issuer provided static CVC. *See* Claim 11k.

265. In related art, Kranzley teaches a "**dynamic code** is a three or four digit code that may be used **in place of a "CVV", "CVC"** or other code (a code generally

used in payment card systems and used to verify that a cardholder was in possession of a payment card during a transaction).” *Kranzley*, [0041] (emphasis added). Kranzley teaches this “dynamic code **is displayed on the display device**.” *Kranzley*, [0011], [0040] (teaching displaying the code for use in online transactions).

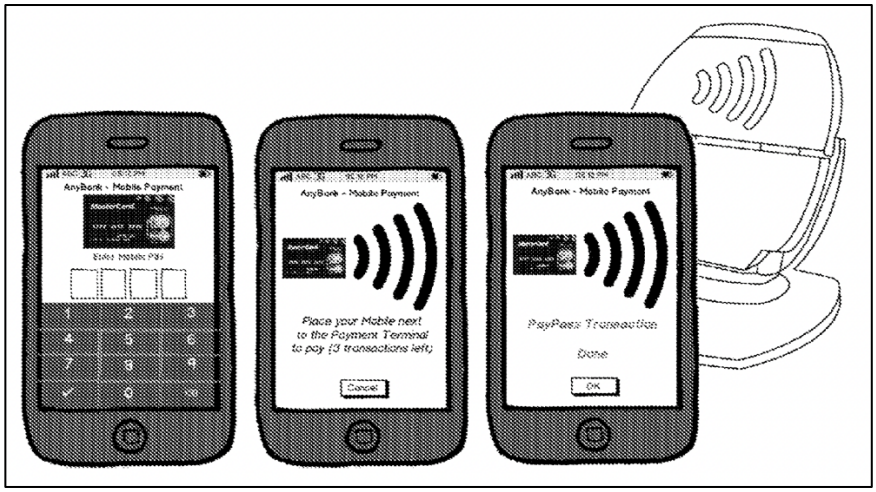
266. It would have been obvious and a POSITA would have been motivated to modify Collinge’s mobile payment application to display Collinge’s payment cryptogram on Collinge’s display as taught by Kranzley for the reasons discussed at Claim 11(pre). A POSITA would have recognized a user’s desire for flexibility to make payments online, and that many online transactions required a CVC-type value to be provided, as taught by Kranzley. *Kranzley,* [0011], [0040] (requiring a “dynamic account validation code” on the webpage).

M. 13(b): wherein the personal computing device is further configured to generate said limited-use card security code responsive to an input request from a valid user, via said user-interface, and

267. Collinge teaches that the touch screen of mobile device 104 receives a user’s input of a “mobile personal identification number (PIN)” (*input request*) to kick-off the process of a payment cryptogram and to validate the user. *Collinge*, [0128], [0133]. The payment cryptogram is “based on…the mobile PIN” and is therefore generated responsive to input of an accurate mobile PIN by the user.

Collinge (Ex.1004), [0135]; *'248 Provisional (Ex.1006),* Fig. 2B ("Request Access Code to use credentials").

268. Collinge teaches that user "must always provide the Mobile PIN for all PayPass transactions[.]" *'248 Provisional (Ex.1008),* 99.



'098 Provisional (Ex.1008), 99; *'248 Provisional (Ex.1006),* Fig. 2B.

N. 13(c): wherein said limited-use number is generated on the personal computing device from at least one information from a set comprising: a payment device user information; a payment device account number; a payment device sequence counter; a payment device identifier; payment device secrets; a payment device key; computing device secrets; computing device keys; payment device issuer secrets; payment device issuer keys; a time; an expiration date; an amount; a merchant locality; an online location; a transaction information; and a cryptographic combination of at least two of the above.[3]

269. Collinge's mobile device generates a payment cryptogram (CVC3) using the single use key [*computing device key/computing device secret*]. *Collinge (Ex.1004)*, [0050]. More specifically, Collinge's CVC3 is generated based on at least "the supplied CVC3 value [a payment card security code/*payment device secret*], the session key unpredictable number [*computing device secret*], the application transaction counter [*a payment device sequence counter*], and the reader unpredictable number." *Collinge (Ex.1004),* [0145].

> The Mobile Payment Application use a specific process to generate the CVC3 using (KS_{UN}, $Cloud\_CVC3_{TRACK1/2}$, ATC and UN_{READER})

[3] I note that the specification of the '820 Patent does not use many of these terms outside of the claim language of Claim 13 – including, for example "payment device key," "computing device key," and "payment device issuer key."

'248 Provisional (Ex.1006), Table 1. Collinge teaches that the payment cryptogram is generated by cryptographically combining information. *Id.; Collinge (Ex.1004),* [0145]. Moreover, the very nature of a "cryptogram" is in the name – it is a product of cryptography. *See* above at VII.C.2.

O. Claim 14(a): The system as described in claim 11 wherein the personal computing device is configured for presenting on the display, a limited-use card account number, and a limited-duration expiration date, for use in payments in place of a card issuer payment information, and

270. *See* Claim 11(pre); *Kranzley,* [0040] ("display a VPAN [*limited-use card account number*], *expiration date*, and dynamic account validation code").

P. 14(b): wherein said personal computing device is further configured to generate said limited-use card payment information responsive to an input request from a valid user, and

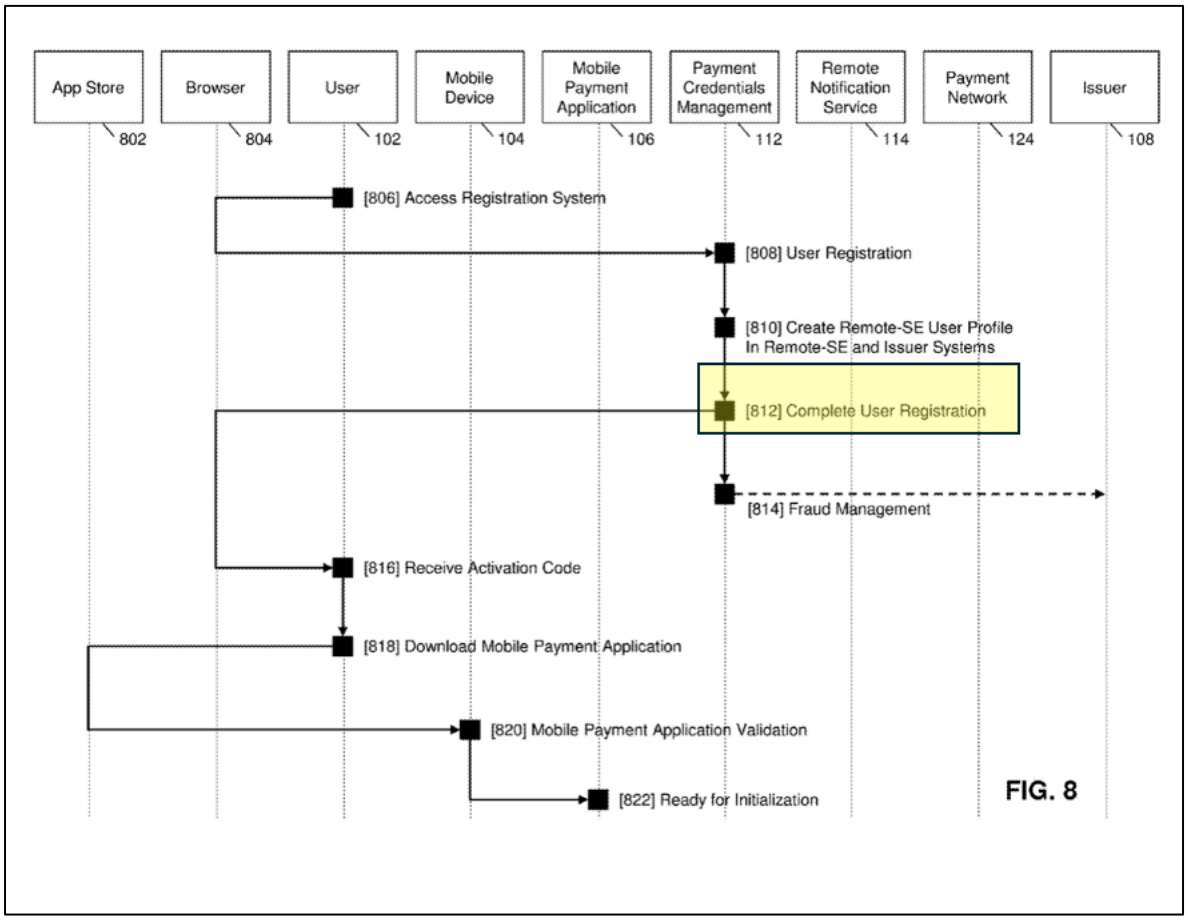
271. *See* Claim 13(b).

Q. 14(c): wherein the personal computing device is configured to identify a valid device-user through at least one user-validation input available to the personal computing device, of a set comprising: a touch ID sensor operable to identify the touch a valid user; a user entering of a valid passcode on a touch sensor-array; a user entering of a valid passcode on a key-pad; a user entering of a valid PIN or Key-Code on the user-interface[…]

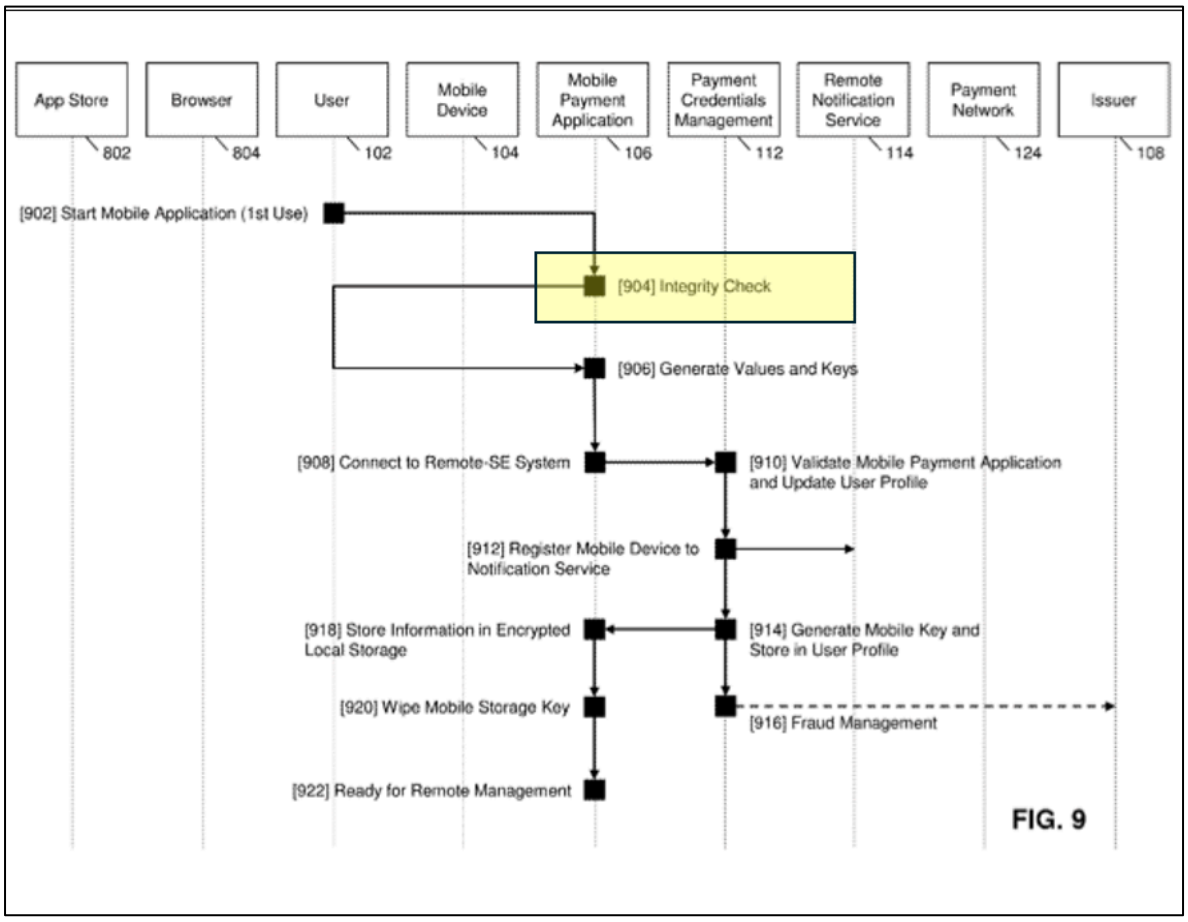
272. *See* Claim 13(b). Collinge teaches that in the registration process, the user "receive[s] an activation code and…**a unique identifier used to identify the user 102**." *Collinge (Ex.1004),* [0065] (emphasis added). When the mobile payment application is loaded, during an integrity check, "the mobile payment

application 106 may **authenticate the user 102 and request the activation code** provided to the user 102 during the registration process (e.g., at step 812 in FIG. 8)."

Collinge (Ex.1004), [0093] (emphasis added).

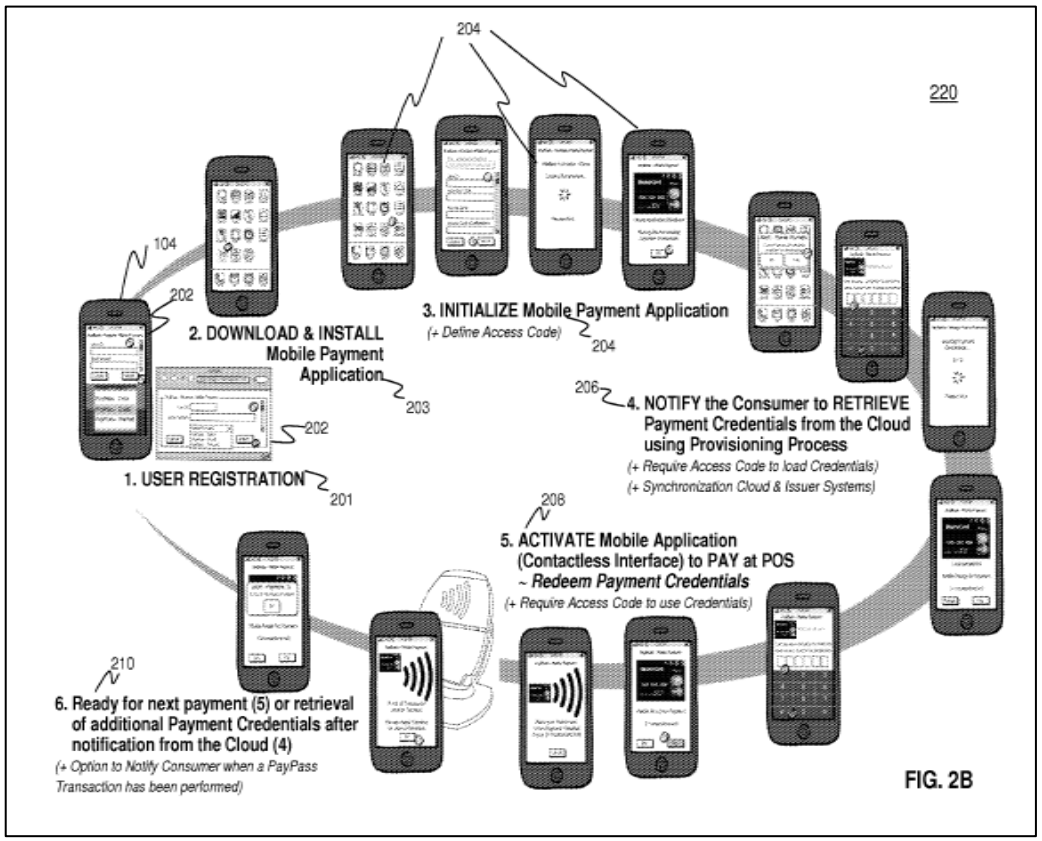


Collinge (Ex.1004), Fig. 8. (annotated)



Collinge (Ex.1004), Fig. 9 (annotated); [0130] (receipt of code is through touch screen input device).

273. Figure 2B (below) which Collinge incorporates by reference further describes a code used to identify a user. For example, in Step 4 the user must provide their access code in order to load payment credentials, and in Step 5 the user must provide an access code in order to use payment credentials—each time authenticating the user via input on the touchscreen user-interface.



'248 Provisional (Ex.1006), Fig. 2B.

R. 14(d) and wherein the personal computing device conveys the limited-use payment information through the user interface.

274. See Claim 14(a).

S. Claim 15(pre):An online payment system comprising:

275. See Claim 11(pre).

T. 15(a): a thin card-shaped payment card device that bears no fixed payment numbers on the card device; and

276. *See* Claim 11(a).

U. 15(b): a computing device operable for completing an online payment transaction and comprising:

277. See Claim 11(pre), (b).

V. 15(c): a display;

278. *See* Claim 11(f).

W. 15(d): a user-interface;

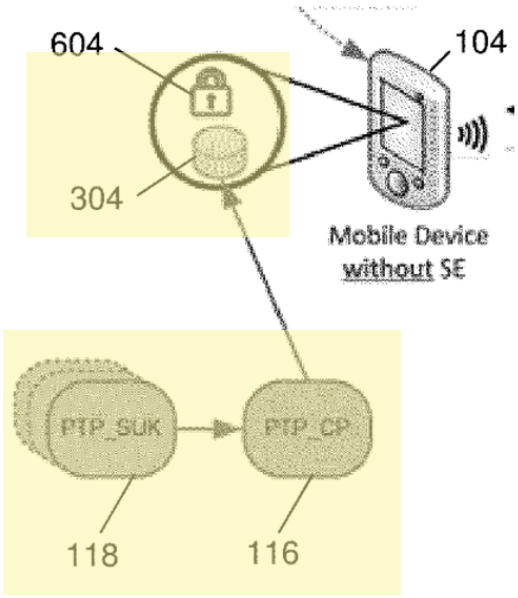
279. *See* Claim 11(g).

X. 15(e): a processor; and

280. *See* Claim 11(c).

Y. 15(f): a memory for storing a payment card information accessible to the processor,

281. *See* Claim 11(d). Collinge teaches storing *payment card information* in storage 304 *(a memory*). Specifically, Collinge teaches storing a card profile 116 (which "include[s] payment credentials") and a single use key 118 (including "generating key" to "generate a dynamic card validation code CVC3 or an application cryptogram (AC)") in storage 304. *Collinge (Ex.1004),* [0048]-[0049], Fig. 6.



Collinge (Ex.1004), Fig. 6 (excerpted, annotated).

Collinge's card profile 116 and single use key 118 are accessible to and used by Collinge's processor to generate and send complete payment information to an NFC terminal. *Collinge (Ex.1004),* [0048]-[0050], [0118]-[0120], Fig. 14.

Z. 15(g): wherein card issuer provided payment card information is wirelessly downloaded into the computing device, and

282. *See* Claim 11(h).

AA. 15(h): wherein at least one of the set comprising: the computing device; and the card-shaped payment device, is configured to dynamically generate a limited-use payment information, upon the authorization of a valid computing device user, and

283. *See* Claims 11(i), 14(c) (identifying a valid user).

BB. 15(i): wherein the payment information provided by the computing device is used in online transactions in place of a card issuers payment card information.

284. *See* Claim 11(k).

CC. Claim 17: The system of claim 15 wherein the dynamically generated limited-use payment information is displayable on a display of the computing device.

285. *See* Claim 14(a).

DD. Claim 18(a): The system of claim 15 wherein the limited-use payment information includes a static limited-use card account number, a limited-duration card expiration date, and a limited-use card security code and,

286. As discussed in Claim 11(i), the limited-use payment information generated by Collinge's mobile device includes a payment cryptogram (dynamic CVC3, a *limited-use card security code*). *Collinge (Ex.1004),* [0077]. Claim 11(i) further explains that Collinge generates complete limited use payment information which includes the payment cryptogram and payment credentials. Collinge's payment credentials include a payment account number (VPAN in the combination) and an expiration date. *Collinge (Ex.1004),* [0049], [0124] ("expiration date in the payment credentials included in the card profile 116,"); As I discuss in greater detail at VII.A.1, a POSITA would have understood that magstripe credentials include an expiration date. The VPAN is a *static limited-use card account number*. *Kranzley,* [0039] (describing a "static VPAN" with "an expiration date").

EE. 18(b): wherein the dynamically generated limited-use payment information is conveyed by the computing device to complete an online transaction.

287. In the combination, Collinge's limited-use payment information is conveyed to the user by the screen of Collinge's mobile device so that it can be used to complete an online transaction. *See* Claim 11(f). Further, Collinge's mobile device conveys the payment information when it is submitted to a webpage shown on Collinge's mobile device for payment. *Id.*

FF. Claim 19(a): The system of claim 15 wherein the computing device is operable to generate a limited-use card security code number, for use in place of a card issuers card security code by generating said limited-use number via cryptographically combining information from at least one of a set comprising: a user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; a transaction information; and a cryptographic combination of at least two of the above set,

288. *See* Claim 13(c). Collinge teaches generating a payment cryptogram such as a CVC3 based on at least Collinge's processor cryptographically combining: "the supplied CVC3 value [*payment card security code*], the session key unpredictable number [(KS_{UN}), *device secret/issuer secret*], the application transaction counter [*device sequence counter*], and the reader unpredictable number." *Collinge (Ex.1004),* [0145]. A POSITA would have understood that

cryptograms are created cryptographically as the name suggests, and as I discuss in greater detail above at VII.C.2 (e.g., discussing hash functions). A POSITA further would have understood that because Collinge's cryptogram is based on a several different inputs as discussed above, it is created by *cryptographically combining information*.

GG. 19(b): and wherein the computing device is operable to display the generated limited-use card security code on the display.

289. *See* Claim 13(a).

HH. Claim 20(a): The system of claim 15 wherein the computing device is further operable to obtain a user payment approval through at least one user-interface element of the computing device, from a set comprising…a display interface, a touch-screen interface…input buttons…

290. Collinge's device *touchscreen* user *interface* is operable to accept *a user approval* (selecting a pay option).

'248 Provisional (Ex.1008), 100; '248 Provisional (Ex.1006), Fig. 2B.

II. 20(b): wherein the computing device is operable to display at least one of a set comprising: the transaction information, the merchant information, the time, the location of the transaction, the payment bank logo, the card issuer icon, the payment card image, and the amount, on a display of the computing device, and,

291. Collinge teaches how to display a *payment card image,* including a MasterCard logo, on Collinge's mobile device.

'248 Provisional (Ex.1008), 100; *'248 Provisional (Ex.1006),* Fig. 2B. Collinge teaches that the payment card is displayed when the user is choosing the payment method to be used in the transaction, prior to the user selecting "pay" to complete the transaction. *Id.*

JJ. 20(c): a user input providing for at least one user action from a set comprising: an approving of a transaction, a denying of a transaction, and an adjusting of a transaction, via the user-interface.

292. Collinge's device touchscreen *user-interface* is operable to accept *a user approving* (selecting a "pay" option) or *denying* (selecting a "quit" option).

'248 Provisional (Ex.1008), 100; '248 Provisional (Ex.1006), Fig. 2B.

XV. GROUND 6: CLAIMS 12 AND 16 ARE OBVIOUS OVER COLLINGE, KRANZLEY, BROWN AND ENG

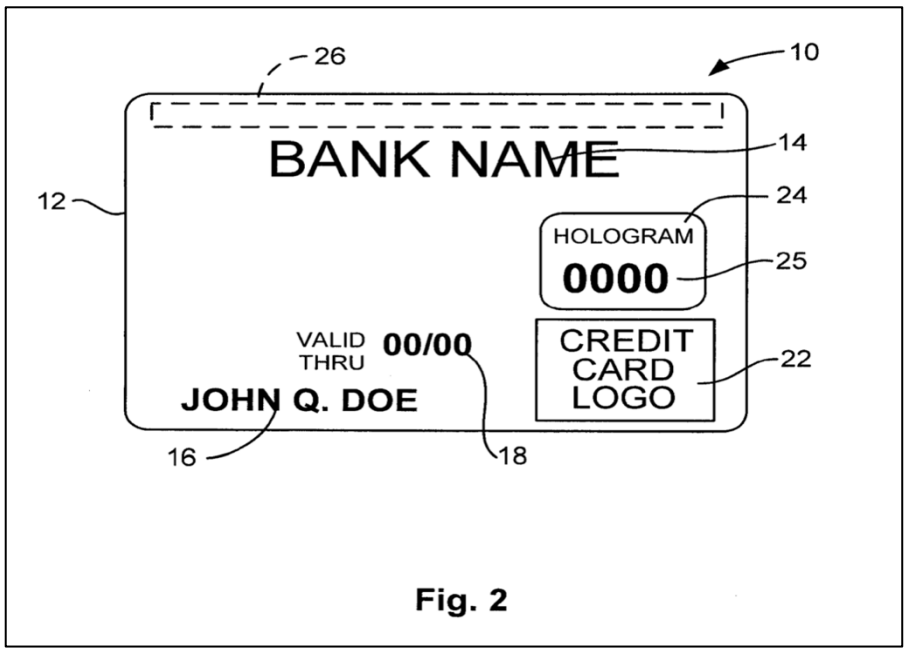
A. Claim 12: The system of claim 11, wherein the thin payment device bears no fixed payment numbers, and bears only: the cardholders name; a brand logo; and the card payment network logo.

293. To the extent this limitation is entitled to patentable weight, it is taught in view of Eng.

294. Brown teaches a thin card with no fixed payment numbers. See Claim 11(a).

295. In related art, Eng teaches a card that has: (1) *a card-holder name,* (2) credit card logo (*card payment network logo*), and a (3) Bank Name (*brand logo)*. *Eng*, [0020]-[0021], [0042]. As discussed above at Claim 2, when a traditional credit

card includes a bank name on the front, the name is typically stylized, i.e., the bank's logo with the bank's chosen font, capitalization scheme, etc.



Eng, Fig. 2.

296. To the extent embodiments of Eng's card also includes an expiration date and a portion of a PAN, a POSITA would have no reason to include those pieces of information on Brown's smart card device, since the payment credentials used by Walker's smart card constantly change. *See* Claim 1(a); *Brown (Ex.1010),* [0200], Fig. 12.

1. Motivation to Combine

297. *See* Claim 2.

B. Claim 16: The system of claim 15 wherein the card device bears no fixed payment numbers, and bears only: the cardholders name; the brand logo; and the card payment network logo.

298. *See* Claim 12.

XIII. CONCLUSION

297. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: 6/27/2025

By: 
Dr. Clifford Neuman

Curriculum Vitae

(June 2025)

B. Clifford Neuman

Education:

- Ph. D. Computer Science, June 1992, University of Washington

  Thesis: The Virtual System Model, A Scalable Approach to Organizing Large Systems. Supervised by Professor Edward D. Lazowska

- M.S. Computer Science, May 1988, University of Washington

- S.B. Computer Science and Engineering June 1985, Massachusetts Institute of Technology

  Thesis: Sentry, A Discretionary Access Control Server.
  Supervised by Dr. David D. Clark

Employment:

- Research Scientist, Information Sciences Institute, University of Southern California, 1991-Present.

- Associate Division Director, Computer Networks Division, Information Sciences Institute, University of Southern California, 2001-June 2005.

- Director, Center for Computer Systems Security, University of Southern California, 2002-Present.

- Associate Professor of Computer Science Practice, Department of Computer Science, University of Southern California, 2016-.

- Research Associate Professor, Department of Computer Science, University of Southern California, 2008-2016.

- Research Assistant Professor, Department of Computer Science, University of Southern California, 1992-2008.

- Chief Scientist, CyberSafe Corporation, 1992 – 2001.

- Pre-Doctoral Research Associate, Department of Computer Science, University of Washington, 1987-1991.

- Project Athena, Massachusetts Institute of Technology 1985-1986.

- Systems Programmer, EECS Computer Facility, Massachusetts Institute of Technology 1982-1985.

Advisory Boards:

- NTT Communications Security Advisory Board, 2003-2006.
- Eyematic Corporation, 1999-2001.
- Net Research Inc / BayBuilder, 2000-2001.

Courses taught:

- DSci429/ENGR599, Security Privacy and Policy in the Age of the Internet. Fall 2019-2024.
- INF/DSci-523 Computer Systems Assurance, Spring 2016, Fall 2017-2024.
- INF 524 Distributed Systems and Network Security, Summer 2015
- INF-526 Secure System Administration, Summer 2016, Spring 2017, Spring 2021.
- INF 527 Secure Systems Engineering, Fall 2015
- INF/DSci-529 Privacy and Security for Informatics, Spring 2016-2025.
- CSci 530 Computer Security Systems (University of Southern California), Fall 2003-2024.
- CSci 555 Advanced Operating Systems (University of Southern California), Fall 1992-2003, 2006-2012, 2014, 2020.
- CSci599 Trusted Computing (University of Southern California), Spring 2007.
- CSci532 Hacking for Defense, Innovation for Defense Applications, Spring 2018-2020, Spring 2022- 2025.
- CSci 451 Operating Systems (for University of Washington Extension), Spring 1987.

Tutorials taught:

Electronic Payment Systems, presented at:

- Usenix Workshop on Electronic Commerce, New York, July 1995.
- Usenix Workshop on Electronic Commerce, Oakland, CA, November 1996.
- Internet Society Symposium on Network and Distributed Systems Security, March 1998.
- Usenix Workshop on Electronic Commerce, Boston, MA, September 1998.
- Internet Society Symposium on Network and Distributed Systems Security, February 1999.
- 8th International World Wide Web Conference, Toronto, Canada May 1999.

Web Security and Beyond: Protecting your Electronic Commerce Application, presented at:

- Internet Society Symposium on Network and Distributed Systems Security, March 1998.
- Internet Society Symposium on Network and Distributed Systems Security, February 1999.

Research Interests:

Dr. Neuman conducts research in distributed computer systems with emphasis on scalability and computer security, especially for cyber-physical systems and critical infrastructure.

In his research, Dr. Neuman works to design and develop scalable information, security, and computing infrastructure for the Internet. He is the principal designer of the Kerberos system, an encryption based authentication system used among other things as the primary authentication method for Microsoft's Windows 2000, XP and many other systems. He has used Kerberos as a base for more comprehensive computer security infrastructure providing authorization, accounting, and audit.

Recent research includes managing computer security policies in federated and coalition environments, and using policy as a unifying element for integrating all security services including authorization, audit, and intrusion detection with systems and applications. This work extends the application of trusted computing to protect mutually suspicious entities from one another and forms the basis for the TrustView security architecture.

Most recently, Dr. Neuman has focused on security for cyber-physical systems, with an emphasis on protection of critical infrastructure, including the power grid. Recent publications discuss cross-domain threat propagation in such systems, and mitigation techniques applied in both the cyber and physical domains.

Dr. Neuman has designed systems for network payment which build upon security infrastructure to provide a secure means to pay for services provided over the Internet. The NetCheque and NetCash systems, which are suitable for micropayments (payments on the order of pennies where the cost of clearing a credit card payment would be prohibitive). NetCheque provides accounting for the flow of funds through the system whereas NetCash supports anonymous transactions.

He is the principal designer of the Prospero system which is used to organize and retrieve information distributed on the Internet. The Prospero system applies the Virtual System Model to construct views of the information available on the network. Prospero is an embedded system that is used by several commercial products.

IPR2025-01147
Apple EX1003 Page 226

The Prospero Resource Manager (PRM) supports the management of computing resources in distributed systems. PRM provides multiple views of the available resources by supporting multiple resource managers, each controlling a subset of the resources in the system, independent of other managers of the same type. The functions of resource management are distributed across three types of managers: system managers, job managers, and node managers. The complexity of these management roles is reduced because each is designed to utilize information at an appropriate level of abstraction.

Awards

- InfoWorld Top Ten Technology Innovators, InfoWorld Magazine, February 2002.
- 2001 Usenix Software Tools User Group Award recipient for contributions to the development of Kerberos.
- DARPA Dynamic Coalitions Program 2003 award for excellence in academic research.
- Usenix Security 2022 Test of Time Award for Kerberos: An Authentication Service for Open Network Systems, Published in 1988 Winter USENIX Technical Conference Proceedings.

Memberships and Professional Activities:

Memberships

- Association for Computing Machinery (ACM) – Life member.
- Institute of Electrical and Electronic Engineers (IEEE) - Senior member
- IEEE Computer Society
- Internet Society (ISOC)
- Internet Engineering Task Force (IETF) - Participant
- Usenix Association

Program and General Chair

- Program Chair, Fourth Annual PKI R&D Workshop: “Multiple Paths to Trust”, Gaithersburg, MD. April 2005.
- General Chair, 2004 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2004.

IPR2025-01147
Apple EX1003 Page 227

- General Chair, 2003 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2003.

- Vice Program Chair, Security Track, International Conference on Distributed Computing Systems (ICDCS), Vienna Austria, 2002.

- Program Chair, 2002 Workshop on Accelerating Trustworthy Internetworking.

- General Chair, 2002 Internet Society Symposium on Network and Distributed System Security. San Diego, CA, February 2002.

- Program Chair, 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland. April 1997.

- Program Chair, 4th Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1997.

- Program Chair, 3rd Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1996.

Editorial and Publication Advisory Boards

- Guest Editor, Journal of High Speed Networking, special issue on managing security policies, 2006.

- Contributed/Edited section of Report of the Workshop on Responding to the Unexpected, February 27, 2002, New York City.

- Editorial Board, International Journal of Electronic Commerce, June 1996 - Present.

- Editorial Board, ACM Transaction on Information and Systems Security, 1998 – 2001.

Program Committees

- Program Committee, 2015 Industrial Control Systems Security Workshop at ACSAC, December 2015, Los Angeles.

- Program Committee, 2015 IEEE International Conference on Intelligence and Security Informatics, May 2015. Baltimore MD, USA.

- Steering Group, 2013 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2014.

IPR2025-01147
Apple EX1003 Page 228

- Program Committee, 2012 IEEE International Conference on Intelligence and Security Informatics, Washington DC, June 2012.

- Program Committee, ACM SIGKDD Workshop on Intelligence and Security Informatics 2012 (ISI-KDD 2012), Beijing China.

- Steering Group, 2013 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2013.

- Steering Group, 2012 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2012.

- Steering Group, 2011 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2011.

- Program Committee, 2010 ACM Symposium on Access Control Models and Technologies (SACMAT2010). Pittsburgh, June 2010.

- Program Committee, 2011 IEEE International Conference on Intelligence and Security Informatics. 011, Beijing China.

- Program Committee, 2010 IEEE International Conference on Intelligence and Security Informatics. May 2010, Vancouver, BC, Canada.

- Program Committee, 9th Symposium on Identity and Trust on the Internet (IDtrust 2010), Gaithersburg, MD, April 2010.

- Steering Group, 2010 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2010.

- Program Committee, 2009 ACM Symposium on Access Control Models and Technologies (SACMAT2009). Stresa, Italy, June 2009.

- Program Committee, 2009 IEEE International Conference on Intelligence and Security Informatics. June 2009, Dallas TX, USA.

- Program Committee, 8th Symposium on Identity and Trust on the Internet (IDtrust 2009), Gaithersburg, MD, April 2009..

- Steering Group, 2009 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2009

- 2008 IEEE International Conference on Intelligence and Security Informatics. June 2008, Taipei, Taiwan.

IPR2025-01147
Apple EX1003 Page 229

- Program Committee, 7th Seventh Symposium on Identity and Trust on the Internet (IDtrust 2008), Gaithersburg, MD, March 2008.

- Program Committee, 2007 IEEE International Conference on Intelligence and Security Informatics. May 2007, New Brunswick NJ. USA.

- Program Committee, 6th Annual PKI R&D Workshop, Gaithersburg, MD. April 2007.

- Steering Group, 2007 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2007.

- The First Workshop on Security, Trust and Privacy in Grid Environments STPG2008), at The 8th IEEE International Symposium on Cluster Computing and the Grid (CCGRID2008), 19-22 May 2008, Lyon, France

- 2006 IEEE Workshop on Policies for Distributed Systems and Networks (Policy2006), London Ontario, June 2006.

- 11th ACM Symposium on Access Control Models and Technologies (SACMAT2006). Lake Tahoe, June 2006.

- 2006 IEEE International Conference on Intelligence and Security Informatics. May 2006, San Diego USA.

- Fifth Annual PKI R&D Workshop, Gaithersburg, MD. April 2006.

- Second International Workshop on Security in Distributed Computing Systems. (in conjunction with 25th International Conference on Distributed Computing Systems ICDCS-2005), Columbus, OH, USA. June 2005.

- 2005 IEEE International Conference on Intelligence and Security Informatics. May 2005, Atlanta USA.

- 2004 IEEE International Conference on Intelligence and Security Informatics. June 2004, Tucson USA.

- 2003 IEEE International Conference on Intelligence and Security Informatics. June 2003, Tucson USA.

- IEEE Sixth International Workshop on Policies for Distributed Systems and Networks (Policy2005). June 2005, Stockholm Sweden..

- IEEE Fifth International Workshop on Policies for Distributed Systems and Networks (Policy2004). June 2004, New York.

IPR2025-01147
Apple EX1003 Page 230

- Steering Group, Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2001 to 2006.

- 21st International Conference on Distributed Computer Systems (ICDCS-21), Phoenix, AZ, April 2001,

- Ninth International World Wide Web Conference, Amsterdam, May 2000.

- 2001 Symposium on Applications and the Internet (SAINT), San Diego, CA, January 2001. (IEEE Computer Society).

- Eighth Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2000.

- Sixth ACM Conference on Computer and Communications Security, Singapore, November 1999.

- First ACM Conference on Electronic Commerce (EC-99), Denver, CO, November 1999.

- Eighth International World Wide Web Conference, Toronto, May 1999.

- Third International Conference on Financial Cryptography, Anguilla, British West Indies, February 1999.

- Seventh IEEE International Symposium on High Performance Distributed Computing, Chicago, IL, July 1998.

- First International Conference on Financial Cryptography, Anguilla, British West Indies, February 1997.

- Second Usenix Workshop on Electronic Commerce, Oakland, CA, November 1996.

- 1996 Conference on The Convergence of Telecommunications and Distributed Computing Technologies (TINA), Heidelberg, Germany, September 1996.

- Sixth Usenix Security Symposium, San Jose, CA July 1996.

- Third ACM Conference on Computer and Communications Security, New Delhi, India, March 1996.

- First Usenix Workshop on Electronic Commerce, New York City, July 1995.

- Second Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1995.

IPR2025-01147
Apple EX1003 Page 231

- Second ACM Conference on Computer and Communications Security, Fairfax VA, November 1994.

- First Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1994.

- First ACM Conference on Computer and Communications Security, Fairfax VA, November 1993.

- PSRG Workshop on Network and Distributed System Security, San Diego, CA, February 1993.

Other positions

- Panel member, National Research Council, CSTB Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government, October 2001.

- Publications Chair, 3rd ACM Conference on Computer and Communications Security, March 1996.

Publications (Journals):

- Wadhawan, Yatin, Clifford Neuman, and Anas AlMajali. "IGNORE: A Policy Server to Prevent Cyber-Attacks from Propagating to the Physical Domain." Applied Sciences 10, no. 18 (2020): 6236.

- AlMajali, Anas, Yatin Wadhawan, Mahmood S. Saadeh, Laith Shalalfeh, and Clifford Neuman. "Risk assessment of smart grids under cyber-physical attacks using Bayesian networks." International Journal of Electronic Security and Digital Forensics 12, no. 4 (2020): 357-385.

- Anas Al Majali, W. Yatin., Neuman, C, Saadeh. Mahmood, Shalalfeh. Laith. “Risk Assessment of Smart Grids under Cyber-physical Attacks using Bayesian Networks”. Accepted in 2019 for International Journal of Electronic Security and Digital Forensics

IPR2025-01147
Apple EX1003 Page 232

- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks", MDPI: A special issue of Electronics: Cyber-Physical Systems. 2018.

- Anas AlMajali, Arun Viswanathan, Clifford Neuman, Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats. Electronics 6(1), 2016.

- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. (A retrospective) Electronic Networking: Research, Applications and Policy, 20(4): 408-419, Winter 2012. (refereed journal)

- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. A Tatyana Ryutov, Clifford Neuman, Li Zhou and Noria Foukia, *Initial Trust Formation in Virtual Organizations*, International Journal of Internet Technology and Security Transactions, 2007.

- Tatyana Ryutov, Clifford Neuman, Dongho Kim and Li Zhou. Integrated Access control and Intrusion Detection for Web Servers. IEEE Transaction on Parallel and Distributed Systems, Vol 14, No. 9, September 2003.

- R. Bajcsy, et. al. Cyber Defense Technology Networking and Evaluation, Communications of the ACM, March 2004.

- Tatyana Ryutov, Grig Gheorghiu, and Clifford Neuman, An Authorization Framework for Metacomputing Applications, Cluster Computing 2(1999), 165-175.

- B. Clifford Neuman and Theodore Ts'o. Kerberos: An Authentication Service for Computer Networks, IEEE Communications, 32(9):33-38. September 1994.

- B. Clifford Neuman and Santosh Rao. The Prospero Resource Manager: A scalable framework for processor allocation in distributed systems, Concurrency: Practice and Experience, 6(4):339-355, June 1994.

- B. Clifford Neuman. Enabling Commerce on the Internet, IEEE Computer29(4):91-92. April 1996.

- B. Clifford Neuman. Security, Payment, and Privacy for Network Commerce, IEEE Journal on Selected Areas in Communications, 13(8):1523-1531. October 1995.

- B. Clifford Neuman. The Prospero File System: A global file system based on the Virtual System Model. Computing Systems, 5(4):407-432, Fall 1992.

- Michael F. Schwartz, Alan Emtage, Brewster Kahle, and B. Clifford Neuman A Comparison of Internet Resource Discovery Techniques. Computing Systems, 5(4):461-493, Fall 1992.

- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. Electronic Networking: Research, Applications and Policy, 2(1): 30-37, Spring 1992. (refereed journal)

Publications (Other):

- C. Pandit, H. Kothari and C. Neuman, "Privacy in time of a pandemic," 2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275), 2020, pp. 1-6, doi: 10.1109/CMI51275.2020.9322737.

- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "PSP: A Framework to Allocate Resources to Power Storage Systems under Cyber-Physical Attacks", 5th International Symposium for ICS-SCADA Cyber Security. 2018.

- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "A Systematic Approach to Analyze Multiple Cyber-Physical Attacks on Smart Grid", International Conference on Cyber Security of Cyber Physical Systems. 2018.

- Yatin Wadhawan , Dr. Clifford Neuman. "RL-BAGS: A Tool for Smart Grid Risk Assessment", International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). 2018.

- Wadhawan, Yatin and Neuman, Clifford,“BAGS: A Tool to Quanify Smar-Grid Resilience”, September 2017, In Proceedigs of the 4th International Workshop on Cyber-Physical Systems at the Federated Conference on Computer Science and Information Systems, Prague, Czech Repulic.

- Wadhawan, Yatin and Neuman, Clifford, and AlMajali, Anas “Analyzing Cyber-Physical Attacks on Smart Grid Systems”, 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), April 2017, Pittsburgh.

- Wadhawan, Yatin and Neuman, Clifford, “Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology”, ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC) 2016.

- Yatin Wadhawan and Clifford Neuman. Defending Cyber-Physical Attacks on Oil Pipeline Systems: A Game-Theoretic Approach Yatin Wadhawan and

Clifford Neuman. International Workshop on AI for Privacy and Security (PRAISE) from 29 August to 2 Septembe 2016, at the Haugue, Netherlands.

- Yatin Wadhawan and Clifford Neuman, A Roadmap to Evaluate Resilience of Oil and Gas Cyber-Physical Systems. 2015 ACSAC Workshop on Industrial and Control System Security, Los Angeles, December 2015.

- Tatyana Ryutov, Anas AlMajali, Clifford Neuman, Modeling Security Policies for Mitigating the Risk of Load Altering Attacks on Smart Grid Systems, in Proceedings of the 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES) (IEEE), Seattle, April 2015.

- Anas AlMajali, Eric Rice, Arun Viswanathan, Kymire Tan, Clifford Neuman, *A Systems Approach to Analysing Cyber-Physical Threats in the Smart-Grid*, in Proceedings of the 4th International Conference on Smart Grid Communications (IEEE SmartGridComm), Vancouver, October 2013.

- Arun Viswanathan, Kymie Tan, Clifford Neuman, *Deconstructing the Assessment of Anomaly-Based Intrusing Detectors for Critical Applications*, in Proceedings of the16th International Symposium on Research in Attacks , Intrusions, and Defenses (RAID2013) St. Lucia, October 2013.

- Hashem Alayed, Fotos Frangoudes, and Clifford Neuman, *Behavioral-Based Cheating Detection in Online First Person Shooters using Machine Learning Techniques*, in Proceedings of IEEE 2013 Conference on Computational Intelligence in Games, Niagara Falls, Canada, August 2013.

- Anas AlMajali, Arun Viswanathan, and Clifford Neuman, *Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack*, in Proceedings of the 5th Workshop on Cyber Security Experimentation and Test (CSET'12) Bellevue, Washington, August 2012.

- Clifford Neuman and Kymie Tan, *Mediating Cyber and Physical Threat Propagation in Security Smart Grid Architecture*, in Proceedings of the 2nd International Conference on Smart Grid Communications (IEEE SmartGridComm), Brussels, October 2011.

Clifford Neuman, *Challenges in Security for Cyber-Physical Systems*, DHS Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, July 22-24, 2009.

- Arun Viswanathan, Clifford Neuman, Secure System Views: A new Paradigm for Secure Usable Sysems. USC-ISI Tehnical Report Number ISI-TR-654, January 2009.

- Terry Benzel, Robert Braden, Dongho Kim, Clifford Neuman, Anthony Joseph, Keith Sklower, Ron Ostrenga, Stephen Schwab, Design Deployment

and use of the DETER testbed.. In Proceedings of the DETER Community Workshop on Cyber-Security and Test, August 2007, Boston.

- Tatyana Ryutov, Clifford Neuman, A Trust Based Approach for Improving Data Reliability in Industrial Sensor Networks, in proceedings of the joint ITRUST and PST Conference on Privacy, Trust Management, and Security, New Brunswick Canada, August 2007. Also, ISI-TR-631, January 2007.

- Tatyana Ryutov, Clifford Neuman, Situational Identity: A Person-centered Identity Management Approach, USC ISI Technical report ISI-TR-630, January 2007.

- Tatyana Ryutov, Clifford Neuman, Ronak Shah, Automated Management of Vulnerability Mitigation Prescriptions. USC ISI Technical report ISI-TR-630, January 2007.

- Clifford Neuman, Managing Multiple Perspectives on Trust, *in proceedings of the 2007 Cyber Security and Information Infrastrcture Research Workshop*, Oak Ridge Tennessee, May 2007.

- Clifford Neuman. *Understanding Trust in SCADA Systems.* Proceedings of Beyond SCADA: Network Embedded Control for Cyber-Physical Systems. Pittsburgh, November 9, 2006. (Refereed Workshop Position Statement)

- Sukumal Kitisin and Clifford Neuman. *Reputation-Based Trust-Aware Recommender System*. Proceedings of the 2nd IEEE Workshop on the Value of Security Through Collaboration (SECOVAL), September 2006, Baltimore. (refereed workshop)

- Ho Chung and Clifford Neuman. *Modeling the Relative Strength of Security Protocols*. Proceedings of the 2nd ACM CCS Workshop on Quality of Protection, October 2006, Alexandria VA. (refereed workshop)

- Clifford Neuman, Chinmay Shah, Kevin Lahey. *Running Live Self-Propagating malware on the DETER Testbed.* Proceedings of the DETER Community Workshop, Arlington VA, June 2006.

- Noria Foukia, Liz Zhou and Clifford Neuman. *Multilateral Decision for Collaborative Defense Against Unsolicited Bulk e-mail*. Proceedings of the 4th International Conference on Trust Management. Pisa, Italy, May 2006. (refereed conference)

- Terry Benzel, Bob Braden, Dongho Kim, Clifford Neuman Anthony Joseph and Keith Sklower Ron Ostrenga and Stephen Schwab, *Experience with DETER: A Testbed for Security Research.* Second IEEE Conference on testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), March 2006, Barcelona. (refereed conference)

IPR2025-01147
Apple EX1003 Page 236

- L. Li, I. Hamadeh, S. Jiwasurat, G. Kesidis, P. Liu, C. Neuman, *Emulating Sequential Scanning Worms on the DETER Testbed,* In Proceedings of 2nd International IEEE/CreateNet Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), March 2006. (refereed conference)

- Tatyana Ryutov, Clifford Neuman, Li Zhou and Noria Foukia, *Establishing Agreements in Dynamic Virtual Organizations*, in Proceedings of the Workshop on the Value of Security through Collaboration, part of IEEE SecureComm, September 2005, Athens. (refereed workshop)

- Tatyana Ryutov, Clifford Neuman, Noria Foukia, Travis Leithead, Kent Seamons, Li Zhou, *Adaptive Trust Negotiation and Access Control for Grids*. 6th IEEE/ACM International Workshop on Grid Computing, Seattle, November 2005. (refereed workshop)

- Sultan Almuhammadi and Clifford Neuman, "Security and Privacy using One-Round Zero Knowledge Proofs", 7th IEEE Conference on E-Commerce Technology, Munich, July 2005. (refereed conference)

- Tatyana Ryutov, Li Zhou, Clifford Neuman, Travis Leithead, and Kent E. Seamons, "**Adaptive Trust Negotiation and Access Control**," *in Proceedings of the ACM Symposium on Access Control Models and Technologies* (SACMAT'05), Stockholm, June 1-3, 2005. (refereed conference)

- Tatyana Ryutov, Clifford Neuman, Dongho Kim and Li Zhou. Integrated Access control and Intrusion Detection for Web Servers. In proceedings of the 23rd International Conference on Distributed Computing Systems, Providence, Rhode Island, May 2003. (refereed conference)

- Tatyana Ryutov, Clifford Neuman and Dongho Kim. Dynamic Authorization and Intrusion Response in Distributed Systems. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition (DISCEX III), April 2003. (refereed conference)

- Tatyana Ryutov and Clifford Neuman. The Specification and Enforcement of Advanced Security Policies. To be published In Proceedings of the Third International Conference on Policies for Distributed Systems and Networks (POLICY 2002), June 2002, in Monterey, California. (refereed conference)

- Tatyana Ryutov and Clifford Neuman, The Set and Function Approach to Modeling Authorization in Distributed Systems, in Proceedings of the Information Assurance in Computer Networks Methods, Models, and

IPR2025-01147
Apple EX1003 Page 237

Architectures for Network Security, May 2001, St. Petersburg, Russia, 189-206. (refereed conference)

- Tatyana Ryutov and Clifford Neuman, Representation and Evaluation of Security Policies for Distributed System Services, in Proceedings of the DARPA Information Survivability Conference and Exposition, January 2000. Hilton Head, SC. (refereed conference)

- Sukumal Imudom and B. Clifford Neuman, A Framework Supporting Collaborative Filtering for Internet Information, AAAI-98 Workshop on Recommender Systems, Madison, WI, July 1998. (refereed conference)

- G. Gheorghiu, T. Ryutov, and B. Clifford Neuman, Authorization for Metacomputing Applications, in Proceedings of the 7th IEEE Symposium on High Performance Distributed Computing, Chicago, IL, July 1998. (refereed conference)

- Sung-Wook Ryu and B. Clifford Neuman, Garbage Collection for Distributed Persistent Objects, in Proceedings of the Workshop on Compositional Software Architectures, Monterey, CA January 1998. (referred conference)

- B. Clifford Neuman and Gennady Medvinsky. Requirements for Network Payment: The NetCheque Perspective In Proceedings of IEEE COMPCON'95. March 1995. (referred conference)

- Clifford Neuman and Genaddy Medvinsky, *NetCheque, NetCash, and the Characteristics of Internet Payment Services*, MIT Workshop on Internet Economics, March, 1995

- Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman. Endorsements, Licensing, and Insurance for Distributed System Services, In Proceedings of 2nd the ACM Conference on Computer and Communication Security. November 1994. (refereed conference)

- B. Clifford Neuman. How to Trust a Distributed System. In Proceedings of the National Computer Security Conference. Baltimore MD, October 1994. (invited conference)

- Gennady Medvinsky and B. Clifford Neuman. Electronic Currency for the Internet, Electronic Markets 3(9/10):23-24, October 1993. Also appeared in Connexions 8(6):19-23, June 1994. (unrefereed journal)

- Gennady Medvinsky and B. Clifford Neuman. NetCash: A design for practical electronic currency on the Internet. In Proceedings of the 1st ACM Conference

IPR2025-01147
Apple EX1003 Page 238

on Computer and Communication Security. November 1993. (refereed conference)

- B. Clifford Neuman, Steven Seger Augart, and Shantaprasad Upasani. Using Prospero to support integrated location independent computing. In Proceedings of the Symposium on Mobile and Location Independent Computing, August 1993. (refereed conference)

- B. Clifford Neuman. Prospero: A base for building information infrastructure. In Proceedings of INET'93, August 1993. (referred conference)

- B. Clifford Neuman and Santosh Rao. Resource Management for Distributed Parallel Systems. In Proceedings of the 2nd International Symposium on High Performance Distributed Computing, July 1993. (refereed conference)

- B. Clifford Neuman. Proxy-Based Authorization and Accounting for Distributed Systems. In Proceedings of the 13th International Conference on Distributed Computing Systems, pages 283-291, May 1993. (refereed conference)

- B. Clifford Neuman and Stuart G. Stubblebine. A Note on the Use of Timestamps as Nonces. Operating Systems Review, 27(2):10-14, April 1993. (unrefereed)

- B. Clifford Neuman. Prospero: A virtual directory service for the Internet, Connexions 6(7):2-9, July 1992. (unrefereed)

- B. Clifford Neuman. The Prospero File System: A global file system based on the Virtual System Model. In Proceedings of the 1st Usenix Workshop on Filesystems May 1992. (refereed conference)

- B. Clifford Neuman. Protection and Security Issues for Future Systems. In Proceedings of the Workshop on Operating Systems of the 90s and Beyond . Dagstuhl Castle, Germany. July 1991.(invited workshop)

- B. Clifford Neuman. The Need for Closure in Large Distributed Systems. Operating Systems Review, 23(4): 28-30, October 1989. (unrefereed)

- B. Clifford Neuman. Workstations and the Virtual System Model. In Proceedings of the 2nd IEEE Workshop on Workstation Operating Systems, pages 91-95, September 1989. (refereed conference)

- B. Clifford Neuman and Jennifer G. Steiner. Authentication of Unknown Entities on an Insecure Network of Untrusted Workstations. In Proceedings of the Usenix

IPR2025-01147
Apple EX1003 Page 239

Workshop on Workstation Security, Portland, OR. August 1988. (refereed conference)

- J. G. Steiner, B. Clifford Neuman, and J.I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In Proceedings of the Winter 1988 Usenix Conference. February, 1988. (Version 4) (refereed conference)

- B. Clifford Neuman and Wayne Yamamoto. Adding Packet Radio to the Ultrix Kernel. In Proceedings of the Winter 1988 Usenix Conference February, 1988. (refereed conference)

- B. Clifford Neuman. Packet Radio and IP for the Unix Operating System. In Proceedings of the Sixth ARRL Computer Networking Conference, Redondo Beach, CA. August, 1987. (refereed conference)

Book Chapters:

- Sanjay Goel, Stephen F. Bush, Clifford Neuman, Smart Grid Security (Chapter 10) in IEEE Vision for Smart Grid Communications: 2030 and Beyond, IEEE Standards Association, 2013.

- Frank Siebenlist, Nataraj Nagaratnam, Von Welch, Clifford Neuman, Security for Virtual Organizations: Federating Trust and Policy Domains. in The GRID 2: Blueprint for a New Computing Infrastructure (edited by Kesselman and Foster), Morgan, Kauffman Publishers, 2004. (invited)

- Clifford Neuman, Security and Privacy, in Cancer Informatics: Essential Technologies for Clinical Trials, Springer-Verlag Inc, 2002. (invited)

- B. Clifford Neuman, Security, Accounting, and Assurance, in The GRID: Blueprint for a New Computing Infrastructure (edited by Kesselman and Foster), Morgan, Kauffman Publishers, 1999. (invited)

- B. Clifford Neuman and Gennady Medvinsky, Internet Payment Services, in Internet Economics, MIT Press. 1997. (refereed conference -> book)

- Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman, Endorsements, Licensing, and Insurance for Distributed Services, in Internet Economics, MIT Press. 1997. (refereed conference -> book)

- B. Clifford Neuman, A Flexible Framework for Network Payment, in Readings in Electronic Commerce, Addison-Wesley. 1996. (invited)

- B. Clifford Neuman, Scale in Distributed Systems, Readings in Distributed Computing Systems, IEEE Computer Society Press, 1994. (refereed book chapter)

- John T. Kohl, B. Clifford Neuman, and Theodore Y. T'so, The Evolution of the Kerberos Authentication System. In Distributed Open Systems, pages 78-94. IEEE Computer Society Press, 1994. (refereed conference -> book)

Theses, Technical Reports, and Working Documents:

- Clifford Neuman, Tom Yu, Sam Hartman, Ken Raeburn, The Kerberos Network Authentication System, RFC 4120. July 2005 (standards specification).

- Dongho Kim and B. Clifford Neuman. Reconstructing Interconnections on Disconnected Mobile Hosts, ISI Technical Report ISI-TR-528, University of Southern California / Information Sciences Institute, April 2000

- John Kohl and B. Clifford Neuman. The Kerberos Network Authentication Service (Version 5). Internet Request for Comments RFC-1510. September 1993.

- B. Clifford Neuman, The Virtual System Model: A Scalable Approach to Organizing Large Systems, Ph.D. Thesis, University of Washington, Department of Computer Science and Engineering Technical Report 92-06-04, June 1992.

- B. Clifford Neuman. Proxy-Based Authorization and Accounting for Distributed Systems. Technical Report 91-02-01, Department of Computer Science and Engineering, University of Washington, March 1991.

- B. Clifford Neuman. The Virtual System Model: A Scalable Approach to Organizing Large Systems (A Thesis Proposal). Technical Report 90-05-01, Department of Computer Science and Engineering, University of Washington, May 1990.

- B. Clifford Neuman. The Virtual System Model for Large Distributed Operating Systems. Technical Report 89-01-07, Department of Computer Science, University of Washington, April, 1989.

- S.P. Miller, B. C. Neuman, J. I. Schiller, and J.H. Saltzer. Section E.2.1: Kebreros Authentication and Authorization System. Project Athena Technical Plan, MIT Project Athena, Cambridge, Massachusetts, October 1988. (Describes Version 4)

- B. Clifford Neuman. Sentry: A Discretionary Access Control Server. Bachelor's Thesis, Massachusetts Institute of Technology, June 1985.

IPR2025-01147
Apple EX1003 Page 241

Students who completed Ph.D. under Dr. Neuman

- Ho Chung, - Ph.D. USC 2009. Modeling the Relative Strength of Security. Now a researcher at Samsung.
- Li Zhou, - Ph.D. USC 2006. Negotiation of Multilateral Security Decisions. Now a researcher at Microsoft, Redmond WA.
- Sultan Almuhammadi – Ph.D. USC 2005, Security and Privacy Using One-Round Zero-Knowledge Proofs, now faculty at King Fahd University, Saudi Arabia.
- Noria Foukia (postdoc at USC 2004/05), currently Lecturer at University of Otago, Dunedin NZ.
- Xuhua Ding, Ph.D. USC 2003 (co-advisor with Gene Tsudik). Fine-grained control of security services. Now assistant professor at Singapore Management University.
- Yongdae Kim, Ph.D. USC 2002 (co-advisor with Gene Tsudik). Group Key Agreement: Theory and Practice, now faculty at University of Minnesota.
- Tatyana Ryutov - Ph.D. USC 2002, The Condition-driven Authorization Model for Distributed System Services, Now at USC Information Sciences Institute
- Dongho Kim – Ph.D. USC 2001, Reconstructing Interconnections on Disconnected Mobile Hosts, Now at USC Information Sciences Institute
- Sukumal Imudom – Ph.D. USC 2001, Distributed Annotation Framework Supporting Collaborative Filtering of Information, now faculty at Kasetsart University, Thailand.
- Eul Gyu Im - Ph.D. USC 2001, A Flexible Framework for Replication in Distributed Systems, now at National Security Research Institute, South Korea.
- Gennady "Ari" Medvinsky - Ph.D. USC 1996, Electronic Payment Services To CyberSafe Corporation, to Excite - @ Home, to Keen.com, to Microsoft.
- Santosh Rao - Ph.D. USC 1996, Resource Management, Parallel Debugging, and PRM, Now at Veritas Software
- Brenda Timmerman - Ph.D. USC - Traffic Flow Confidentiality, Faculty at Cal State Northridge
- Sung-Wook Ryu - Ph.D. USC - Garbage Collection for Prospero, Now at Veritas Software

IPR2025-01147
Apple EX1003 Page 242

- Konstadinos Kutsikos – Ph.D. USC - Electronic Commerce and Economics, now faculty at University of the Aegean, Greece.

- Anas Almajali – Ph.D. USC – Analysis of Threats in Cyber-Physical Systems. Now faculty at Hashemite University, Jordan.

- Hashem Alayed – Ph.D. USC – Security in Online games, now faculty at King Saud University, Saudi Arabia.

- Arun Viswanathan – Ph.D. USC – Situational Awareness and Intrusion Detection in Cyber-physical systems. Now working for NASA Jet Propulsion Lab.

- Yatin Wadhawan – Ph.D. USC - Analyzing Cyber-Physical Attacks on Industrial Control Systems. Now working at Microsoft.

- Abdulla Alwabel – Ph.D. USC Overcoming Challenges Facing Malware Behavioral Analysis.

IPR2025-01147
Apple EX1003 Page 243