

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA, INC.,

Petitioner,

v.

CORTEX MCP, INC.,

Patent Owner.

IPR2024-00488

PATENT NO. 9,954,854

DECLARATION OF MICHAEL IAN SHAMOS, PH.D., J.D.

TABLE OF CONTENTS

I. INTRODUCTION AND QUALIFICATIONS	1
II. MATERIALS CONSIDERED	5
III. SUMMARY OF OPINIONS	8
IV. LEGAL PRINCIPLES	9
V. THE CHALLENGED PATENT.....	15
VI. LEVEL OF ORDINARY SKILL IN THE ART	23
VII. CLAIM CONSTRUCTION	24
A. “officially verifiable electronic representation”/”OVER” file.....	25
B. “scan”	29
C. “...verified by an issuing agency...”	32
VIII. BACKGROUND OF THE PRIOR ART	34
A. Secure Credentials.....	34
B. Tokens	38
C. QR Codes.....	72
D. Near-Field Communication.....	77
E. Credential Identifiers.....	80
F. Device Identifiers	81
G. Status Indicators	83
H. Reason for Invalid Credential	84
IX. Ground 1: Claims 1-17 were Obvious over Osborne	85
A. Overview of Ground.....	85
B. Claim 1	87
1. Preamble.....	87
2. Limitation 1.1	87
3. Limitation 1.2	97
4. Limitation 1.3	98
5. Limitation 1.4	103
6. Limitations 1.5-1.8	103

C.	Claim 8	105
1.	Preamble.....	105
2.	Limitations 8.1-8.2	106
3.	Limitations 8.3-8.10	108
D.	Claim 15	108
E.	Claims 2, 9, and 16.....	109
F.	Claims 3-4, 10-11, and 17	111
G.	Claims 5 and 12.....	112
H.	Claims 6 and 13.....	114
I.	Claims 7 and 14.....	115
X.	Ground 2: Claims 1-17 were Obvious over Osborne in view of Neafsey.....	117
A.	Rationale to Combine.....	117
XI.	Ground 3: Claims 1-17 were Obvious over Stafford in view of Purves further in view of Neafsey	118
A.	Overview and Rationale to Combine	118
B.	Claim 1	123
1.	Preamble.....	123
2.	Limitation 1.1	123
3.	Limitation 1.2	131
4.	Limitation 1.3	132
5.	Limitation 1.4	133
6.	Limitations 1.5-1.8	134
C.	Claim 8	135
1.	Preamble.....	135
2.	Limitations 8.1-8.2	136
3.	Limitations 8.3-8.10	137
D.	Claim 15	138
E.	Claims 2, 9, and 16.....	139
F.	Claims 3-4, 10-11, and 17	140
G.	Claims 5 and 12.....	140
H.	Claims 6 and 13.....	140

I. Claims 7 and 14.....	142
XII.CONCLUDING STATEMENT	143
XIII. JURAT.....	143

I, Michael I. Shamos, declare as follows.

I. INTRODUCTION AND QUALIFICATIONS

1. I have been retained by Wilson Sonsini Goodrich & Rosati Professional Corporation on behalf of Petitioner Visa, Inc. (“Visa”) to provide my opinions concerning the validity of claims 1-17 (the “Challenged Claims”), constituting all claims of U.S. Patent No. 9,954,854 (“’854 Patent,” or the “Patent,” EX1002) in support of Petitioner’s Petition for *Inter Partes* Review of the ’854 Patent (the “Petition”).

2. I have been retained as an independent expert consultant in this proceeding before the United States Patent and Trademark Office. Although I am being compensated at my rate of \$600.00 per hour for the time I spend on this matter, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding, any of the parties, or the subject patent.

3. A detailed description of my professional qualifications, including a listing of my specialties/expertise and professional activities and publications, is contained in my curriculum vitae, a copy of which is provided as EX1006. Below is a short summary of my professional qualifications.

4. I received an A.B. (1968) from Princeton University in Physics; a M.A. (1970) from Vassar College in Physics; a M.S. (1972) from American University in Technology of Management, a field that covers quantitative tools used in managing

organizations, such as statistics, operations research and cost-benefit analysis; a M.S. (1973), and M.Phil. (1974) and a Ph.D. (1974) from Yale University in Computer Science; and a J.D. (1981) from Duquesne University.

5. I currently hold the title of Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. I am a member of two departments in that School, the Software and Societal Systems Department and the Language Technologies Institute. I was a founder and Co-Director of the Institute for eCommerce at Carnegie Mellon from 1998-2004 and from 2004-2018 was Director of the eBusiness Technology graduate program in the Carnegie Mellon University School of Computer Science. Since 2018, I have been Director of the M.S. in Artificial Intelligence and Innovation degree program at Carnegie Mellon.

6. I have taught graduate courses at Carnegie Mellon in Electronic Commerce, including eCommerce Technology, Electronic Payment Systems, Electronic Voting, Internet of Things, Electronic Payment Systems and eCommerce Law and Regulation, as well as Analysis of Algorithms. Since 2007 I have taught an annual course in Law of Computer Technology. I currently also teach Artificial Intelligence and Future Markets.

7. I am the author and lecturer in a 24-hour video course on Internet protocols and have taught computer networking, wireless communication, and Internet architecture since 1999.

8. From 2001-2021, I was a Visiting Professor at the University of Hong Kong, where I taught an annual course in Electronic Payment Systems. This is one of only a handful of graduate courses taught on this subject in the world.

9. I was the Director of Carnegie Mellon's graduate degree program in eBusiness Technology from 1999-2018 and am now a faculty member in the Privacy Engineering degree program at Carnegie Mellon. My course on Law of Computer Technology is required for all students in that program, the M.S. in Artificial Intelligence and Innovation program and in the Societal Computing Ph.D. program.

10. From 1979-1987, I was the founder and president of two computer software development companies in Pittsburgh, Pennsylvania, Unilogic, Ltd. and Lexeme Corporation.

11. I am an attorney admitted to practice in Pennsylvania and have been admitted to the Bar of the U.S. Patent and Trademark Office since 1981. I have been asked to render opinions in this Declaration as a technical expert. I have not been asked to offer any opinions on patent law in this proceeding.

12. I am a named co-inventor on the following six issued patents relating to electronic commerce: U.S. Patent Nos. 7,330,839, 7,421,278, 7,747,465, 8,195,197, 8,280,773, and 9,456,299.

13. I have previously served as an expert in over 375 cases concerning computer technology. In particular, I have been involved in at least 40 cases involving electronic payments.

14. I am aware of contemporaneous litigation involving the parties in a case styled *Cortex MCP, Inc. v. Visa, Inc.*, 6:23-cv-00048-FB (W.D. Texas) (the “Litigation”).

15. This IPR petitions involves the ’854 Patent, which evolved as follows. The ’531 Patent claims priority to U.S. Provisional Patent Application 71/740,731 (the “’731 Provisional”), filed December 21, 2012. At least three other patents descend from the ’531 Patent. U.S. Patent 9,954,854 (the “’854 Patent,” EX1002) is a continuation of the ’531 Patent, and also claims priority to December 21, 2012. U.S. Patent 10,749,859 (the “’859 Patent,” EX1003) is a continuation of the ’854 Patent and further claims priority to December 21, 2012. U.S. Patent 11,329,973 (the “’973 Patent,” EX1004) is a continuation of the ’859 Patent and likewise claims priority to December 21, 2012. I refer to these four patents collectively as the “Cortex Patents.” I understand that IPR petitions have been concurrently filed on

this day challenging all four Cortex Patents. I am providing supporting declarations those IPR proceedings.

16. I have been asked to assume, for purposes of these IPR proceedings only, and without offering an opinion on the point, that the claims of the four listed patents are all entitled to a Priority Date of December 21, 2012.

17. I have no financial interest in Patent Owner or the Cortex Patents. It is conceivable that I may own mutual funds whose portfolios include stock in Petitioner. If this is the case, the value of such holding would not constitute a material part of my net worth.

18. The statements made and opinions provided in this Declaration are based on my own personal knowledge and, if called as a witness, I could and would testify in a manner consistent with this Declaration.

19. In this Declaration, all emphasis has been added unless otherwise noted.

II. MATERIALS CONSIDERED

20. In forming my opinions, I have reviewed and am familiar with the '531 patent and its prosecution history, the materials cited herein, and the following exhibits to the Petition.

Exhibit No.	Description
1001	U.S. Patent No. 9,251,531 to Shaunt M. Sarkissian
1002	U.S. Patent No. 9,954,854 to Shaunt M. Sarkissian

Declaration of Michael I. Shamos
U.S. Patent 9,954,854

1003	U.S. Patent No. 10,749,859 to Shaunt M. Sarkissian
1004	U.S. Patent No. 11,329,973 to Shaunt M. Sarkissian
1006	Curriculum vitae of Michael I. Shamos
1007	U.S. Patent Application No. 13/794,878 File History
1008	U.S. Patent Application No. 14/982,981 File History
1009	U.S. Patent Application No. 16/422,715 File History
1010	U.S. Patent Application No. 16/893,023 File History
1011	Oborne U.S. Patent Pub. No. 2012/0316992(“Oborne”)
1012	Stafford U.S. Patent Pub. No. 2009/0271321 (“Stafford”)
1013	Purves et al. U.S. Patent Pub. No. 2013/0054454(“Purves”)
1014	Harris et al. U.S. Patent Pub. No. 2012/0310838 (“Harris”)
1015	Neafsey et al. U.S. Patent Pub. No. 2013/0212248 (“Neafsey”)
1016	U.S. Provisional Patent Application No. 61/598,219 (“Neafsey Provisional”)
1017	Morin et al. U.S. Patent Publication No. 2008/0270166et al. (“Morin”)
1018	First Amended Complaint (Dkt. No. 25) <i>Cortex MCP, Inc. v. Visa, Inc.</i> , No. 5-23-cv-05720 (N.D. Cal.), <i>as filed in</i> No. 6-23-cv-00048 (W.D. Tex) (Apr. 10, 2023) (“Complaint”)
1019	Steiner et al., “Kerberos: An Authentication Service for Open Network Systems.” <i>Usenix Winter</i> (1988) (“Steiner”)
1020	Cross River, “Tokenization in Card Networks” (May 2023) (“Cross River”)
1021	U.S. Patent No. 7,014,107 to Singer et al. (“Singer”)
1022	Heather Mark. “Shift4: Secure Payment Processing” (2006) (“Shift4”)

1023	Tom Arnold. “Credit Card Information Surrogate: A Method and System for using surrogates to integrate PCI-level security for legacy information systems.” (2007) (“Arnold”)
1024	Brown et al. “Microsoft Code Name ‘Geneva’ Framework Whitepaper for Developers” (2008) (“Brown”)
1025	Thakar et al. <i>PCI Compliance for Dummies</i> (2009) (“Thakar”)
1026	Ben Jackson. “Token Gestures.” <i>Digital Transactions</i> (2009) (“Jackson”)
1027	First Data. “Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance.” (2009) (“First Data 2009”)
1028	Mattson U.S. Patent Pub. No. 2009/0249082 (“Mattson”)
1029	Leach U.S. Patent Pub. No. 2010/0070754 (“Leach”)
1030	ProPay Press Release. “ProPay Adds Automated Clearing House (ACH) Data Encryption And Tokenization To Its Suite Of ProtectPay Services.” (May 10, 2010) (“ProPay”)
1031	Richard J. Sullivan. “The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy.” (2010) (“Sullivan”)
1032	CyberSource. “CyberSource Electronic Check Services Implementation Guide” (2010) (“CyberSource”)
1033	Visa. “Visa Best Practices for Tokenization Version 1.0.” (2010) (“Visa Best Practices”)
1034	U.S. Patent No. 8,458,487 to Gary Palgon et al. (“Palgon”)
1035	PCI Security Standards Council. “PCI DSS Tokenization Guidelines.” (2011) (“Tokenization Guidelines”)
1036	Shader et al. U.S. Patent Pub. No. 2011/0258122 (“Shader”)
1037	Randazza et al. U.S. Patent Pub. No. 2011/0320316 (“Randazza”)

1038	Tim Horton et al. “A Primer on Payment Security Technologies: Encryption and Tokenization.” (2011) (“First Data 2011”)
1039	Smith et al. U.S. Patent Pub. No. 2012/0016731 (“Smith”)
1040	Langley U.S. Patent Pub. No. 2012/0150669 (“Langley”)
1041	Guenther Starnberger et al. “QR-TAN: Secure Mobile Transaction Authentication.” <i>2009 International Conference on Availability, Reliability and Security</i> . IEEE. (2009) (“Starnberger”)
1042	Laracey U.S. Patent Pub. No. US 2011/0251892 (“Laracey”)
1043	Hammad et al. U.S. Patent Pub. No. 2012/0209749 (“Hammad”)
1044	Adams U.S. Patent Pub. No. 2009/0113543 (“Adams”)

21. I have also relied on my education, skill, training, and experience in the relevant fields of technology. I have further considered the viewpoint of a person of ordinary skill in the art (“POSITA”) in the subject matter of the ’513 Patent as of December 21, 2012.

22. I reserve the right to supplement my opinions as expressed in this Declaration to address any new information obtained in the course of this proceeding, or based on any new positions taken by Patent Owner.

III. SUMMARY OF OPINIONS

23. It is my understanding that the following table summarizes the grounds of challenge (“Grounds”) raised in the Petitions:

Grd.	Sec.	References	Challenged Claims
1	103	Oborne	1-17

2	103	Oborne, Neafsey	1-17
3	103	Stafford, Purves, and Neafsey	1-17

24. After a review of the '854 Patent and the prior art asserted by Petitioner, it is my opinion that the Challenged Claims are invalid under the respective Grounds. My opinions, and the bases therefor, are detailed throughout this Declaration.

IV. LEGAL PRINCIPLES

25. Counsel for Patent Owner has informed me of the legal principles that apply in this proceeding.

26. I understand that for a claim to be anticipated under 35 U.S.C. § 102, each claim element must be disclosed, either expressly or inherently, in a single item of prior art, and the claimed arrangement or combination of those elements in the claim must also be disclosed, either expressly or inherently, in that same item of prior art.

27. A prior art reference can disclose a limitation that is not expressly disclosed in the reference if it is “inherently present” in the reference. I further understand that to be “inherently present,” the missing disclosure must necessarily and inevitably be present in the element or process described in the reference. It is my understanding that a limitation is not disclosed by inherency if the missing limitation is only probably present or if there is merely a possibility that it is present.

28. Material not explicitly contained in a single prior art document may still be considered for purposes of anticipation if that material is incorporated by reference into the document. I understand that incorporation by reference provides a method for integrating material from various documents into a host document—a patent or printed publication in an anticipation determination—by citing such material in a manner that makes clear to one of ordinary skill in the art that the material is effectively part of the host document as if explicitly contained therein.

29. I understand that a claim is unpatentable for obviousness under 35 U.S.C. § 103 “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” Obviousness may be based upon a combination of references. Obviousness may be based upon a combination of references. Obviousness may also be based on a single reference combined with the knowledge of a person of ordinary skill in the art (“POSITA”) at the time the filing of the application that led to patent.

30. For a claim to be obvious in view of a combination of known elements, there must be some apparent reason to combine the known elements in the fashion of the claim at issue by considering the teachings of prior art references, the effects of demands known to people working in the field or present in the marketplace, and

the background knowledge possessed by a POSITA. Identifying a reason the elements should be combined is important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, was already known. The prior art references themselves may provide a suggestion, motivation, or reason to combine, but the nexus linking two or more prior art references is sometimes simple common sense.

31. An obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the pertinent art; and (4) any objective indicia of non-obviousness, such as commercial success, long-felt but unresolved need, failure of others, industry recognition, copying, and unexpected results.

32. Such secondary considerations include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unmet 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) the taking of licenses under the patent by others and (h) the patentee proceeded contrary to the accepted wisdom of the prior art. Secondary considerations are relevant where there is a connection, or nexus, between the evidence and the claimed

invention. I am not aware of any such objective evidence of non-obviousness of the Challenged Claims at this time.

33. In addition, I understand that the obviousness inquiry should not be done in hindsight, but must be done using the perspective of a person of ordinary skill in the relevant art as of the effective filing date of the patent claims.

34. Obviousness may also be shown by demonstrating that it would have been obvious to modify what is taught in a single piece of prior art to create the patented invention. Obviousness may be shown by establishing that it would have been obvious to combine the teachings of more than one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of one of ordinary skill in the art, the following are examples of approaches and rationales that may be considered:

(A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of a known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) Applying a technique or approach that would have been “obvious to try” (i.e., choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success); (F) 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 would have been predictable to one of ordinary skill in the art; or (G) Some 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 prior art reference teachings to arrive at the claimed invention. I also understand this suggestion or motivation may come from such sources as explicit statements in the prior art, or from the knowledge or common sense of one of ordinary skill in the art.

35. I understand that an invention that might be considered an obvious variation or modification of the prior art may be considered non-obvious if one or more prior art references discourages or lead away from the line of inquiry disclosed in the reference(s). A reference does not “teach away” from an invention simply because the reference suggests that another embodiment of the invention is better or preferred. My understanding is that for a reference to teach away the reference must clearly indicate that the combination should not be attempted (e.g., because it would not work or explicit statement saying the combination should not be made).

36. I further understand that obviousness must be determined in light of all of the facts, and that there is no rule that if a reference teaches away a finding of nonobviousness is mandated. I understand this to be the rule because, for example, a given course of action often has simultaneous advantages and disadvantages, and

thus teaching away does not necessarily obviate motivation to combine. Thus, I understand that where the prior art contains apparently conflicting teachings (for example, where some references teach the combination and others teach away from it) each reference must be considered for its power to suggest solutions to a POSITA considering the degree to which one reference might accurately discredit another. I am informed that the degree of teaching away depends upon the particular facts of each circumstance and that rigid rules that prevent the application of common sense are not mandated.

37. I further understand that obviousness also requires that a POSITA would have perceived that the proposed combination would have had a reasonable expectation of success. I am informed that reasonable expectation of success does not mean certainty of success. If a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond their skill.

38. Practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. A POSITA looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. An obviousness analysis

therefore takes into account the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

39. A proper obviousness analysis focuses on what was known or obvious to a POSITA at the time of invention, not to the patentee. Accordingly, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

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

41. I understand that in an *inter partes* review, “the petitioner shall have the burden of proving a proposition of unpatentability,” including a proposition of obviousness, “by a preponderance of the evidence.” 35 U.S.C. §316(e).

V. THE CHALLENGED PATENT

42. I understand that Petitioner is challenging all claims (1-17) of the '854 Patent in a petition for *Inter Partes* Review.

43. The Patent asserts a need for secure electronic credentials:

Additionally, as more users move to a digital transaction model, the need for digital identification also increases. As fewer users carry wallets or traditional payment forms, traditional forms of ID will become less common. Current platforms are insecure and carrying digital credentials increases the risk of identity theft or fraud in transactions. What is needed is secure system for storing and displaying user credentials. EX1002, 1:35-42

44. The Patent purports to solve this problem in a conventional manner through the following steps in claim 1:

45. [1.1] “accessing, by an officially verifiable electronic representation (OVER) file verifying device, a first OVER file stored on a first OVER file client device, the first OVER file comprising.” That is, a first party accesses an electronic representation of a credential information. This occurs every time a person uses a credit card online and was conventional.

46. [1.1.1] “a first virtual representation of an original credential of a user that has been verified by an issuing agency to be a first official representation of the original credential of the user for proving the user's identity or qualifications, based on information associated with the original credential of the user.” Electronic credit card information is “a first virtual representation of an original credential of a user that has been verified by an issuing agency to be a first official representation of the original credential of the user for proving the user's identity or qualifications,” and

the use of such information occurs every time a person uses a credit card online and was conventional.

47. [1.1.2] “wherein the first OVER file is itself a first new credential of the user.” This limitation was met every time a credit card customer obtained an electronic version of a credit card, and was conventional.

48. [1.1.3] “the first OVER file generated by an OVER engine configured to: store the information associated with the original credential of the user.” The purpose of an electronic credential is to store information associated with the original credential. This limitation was met every time an electronic version of a credit card was created for a credit card customer, and was conventional.

49. [1.1.4] “transmit the first generated OVER file to the first OVER file client device.” This limitation was met when an issuing bank transmitted an electronic version of a credit card to a customer, and was conventional.

50. [1.2] “transmitting, by the OVER file verifying device, to the OVER engine, a first verifying request to verify that the first OVER file accessed from the first OVER file client device authenticates the user.” This limitation was met, for example, when a credit card user used a credit card over the Internet. The merchant, operating an OVER file verifying device, transmitted a request to verify an electronic version of a credit card. Hence this limitation was conventional.

51. [1.3] “receiving, by the OVER file verifying device, a first authentication message comprising a first indication of whether a first scan associated with the first OVER file on the first OVER file client device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine.” That is, the merchant receives a message confirming that the credential was genuine. This limitation every time a merchant receive an authorization code for a credit card transaction, hence was conventional.

52. [1.4] “outputting a first status indicator expressing whether the first OVER file authenticates the user.” This limitation was performed in every credit card transaction when the merchant received an authorization code indicating that the user was authenticated. Hence, this limitation was conventional.

53. [1.5] “accessing, by the OVER file verifying device, a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential.” This limitation is meaningless as written. The phrase “the second OVER file is itself a second new credential over the first OVER file and the original credential” is incomprehensible because it is not

clear what it means for a “new credential” to be “over” the “original credential.” As best as I can make out, the concept behind this limitation is that the user has two OVER file client devices, each of which has an official representation of the original credential. Possibly this limitation is intended to handle the case in which the first authentication attempt fails and in which the user is asked for a second representation of the credential. Yet it is still not clear what it means for a “new credential” to be “over” the “original credential.” I believe a POSITA would understand this, conceivably to mean that the “new credential” is “preferred over” the first OVER file. If this is not what the limitation means, then I have no idea what it means. If that is what it means, this corresponds to the common case of the user being asked for a different credit card, which was conventional if the first credit card was invalid. Hence this limitation (properly understood) was conventional.

54. [1.6] “transmitting, by the OVER file verifying device, to the OVER engine, a second verifying request to verify that the second OVER file scanned at the second client device authenticates the user.” That is, the merchant asks for validation of the second credit card. This, which was common and conventional.

55. [1.7] “receiving, by the OVER file verifying device, a second authentication message comprising a second indication of whether the second scan associated with the second OVER file on the device of the user corresponds to the information associated with the original credential of the user that is stored in the

OVER engine.” This was conventional because it is the step performed when a customer used a second credit card in place of the first one.

56. [1.8] “outputting a second status indicator expressing whether the second OVER file authenticates the user.” This was conventional because it occurred when the customer presented a second credit card.

57. All of the Challenged Claims recite merely conventional steps using conventional mechanisms for their commonly intended purpose. Immediately below I offer a high-level explanation why this is true for each of the remaining Challenged Claims. Detailed explanation is given later in discussion of the relevant Grounds.

58. Claim 2 depends from claim 1, and adds that a device identifier is used to limit the credential to the OVER file storage client device. This was also conventional. As discussed below, it was conventional to use a device identifier to limit the use of a credential to a particular device for security purposes. That is, a wrongdoer or eavesdropper who somehow obtained the credential representation would be unable to use it except on the device of the authorized user.

59. Claim 3 depends from claim 1 and adds that the OVER engine comprises user-specific information. This was not only conventional, but practically universal. A credential, such as a credit card, driver’s license, passport, employee ID card, etc. typically bears the name of the holder. Indeed, the main purpose of an

identification document is to identify the holder, which requires user-specific information.

60. Claim 4 depends from claim 3 and restricts the user-specific information includes one or more of “biometric information, location information, a password, or a device identifier.” This was conventional, at least because it was common for a credential to contain a fingerprint (biometric information on an ID card) or location information (address of the driver on a driver’s license).

61. Claim 5 depends from claim 1 and adds that “the first OVER file comprises a portion of the original credential stored by the OVER engine.” This was also conventional, as it is difficult to imagine a virtual representation of a credential that would include no portion of the original credential itself.

62. Claim 6 depends from claim 1 and adds that “the first authentication message comprises an indication that the first OVER file is expired.” This was also conventional, as it was known that a merchant would receive an authentication message indicating that a credit card had expired.

63. Claim 7 depends from claim 1 and adds “accessing, by the verifying device, from the first OVER file client device, additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been satisfied.” The specification contains no disclosure of what such a “secondary condition” might be. However, it was well known in credit

card transactions that a user would have to supply “additional credential information,” such as a PIN, expiration date, ZIP code or CVV, for a transaction to be authorized. Therefore, this limitation was conventional.

64. Claim 8 is an apparatus form of claim 1 and was conventional for the same reasons.

65. Claim 9 is an apparatus form of claim 2 and was conventional for the same reasons.

66. Claim 10 is an apparatus form of claim 3 and was conventional for the same reasons.

67. Claim 11 is an apparatus form of claim 4 and was conventional for the same reasons.

68. Claim 12 is an apparatus form of claim 5 and was conventional for the same reasons.

69. Claim 13 is an apparatus form of claim 6 and was conventional for the same reasons.

70. Claim 14 is an apparatus form of claim 7 and was conventional for the same reasons.

71. Claim 15 is a computer-readable medium form of claim 1, and was conventional for the same reasons.

72. Claim 16 is a computer-readable medium form of claim 2, and was conventional for the same reasons.

73. Claim 17 computer-readable medium form combining the limitations of claims 3 and 4, and was conventional for the same reasons.

VI. LEVEL OF ORDINARY SKILL IN THE ART

74. I understand that the Board will be asked to characterize a person having ordinary skill in the art (“POSITA”) at the time the purported invention was made. To make that determination, it is my understanding that the Board considers the following factors: (i) the educational level of active workers in the field, (ii) the type of problems encountered in the art, (iii) the prior art solutions to those problems, the rapidity with which innovations are made, and (v) the sophistication of the technology in the art. It is my understanding that the importance of each factor varies from case to case.

75. The ’854 Patent defines its field of invention as follows:

The present disclosure relates to electronic transactions, and more particularly to systems, methods, and apparatuses for securely storing and displaying user credentials. EX10021, 1:20-22.

76. The Specification of the ’854 Patent (“Specification”) discloses the use of electronic credentials for virtual wallets and payment platforms for e.g., credit card payments. EX1002, 9:64-10:5.

77. The claims of the '854 Patent are drawn to generating verifiable representations of authentic credentials, transmitting the representations to a client device, and validating the representations.

78. In my opinion, in order to understand the Specification and make and use the claimed invention without undue experimentation as of December 21, 2012, one of ordinary skill in the art of the '854 Patent would have been someone with (1) a bachelor's degree in computer science or computer engineering or equivalent experience; and (2) two years' experience with electronic payment systems and/or network authentication systems involving electronic credentials.

79. I had at least the background of such a POSITA at least as early as December 21, 2012.

VII. CLAIM CONSTRUCTION

80. I understand that, in the absence of an express definition or disclaimer, claim terms are given their ordinary and customary meaning, as would have been understood by a POSITA at the time of the alleged invention.

81. In considering the meaning of the claims, however, I understand that one must consider the language of the claims in light of "the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." 37 C.F.R. § 42.100(b).

82. I provide below my understanding of the plain and ordinary meaning to a POSITA of certain terms used in the Challenged Claims.

A. “officially verifiable electronic representation”/“OVER” file

83. The term “officially verifiable electronic representation” is not a term of art. It was devised purely for use in the Cortex Patents. A Google search I conducted on January 2, 2024, for the string “officially verifiable electronic representation” produced exactly five hits (out of 400 billion documents in Google’s index¹). All five hits relate to the Cortex Patents. The term has never appeared in the technical literature, or any other place to my knowledge.

84. Each independent claim of the ’864 Patent recites an OVER file and uses the term “OVER” or “OVER file” to characterize other elements, such as an “OVER file verifying device” (a device that verifies an OVER file), and an “OVER file client device” (a device that stores an OVER file).

85. The specification of the ’854 Patent describes that an OVER file may contain “credential information.” EX1002, 6:33-35 (“OVER file containing the entered credential information”). An OVER file may also contain or act as a credential, which may in turn be representative of another credential, such as a

¹ See “Google’s Index Size Revealed: 400 Billion Docs (& Changing),” available at <https://zyppy.com/seo/google-index-size/>

driver's license. EX1002, 12:25-26 ("OVER File credential representative of the user's driver's license"). This "OVER file credential" may include an image from an issuing agency, such as a logo or a card image, and the OVER file may also include a scannable code, like a QR code. EX1002, 9:26-34, 12:26-39, 13:24-30, 14:26-29, Fig. 11 (image field 808).

86. The '854 patent does not discuss tokens or describe that tokens may be either an OVER file or a part of an OVER file (such as a representation of a credential). However, in the "First Amended Complaint for Patent Infringement and Jury Demand" (EX1018, "Amended Complaint"), Patent Owner made the following allegations:

The OVER File platform allows consumers to store credit card data and associated personal identifying information on a mobile device without the associated risk if this data is accessed by hackers. Each OVER File is a token that is unique to the user and device. The OVER File is also encrypted, which prevents the use or manipulation of data even if a hacker gains access to the device or to the file. When a customer presents an OVER File identification at a point of sale, the merchant can validate the user's credentials through an authentication application designed to interact with the token. Importantly, the technology is compatible not only with all major smartphones but also with the existing point-of-sale infrastructure used by merchants.

...

Visa makes, uses, offers for sale, and/or sells certain products (“’854 Accused Products”), including within this Judicial District, such as the VTS..

...

The ’854 Accused Products also involve a first OVER file generated by an OVER engine, which is configured to store the information associated with the original credential of the user and transmit the first generated OVER file to the first OVER file client device. The Visa Network functions as the “OVER engine.” The Visa Network includes the Token Vault, which stores the user’s original credentials and generates a token, which is transmitted to the client device.

...

The ’854 Accused Products also include instructions that cause a processor to access a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential. The second OVER file corresponds to a second OVER file client device, i.e., a second mobile phone. The second OVER

file, or token, becomes the second virtual representation to the original credentials, i.e., the user's PAN and other information.

The '854 Accused Products also include instructions that cause a processor to access a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential. The second OVER file corresponds to a second OVER file client device, i.e., a second mobile phone. The second OVER file, or token, becomes the second virtual representation to the original credentials, i.e., the user's PAN and other information.

EX1018, ¶¶9, 37, 41, 45, 46.

87. When describing the '854, which is a continuation of the '531 Patent, the Amended Complaint further equates a token to an OVER file, as well as asserting that it acts as a virtual representation of the user's credentials:

The '854 Accused Products also involve a first OVER file comprising a first virtual representation of an original credential that has been verified by an issuing agency to be a first official representation of the original credential of a user for proving the user's identity or qualifications, based on information associated

with the original credential of the user, wherein the first OVER file is itself a first credential of the user. The token (i.e., “first OVER file”) acts a first virtual representation of the user’s credentials, such as the user’s PAN.

EX1018, ¶40.

88. In light of the claim language and the disclosure in the specification of the '854 Patent, as well as Patent Owners allegations in the Amended Complaint, I interpret an OVER file as encompassing a file comprising a virtual representation in the form of an image of (or associated with) the credential, but also encompassing a file comprising a virtual representation in the form of a token.

B. “scan”

89. In contrast to the term “officially verifiable electronic representation,” the term “scan” is a term of art, and is used in its plain and ordinary meaning in the Cortex Patents.

90. The Patent discloses that there is more than one way to “interact” with an OVER File, and one of those ways is by scanning:

*The OVER File third party client 6 may allow a third party to **scan** or otherwise interact with OVER File credentials **displayed** on a user device.*

EX1002, 4:18-20.

91. That is, to be “scanned,” information must be “displayed,” i.e., in a visual form. The scan described by the ’854 patent is thus an optical scan, as it is a scan of visible information.

92. The Patent goes on to distinguish “scanning” from radio or other forms of “transmission”:

*For example, information necessary for the generation of an OVER File credential may be entered by **scanning** an information code. The information code may be represented, for example, by a **quick-response (QR) Code, standard one dimensional bar code, alpha numeric bar code (for example, Type-128), and/or other suitable information codes. The information code may be represented data sent by a radio transmission or by an electronic transmission broadcast over a network.***

EX1002, 5:19-27.

93. I note that all the examples given in the Patent of information to be scanned are visual, i.e., they are barcodes. The Patent expressly discloses NFC as another method transferring OVER File information, and distinguishes it from scanning:

*In another embodiment, the OVER File storage client may generate an information code in the form of a networked or radio transmission, such as, for example, a **Near Field Communication (NFC) or Bluetooth, or in the form of sensor***

*information, such as, for example, a bump. A credential code screen 536 **may be generated** on the user device. The credential code screen 536 may comprise a **scannable** information code 538 representative of the selected OVER File credential.*

EX1002, 12:30-39

94. That is, a code transmitted by NFC is not “scannable” by itself, but a scannable information code 538 may be **generated** from the NFC transmission.

95. However, in the Amended Complaint, Patent Owner expands the meaning of “scan” to include acts that do not constitute a “scan” as a POSITA would normally understand the term, as no display is involved:

*The '854 Accused Products also include instructions that cause a processor to receive a first authentication message comprising a first indication of whether a first scan associated with the first OVER file on the first OVER file client device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine. The user begins a transaction with a merchant **via a scan of the first OVER file at the POS terminal. The merchant POS terminal must have the ability to scan the OVER file stored in the digital wallet on the client device, such as through NFC (near-field communication) or a card reader.***

EX1018, ¶¶43.

96. The phrase “places their device near a payment terminal” includes NFC transmission, which also corresponds to the “proximity-payment request.” *See also id.*, ¶43 (“The merchant POS terminal must have the ability to scan the OVER file stored in the digital wallet on the client device, such as through NFC (near-field communication) or a card reader.”). Therefore, it is Patent Owner’s position in the Litigation that an NFC transmission of an OVER File is a “scan.” For the purposes of my analysis, I have applied an interpretation of “scan” that encompasses an optical scan (in accordance with the understanding of a POSITA), as well as encompassing an NFC interaction (as asserted in the Amended Complaint).

C. “...verified by an issuing agency...”

97. Each independent claim recites an OVER file comprising “a virtual representation of the credential that has been verified by an issuing agency to be a ... official representation of the original credential.” During prosecution of the parent application, the Applicant argued that this phrase requires that the issuing agency verify that the *virtual representation* is an official representation of the credential. *See* EX1007, 44-45 (arguing that there “is no discussion of how [prior art] electronic documents are verified by an issuing agency to be an official representation of the credential of the user”).

98. The Applicant also quoted several parts of the specification to support the meaning of this phrase. *See also id.* 40 (citing material appearing at EX1001, 3:50-4:6, 4:25-41, 5:7-25, 6:12-36). I have reproduced the passages quoted below:

"An OVER File generation and authorization engine 8 may generate OVER File credentials in response to request from an OVER File storage client 4 or an OVER File third party client 6," at [0027]. OVER Files are "representative of the user's credentials"; the "OVER File may also comprise ... any other credential that may be electronically verified by an issuing agency," at [0025]. Also, the "issuing agency database 130" may be used "for verification of the credential," at [0030]. Also, the "issuing agency datastore" may be used "to verify the information contained in the OVER File generation request and to obtain additional credential information stored by the issuing agency database 130," at [0033].

Id.

99. In light of the specification and the statements by the Applicant during prosecution, a POSITA would interpret "a virtual representation of the credential that has been verified by an issuing agency to be an official of representation the credential" to require that an issuing agency have verified a *virtual representation* in an OVER file as being an official representation of a credential.

100. I have accorded all of the claim terms their plain and ordinary meaning to a POSITA.

VIII. BACKGROUND OF THE PRIOR ART

101. In this section, I discuss the state of the art prior to the alleged invention with respect to certain technologies relevant to the subject matter of the '854 Patent as of December 21, 2012. As a POSITA is presumed to have been familiar with all relevant prior art, a POSITA would have been familiar with the material in this section.

A. Secure Credentials

102. Credentials in the physical world, sometimes referred to as identity documents, such as driver's licenses, passports and credit cards are physical objects designed to be difficult to forge or alter. Their legitimacy stems from the fact that the authority issuing them can be readily recognized by inspecting the credential itself. They also carry information to be used in verifying the identity of the person presenting the credential by means of a "challenge." For example, passports and driver's licenses carry a photograph of authorized holder. The "challenge" consists of having the holder exhibit their face. If the face matches the photograph on the credential, then the presenter is known to be the authorized holder. A credit card carries the signature of the authorized holder. In the case of a credit card, the "challenge" is requiring the presenter to sign a receipt. If the signature on the receipt matches the signature on the credit card, the presenter is believed to be the authorized cardholder.

103. Creating identity documents in the digital world was challenging for several reasons: (1) it was not easy to determine if a digital credential was issued by a recognized authority; (2) a digital credential can easily be copied, forged, or altered and it is difficult to issue a “challenge” to a remote networked user to prove that they are the person named in the credential. An eavesdropper who obtains both the credential and the answer to the challenge can later pretend successfully to be the person named in the credential.

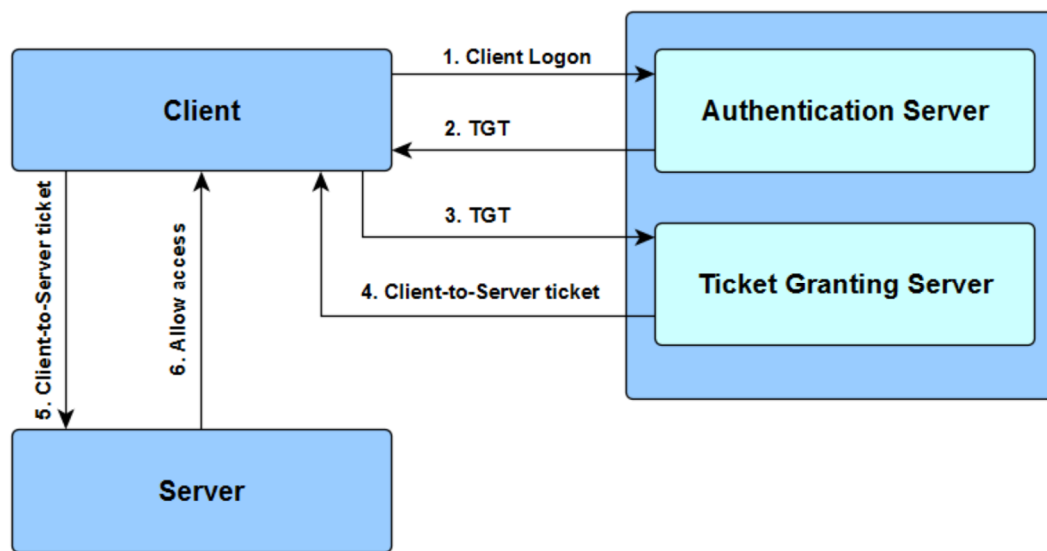
104. These problems were recognized and solved long before the Patent. A solution to (1) is to have the issuer include some encrypted material in the credential that only the true issuer is able to generate, e.g., a digital signature. Digital signatures have been known since 1976. Another solution to (1) is to have the issuer verify over a network in real-time that the credential is valid. This has commonly been done in everyday credit and debit card transactions since 1973. When a customer presents a credit card to a merchant, the merchant makes a request in real-time whether the card is valid and whether the card has sufficient credit to cover the transaction. The request is routed to the bank that issued the credit card, and a response is received within 5-15 seconds. Such requests were originally made over private dial-up networks maintained by credit card agencies, such as Visa, and were later made (at least partially) over the Internet. Note that solving (1) validates the credential, but

does not prove that the presenter of the credential is the person named in the credential.

105. A solution to (2) is to require the presenter of the credential to furnish additional information to prove that they are the person named in the credential. This protects against credentials being copied or stolen. In the banking industry, this was done starting in 1967 by requiring the user to enter a PIN at an ATM machine. A thief who stole an ATM card would not be able to use it without knowing the PIN. PINs are still used in the credit/debit card industry even though embedded chips and NFC communication have replaced magnetic stripes.

106. The problem of remote authentication of a user over a network was solved at MIT in the 1980s using a mechanism called “Kerberos.” *See* EX1019. Fundamentally, users need access to various resources on a network such as documents and network services. It is impractical to require every server on a network to maintain a database containing encrypted passwords of every authorized user and to force users to enter a username and password each time they request a document or service. The Kerberos solution was to maintain a single server (the Authentication Server) storing usernames and passwords, analogous to the OVER engine of the Patent. The Client seeking network services would authenticate themselves once to the Authentication Server using the traditional username/password process. The Authentication Server then generates a ticket-

granting ticket (TGT) and sends it back to the Client. When the Client wants to access a Server, it requests a ticket for that particular server from a Ticket Granting Server. To do so, the Client must send the TGT and the identity of the desired Server. The Ticket Granting Server then sends to the Client a Client-to-Server Ticket, which, when presented to the Server by that Client, will authenticate the Client to the Server and the Server will perform services for the Client. The process is shown in the diagram below, which is not from EX1019, but accurately reflects the Kerberos process.



107. It can readily be seen that the Authentication Server and the Ticket Granting Server correspond to the OVER engine of the Patent. The Client-to-Server Ticket corresponds to the OVER File of the Patent. The Server corresponds to the third-party client verifying device of the Patent. Step [1.6] of the Patent, “receiving, from an OVER file third-party client verifying device, a verifying request to verify

that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file storage client device of the user,” is not literally present in the diagram because the OVER file is sent from the Client to the Server along with the request for service and no “scan” is performed. Instead, the Over File itself is transmitted to the Server. Step [1.7] of the Patent is also not literally present in the diagram because (1) there is no “scan”; and (2) the claimed “authentication message” is actually contained in the initial request to the Server. For these reasons, Kerberos does not anticipate any Challenged Claim. However, it will readily be recognized that the Client-to-Server Ticket of Kerberos is a “token” corresponding to the user’s original credential (username/password) maintained on the Authentication Server.

108. Thus, by December 21, 2012, there was nothing inventive using a secure credential for authentication.

B. Tokens

109. The use of a surrogate or “token” in place of an actual credit card number or other credential was a well-known security practice long before the Patent. It was long known that fraud can occur if an unauthorized party obtains a user’s credit card number. Unfortunately, in older credit card transactions, there was no way to prevent the merchant itself from obtaining the user’s credit card number,

as the merchant had to present that number to a credit card network in order to be paid.

110. In 2001, the idea of token was introduced by the company TrustCommerce, which replaced the credit card number (primary account number or “PAN”) with a randomized number, called a token. *See* EX1020. When a merchant needed to process a payment, it could use the associated token and TrustCommerce would process the payment on their behalf, replacing it with the true credit card number before introducing the transaction into the credit card network. In this manner, the merchant never learned the user’s credit card number. In such systems, the credential itself was stored remotely from the token and would not be transmitted with the token. Thus a wrongdoer who somehow obtained the token would not gain any information about the credential itself.

111. On July 20, 2004, Singer at al. filed an application that became U.S. Patent 7,014,107 on March 21, 2006, entitled “Wireless Payment Processing System” (“Singer,” EX1021). It discloses a tokenization process for making credit card payments, as shown in its Fig. 1., below:

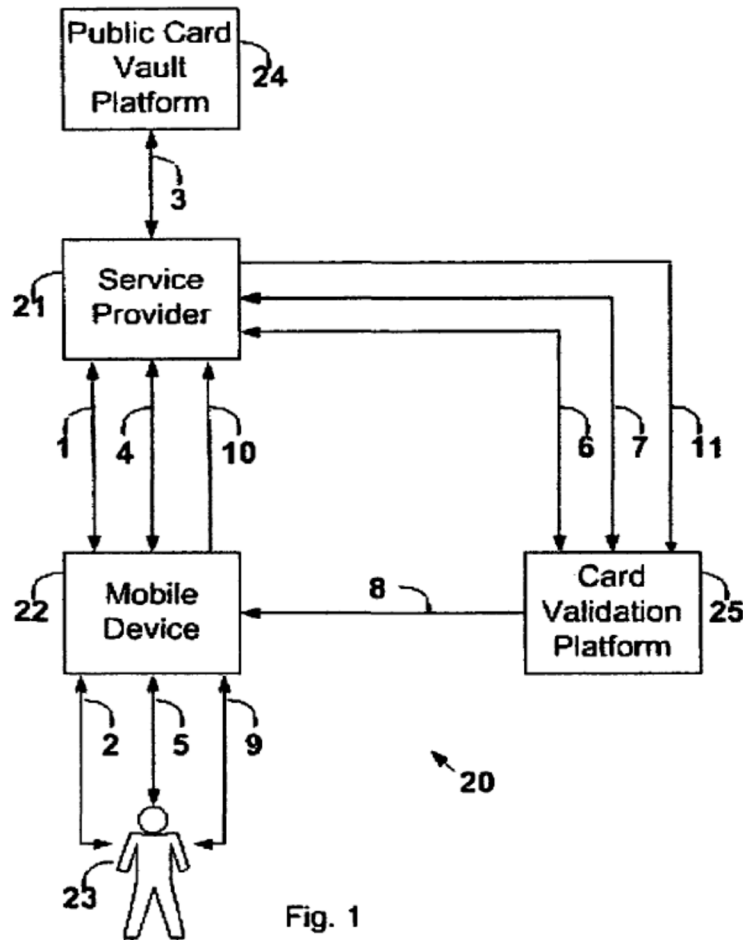


Fig. 1

112. The Card Owner 23 wishes to make a payment to Service Provider 21 from Mobile Device 22 but does not want the Service Provider to learn the credit card number. Singer discloses that the communications between Mobile Device 22 and Service Provider 21 are close-range, using Bluetooth. As described at 2:33-3:57, the process starts when 21 sends message 1 to 22 requesting a credential. The credential can be a password, PIN or biometric of the Card Owner. The device 22 sends to 21 the credential and an identifier of the Mobile Device.

113. Service Provider 21 then sends the credential and identifier to Public Card Vault Platform 24. This is a repository of names of credit card holders along with their identifiers and credentials and incomplete information about their credit cards (e.g., the last two digits of each card number and a card name). Platform 24 sends to 21 the available cards for the Card Owner, which 21 then sends to Mobile Device 22. The Card Owner then selects one of the cards for payment and the selection is passed to Service Provider 21. The Service Provider 21 then requests a preauthorization for the selected card by sending a message 6 to the Card Validation Platform 25 that includes the credential, identifier, and incomplete card data. The Card Validation Platform contacts the issuing bank (not shown in the drawing) to validate the selected card. If the card is validated, the Platform 25 generates a temporary card token and sends it back to the Service Provider 21. The purpose of the preauthorization is to confirm that the card is valid.

114. Service Provider 21 returns the temporary card token to Platform 25 along with a transaction amount. Platform 25 obtains an authorization from the issuing bank for that transaction amount and also receives an authorization token containing a public part and a private part. Platform 25 then sends 21 the public part of the authorization token and a check digit of the private part of the authentication token. Platform 25 sends a text message to Mobile Device 22 along with the card token and the private part of the authorization token.

115. The Card Owner 23 is then asked whether or not to authorize the payment. If so, Mobile Device 22 sends the Service Provider the card token and the private part of the authorization token. In order to receive payment, the Service Provider 21 sends the card token along with the (now complete) authorization token to the Card Validation Platform 25, which then processes the payment through a credit card network.

116. Singer discloses the use of a card token and proximity transmission between the Card Owner's Mobile Device and the Service Provider. The process of Singer was rather clumsy and was refined by the industry in the ensuing years.

117. Shift4 Corporation released a system to the public during an industry Security Summit in Las Vegas, Nevada in 2005. In a 2006 manual, Shift4 defined tokenization as a "term used to describe the replacement of the card number used in transactions processing with a Token. The Token is a unique identifier comprised of a 16-character, alphanumeric code that is used to reference sensitive cardholder data. In keeping with PCI, as well as the legal requirements of the FACT Act, the Token contains only the last four digits of the card number. The last four digits of the account number become the first four in the Token. Spaces 5-16 are random characters that are globally unique to that transaction." *See* EX1022. The abbreviation PCI in the preceding quote refers to the Payment Card Industry, which developed standard for handling credit card transaction data.

118. On March 1, 2007, Arnold published “Credit Card Information Surrogate: A Method and System for using surrogates to integrate PCI-level security for legacy information systems.” *See* EX1023. It discloses “a method and system for assignment of a consumer credit card surrogate, based on card account number issuing methods.” *Id.* at. 1. (A “surrogate” is another word for “token.”) It continues, “For protection of credit card data, to help educate and expose some of the issues with card account surrogate (vendors sometimes refer to a tokenization) systems that are offered from payment gateway and software vendors.: *Id.* at 3. Further, “Surrogate Implementation. The Data Vault implements the generation and storage of surrogates at the time an initial authorization is run on a credit card. The surrogate is stored in the vault with the encrypted and salted-SHA1 of the card account number. If a card transaction comes into the payment application where the card account number begins in a 9, payment application knows to ask the Data Vault to exchange the surrogate for the actual account number. The payment application then proceeds to process the transaction as though any normal payment request.” *Id.* at 10.

119. In 2008, Microsoft unveiled its “Geneva” Framework for authenticating credentials securely over networks. *See* EX1024. It discloses at pp. 6-7:

Security Token. *The user delivers a set of claims to your application piggybacked along with her request. In a web service, these claims are carried in the security header of the SOAP envelope. In a browser-based web application, the claims arrive via an HTTP POST from the user's browser, and may later be cached in a cookie if a session is desired. Regardless of how they arrive, they must be serialized somehow, and this is where security **tokens** come in. A security **token** is a serialized set of claims that is digitally signed by the issuing authority. The signature is important – it gives you assurance that the user didn't just make up a bunch of claims and send them to you.*

Issuing Authority. *There are lots of different types of issuing authorities, from domain controllers that issue Kerberos tickets, to certificate authorities that issue X.509 certificates, but the specific type of authority I'll be talking about in this paper issues security **tokens** that contain claims. The issuing authority I'm speaking of is a web application or web service that knows how to issue security **tokens**. It must have enough knowledge to be able to issue the proper claims for the target relying party given the user making the request, and may be responsible for interacting with user stores to look up claims and authenticate the users themselves.*

Security Token Service (STS). *A security **token** service (STS) is the plumbing that builds, signs, and issues security **tokens** according to the interoperable protocols that I'll discuss in the upcoming section called Standards. There's a lot of work that*

goes into implementing these protocols, but Geneva Framework does all of this heavy lifting for you, making it feasible for someone who isn't an expert in the protocols to get an STS up and running with very little effort.

120. Microsoft's Geneva was a very general system for remote authentication using tokens that was not limited to online payments.

121. Naturally, the PCI was interested in payment security, so it developed tokenization standards. In 2011, Thakar et al. published "PCI Compliance for Dummies" (EX1025) to help explain these standards. It discloses on p. 28: "The goal of protecting cardholder data is at the heart of PCI. Various technical methods of protecting cardholder data exist, such as encryption, tokenization, truncation, masking and hashing. But you don't have to be a tech guru to understand their purpose: to make cardholder data *unreadable* to unauthorized people." (emphasis in original). Further on p. 37: "For all remote access to the network, you need to implement two-factor authentication. The standard suggests using a remote authentication and dial-in service, a terminal access controller access-control system with tokens, or a virtual private network (VPN) with individual certificates."

122. Later in 2009, the call for tokenization grew. In May 2009, the trade magazine *Digital Transactions* published an article by Ben Jackson entitled "Token Gestures" (EX1026), which discloses:

*With no end in sight to the rash of data breaches, the concept of replacing card data with so-called **tokens** is catching on.*

*Broadly, **tokens** work as follows: A merchant hires a company that takes the card number from its system and returns a **token** that the merchant uses for its records. The **token** acts as an index or reference number that the vendor could use to look up the actual information. The **token** vendor then sends the actual card number to the processor and authorizing bank.*

*The **tokens** help large enterprises because once they replace credit card numbers with **tokens**, companies can share data across different business units without needing to create PCI protections in each unit. The **tokens** contain the last four digits of a credit card number so that companies can use them for analysis and customer relationship services.*

123. In September 2009, First Data, a large credit card processor, publishes a whitepaper entitled, “Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance” (EX1027). “DSS” refers to the Data Security Standard. The whitepaper discloses on p. 12:

*“**Tokenization** of sensitive data. An increasingly popular approach for the protection of sensitive data is the use of a token (or alias) as a substitute for a real credit card number. In the process of **tokenization**, a payment card is used in a transaction and, once authorized, the cardholder data is sent to a centralized*

*and highly secure server called a “vault,” where it is stored securely. Immediately after, a random unique number is generated and returned to the merchant’s systems for use in place of the cardholder data. The end result is that the **token** can be used in various business applications as a reliable substitute for the real card data.*

124. On October 1, 2009, Mattsson U.S. Patent Application Publication 2009/0249082, was published, entitled “Method and Apparatus for Tokenization of Sensitive Sets of Characters” (“Mattsson,” EX1028) It discloses at [0105]:

***Tokenization** is often based on two key facets in an enterprise: First-Centralization of sensitive information. All credit card numbers stored in disparate business applications and databases are removed from those systems and placed in a highly secure, centralized encryption management server that can be protected and monitored utilizing robust encryption technology. **Tokenization** is like network segmentation, as a way to move card data to another internal or external server. However, the access to the card data is still in your POS or other systems, so be careful of how a **tokenized** system can be attacked. Secondly, **tokenization** of information. Each credit card number that previously resided on an application or database is replaced With a **token** that references the credit card number. A **token** can be thought of as a claim check that an authorized user or system can use to obtain the associated credit card number.*

125. The Mattsson theme was followed on March 18, 2010, with Leach U.S. Patent Application Publication 2010/0070754, entitled “Payment Encryption Accelerator” (“Leach,” EX1029). Its Abstract discloses:

*Embodiments of the invention provide a system for encrypting web session data which may include a session management module adapted to receive data from a web application module and provide a **token** that represents the data in encrypted form to the web application, wherein the web application is adapted to use the **token** to represent the data. The system may also include a **tokenizer** module communicably coupled to the session management module, wherein the **tokenizer** module is adapted to receive the data and generate the **token**. Further, the system may include a database communicably coupled to the session management module, wherein the database is adapted to receive the **token** and the data, associate the **token** with the data, and store the **token** and the data.*

126. On October 29, 2009, Stafford U.S. Patent Application Publication 2009/0271321 was published, entitled “Method and System for Verification of Personal Information” (“Stafford,” EX1012). Its Abstract discloses:

In one form, there is disclosed a system (100) for storing, validating and disseminating credential information about an entity. The system (100) generates data representing at least part of the credential information and a data representation of at least part of a document supporting that information and stores the

*credential information and data representation in a database
(120) in an encrypted form.*

127. Stafford's system receives and stores credential information, including scans of credentials, and distributes sensitive credential information to third parties using key signatures to unlock their release. EX1012 at [0010] ("Receiving a document including credential information about an entity; Verifying at least part of the credential information included in the document; Generating data representing at least part of the credential information; Generating a data representation of at least part of the document; and Storing at least part of the credential information and data representation in a database in an encrypted form."), [0062] (scanning credential documents), [0073]-[0075] ("Preferably sensitive information can only be released...after confirmation by the entity as well as the generation (and purchase) of key signatures."), [0093]-[0097] (providing key signatures), [0107]-[0125] (releasing credential information), Figs. 2-3.

128. Stafford also refers to a "token" for holding credential information, but the "token" of Stafford is a physical device that does not correspond to the "tokens" accused by Patent Owner to be virtual representations of credentials. Hence I make no further reference to the physical tokens of Stafford. The OVER files of the '854 Patent correspond instead to Stafford's encrypted credential information, which pertains to an "entity," which may be an individual.

129. Stafford's credential information is verified:

*In a third aspect the present invention provides a system for providing credential information about an entity, the system including: a database storing, encrypted verified entity characteristic data relating to the entity, said verified entity data including, a representation of at least part of a document attesting to one or more characteristics of the entity, data representative of said one or more characteristics of the entity; and entity identification data associated with the **encrypted verified entity characteristic data**.*

Id. at [0024].

130. On May 10, 2010, ProPay issued a press release (EX1030) containing the following:

*Lehi, Utah – May 10, 2010 – On the heels of winning the 2010 ETA ISO of the Year Award ProPay (www.propay.com), an industry leader in End-to-End Payment Security, credit card processing, and electronic payment services, announced today that is has added encryption and **tokenization** of Automated Clearing House (ACH) data (bank routing and account numbers) to its suite of ProtectPay services. The addition of this functionality illustrates ProPay's proactive approach to helping organizations protect sensitive data.*

131. By that time, the importance of tokenization had become apparent to the Federal Reserve Bank, which published a whitepaper by Sullivan entitled "The

Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy” on May 21, 2010 (EX1031). It discloses on p. 16:

*Another initiative disguises a card account number by replacing it with a **token** number. This “**tokenization**” would occur after a card payment has been authorized so that a merchant can store the transaction information without having to store the card account number (Taylor). Merchants can retrieve the card account number for later processing, if needed. Both of these options could make merchant and processor computer networks less of a target because they would not store or transmit sensitive payment card information in forms that would be useful to hackers.”*

132. Also in May 2010, CyberSource issued a manual on how to implement tokenization, entitled “CyberSource Electronic Check Services Implementation Guide” (“CyberSource,” EX1032). It discloses on p. 62:

***Payment Tokenization.** If you are using Payment **Tokenization**, you can process a debit or credit by using information that is stored in a customer profile. CyberSource uses the subscription ID to reference the customer profile information in the CyberSource database. Instead of providing all the information that is normally required for a transaction, you only need to provide the following values:*

- *Merchant ID*
- *Merchant reference code*

- *Amount of the payment or credit*
- *Subscription ID*

133. On July 14, 2010, Petitioner Visa published “Visa Best Practices for Tokenization Version 1.0” (EX1033). It discloses on p. 1:

*How **Tokenization** Works. **Tokenization** defines a process through which PAN data is replaced with a surrogate value known as a “**token**.” The security of an individual **token** relies on properties of uniqueness and the infeasibility to determine the original PAN knowing only the surrogate value. As a reference or surrogate value for the original PAN, a **token** can be used freely by systems and applications within a merchant environment. Where properly implemented, **tokenization** allows merchants to limit the storage of cardholder data to within the **tokenization** system, potentially simplifying an entity’s assessment against the PCI DSS. As a reference or surrogate value for the original PAN, a **token** can be used by systems and applications within a merchant environment without having to consider the security implications associated with the use of cardholder data.*

134. On March 3, 2011, Palgon et al. filed an application that matured into U.S. Patent 8,458,487, entitled “System and Method for Format Preserving Tokenization of Sensitive Information” (EX1034). Its Abstract discloses:

Systems and methods for secure access and utilization of sensitive data such as credit card numbers, Social Security

*Numbers, personal identifying information, etc. A tokenizing strategy component provides for creating, managing, and storing **tokenization** strategies on behalf of a plurality of users. A data **tokenizing** component is operative to (a) receive an input data string of sensitive data from a user, (b) apply a selected **tokenization** strategy to the input data string to generate a **tokenized** data string, and (c) provide the **tokenized** data string for storage in association with the input data string. A secure server including a secure database stores the **tokenized** data string and the input data string in a corresponding mapped relationship.*

135. Tokenization was adopted by the PCI, which established a Tokenization Taskforce. In August 2011, it published “PCI DSS Tokenization Guidelines” (EX1035) to supplement Version 2.0 of the PCI Data Security Standard. It explains different ways of generating tokens, stating:

*One of the primary goals of a **tokenization** solution should be to replace sensitive PAN values with non-sensitive **token** values. For a **token** to be considered non-sensitive, and thus not require any security or protection, the **token** must have no value to an attacker. **Tokens** come in many sizes and formats. Examples of some common **token** formats are included in the following table.*

Table 1: Selected Examples of Token Formats*

PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cw15x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

* **Note:** This table provides a selection of examples only, and does not include all possible token formats.

EX1035, p. 5

136. The Tokenization Guidelines go on to explain the difference between single-use and multi-use tokens:

***Tokens** can be generally identified as either single-use or multi-use. A single-use **token** is typically used to represent a specific, single transaction. A multi-use **token** represents a specific PAN, and may be used to track an individual PAN across multiple transactions. A multi-use **token** always maps a particular PAN value to the same **token** value within the **tokenization** system. Determining whether single-use or multi-use **tokens**, or a combination of both, are appropriate for a particular merchant environment will depend on the merchant's specific business need for retaining tokens.*

EX1035, p. 5

137. Further at p. 9:

1. *The requesting application passes a **token**, along with necessary authentication information, to a **tokenization** system.*
2. *The **tokenization** system verifies the authentication information presented by the requesting application. If this check fails, the **de-tokenization** process fails, and information is logged for monitoring. Otherwise, the process continues to Step 3.*
3. *The **tokenization** system queries the card data vault for a record associated with the **token**, retrieves the PAN if found, and proceeds to Step 4. If no such **token** exists, the de-tokenization operation fails, and information is logged for monitoring.*
4. *The **tokenization** system returns the PAN value retrieved from the card data vault, if found, to the requesting application. If the PAN is not found, then an error message is returned.*

138. On October 20, 2011, Shader et al. U.S. Patent Application Publication 2011/0258122, entitled “Payment System to Facilitate Transactions,” was published (“Shader,” EX1036). Its Abstract reads:

*Disclosed herein are systems and method for facilitating transactions between a merchant-partner and a customer. In general, the systems and methods include: (a) staging a transaction between the merchant-partner and the customer; (b) **tokenizing** the transaction by linking one or more transaction instructions to a **token ID**; (c) providing the customer with the **token ID**, wherein the customer can then present the **token ID** and a payment to a point-of-sale terminal; (d) receiving*

*confirmation that the customer has presented, to a point-of-sale terminal, the **token** ID and a payment in accordance with the one or more transaction instructions; (e) notifying the merchant-partner that the customer provided the payment to the point-of-sale terminal; and (f) settling the transaction between the point-of-sale terminal and the merchant-partner.*

139. On December 29, 2011, Randazza et al. U.S. Patent Application Publication 2011/0320316, entitled “Payment System and Methods” was published (“Randazza,” EX1037). It contains the following disclosures:

*Examples of a payment **token** useable in the invention include, e.g., a driver's license card or other physical card, an electronic **token**, a **token stored in a mobile payment device, a cellular device, a smart phone**, a wireless device, a handheld electronic device; a personal digital assistant; etc. Preferably the payment **token** is not a card with a magnetic stripe or bar code conventionally used to conduct a debit or credit card transaction by a financial institution or third party processor for financial settlement of funds due a retailer. Id. at [0047]*

*In another preferred embodiment, the invention provides a method for a system having a plurality of persons; a plurality of payment **tokens** issued under authority of an entity (such as, e.g., Apple; AT&T; etc.); a retail site configured with a first signal, the first signal being common to the plurality of payment **tokens**; a routing system for receiving a signal and generating a network address in response to the received signal, the routing system*

*including a plurality of wide area communication links, the routing system being configured using the first signal, the system further including a second signal on a first payment token in the plurality of payment **tokens**; and a second system storing an association between the second signal and account information, the entity and an owner of the second system not being affiliated, the entity not being affiliated with a retailer, method comprising the steps, performed at the retail site, of: receiving the first and second signals from the first payment **token**; sending the first and second signals into the routing system, to cause the second system to perform the steps of determining whether the first payment **token** can effect payment; responsive to the determining step, conditionally sending a message to cause an institution to send an ACH entry to the Federal Reserve ACH system, to pass the entry to a bank, where an account is issued a debit, to cause a transfer of funds to the owner of the retail site, and making an entry in an accounting system, to effectively increment an amount owed by the owner of the retail site to the owner of the second system; wherein the method further includes the step, performed at the retail site, of: conditionally effecting a transaction with a holder of the first payment **token**, depending on a signal received from the second system. *Id.* at [0022]*

140. In 2011, First Data published “A Primer on Payment Security Technologies: Encryption and Tokenization” (EX1038). It discloses on p. 5:

***Tokenization.** An increasingly popular approach for the protection of sensitive data is the use of data substitution with a*

***token** (or alias) as a replacement for a real credit card number.*

*In the process of **tokenization**, actual cardholder data is used in a payment transaction and, once the transaction is authorized, this very sensitive data is sent to a centralized and highly secure server called a “vault” where it is stored securely. At the same time, a random unique number is generated and returned to the merchant’s systems for use in place of the cardholder data. The vault manager maintains a reference database that allows the **token** number to be exchanged for the real cardholder data if it is needed again for, say, a chargeback. Meanwhile the **token** number, which cannot be monetized, can be used in various auxiliary business applications as a reliable substitute for the real card data.*

141. By 2012, tokenization was becoming widespread. On January 19, 2012, Smith et al. U.S. Patent Application Publication 2012/0016731, entitled “Mobile System and Method for Payments and Non-Financial Transactions” (“Smith,” EX1039) was published. It discloses at [0027]:

*The e-wallet is consumer centric because it enables consumers to upload all types of card accounts to the e-wallet. The e-wallet is a service provided by the TPPN (third Party payment network or gateway provider for mobile payment services) and may be a customized e-wallet solution for the mobile payment system. The CMA has ability to select the **tokenized** payment method data used by the TAS for calling the TPPN's e-wallet according to he [sic] corresponding **token** and card account of the user.*

142. On February 13, 2012, Neafsey et al. filed provisional application 61/598,212 (“Neafsey Provisional,” EX1016). Subsequently, an application claiming priority to the Neafsey Provisional was filed on February 13, 2013, which published on August 15, 2013, as U.S. Patent Application Publication 2013/0212248 (“Neafsey,” EX1015) entitled “Credential Management System”.

143. I understand that the disclosure in Neafsey is available as prior art as of the filing date of the Neafsey Provisional insofar as the same subject matter is disclosed in the Neafsey Provisional and the Neafsey Provisional provides written description support for at least one claim in Neafsey. As I discuss below, the Neafsey Provisional supports at least claim 1 of Neafsey. I illustrate that the same subject matter is present in both Neafsey references by providing citations to the matching disclosure in both references throughout the remainder of my declaration.

144. Claim 1 of Neafsey recites the following:

[Preamble] A method, comprising:

[1.1] providing, with at least one server, a cloud credential management service including generating credentials of at least two different types;

[1.2] receiving, with the server, a credential request from a customer computer to assign a virtual credential to a mobile device;
and

[1.3] transmitting, with the server, the virtual credential to the mobile device.

145. Below, I illustrate that the Neafsey Provisional discloses a method including each of these claim limitations.

146. **Preamble**: The Neafsey Provisional discloses embodiments including “apparatuses, systems, devices, hardware, methods, and combinations for credential management services.” EX1016, 2; *see also id.*, claims 1-14, 18 (each reciting a method).

147. **Neafsey Step [1.1]**: The Neafsey provisional discloses “providing, with at least one server, a cloud credential management service including generating credentials of at least two different types.” For example, the Neafsey provisional discloses that “[g]enerally, a provider makes the cloud credential management service 102 available to one or more customers over the Internet.” EX1016, 5; *see also id.*, Fig. 1. The cloud credential management service includes credentials of at least two different types. *See* EX1016, 11-12 (“[D]ifferent types of credentials may be generated and hosted in a cloud credential management service 504. There are credentials of different types...and each credential type has distinct algorithms...”); *see also id.*, 12 (“Virtual credentials 502 can be generated by the cloud credential management service 504 in multiple formats (e.g., prox, Mifare, EVI, optical, XceedID, eISA) depending on the requesting host.”), Fig. 9.

148. **Neafsey Step [1.2]**: The Neafsey provisional discloses “receiving, with the server, a credential request from a customer computer to assign a virtual

credential to a mobile device.” For example, Neafsey discloses that “Virtual credentials 502 can be generated by the cloud credential management service 504 in multiple formats...depending on the requesting host.” EX1016, 12. By “requesting host,” the Neafsey Provisional is referring to a customer’s computing device, such as a mobile device, that has requested to be assigned a virtual credential. *See* EX1016, 8 (“FIG. 4 illustrates a cloud credential management service 308 that transmits virtual credentials 302 to a credential host 310, such as a mobile device.”), 4 (“The mobile device 104 may be a mobile phone, such as a cell phone or smartphone, a tablet computer, such as an iPad, a smartcard, or any other type of mobile computing device.”).

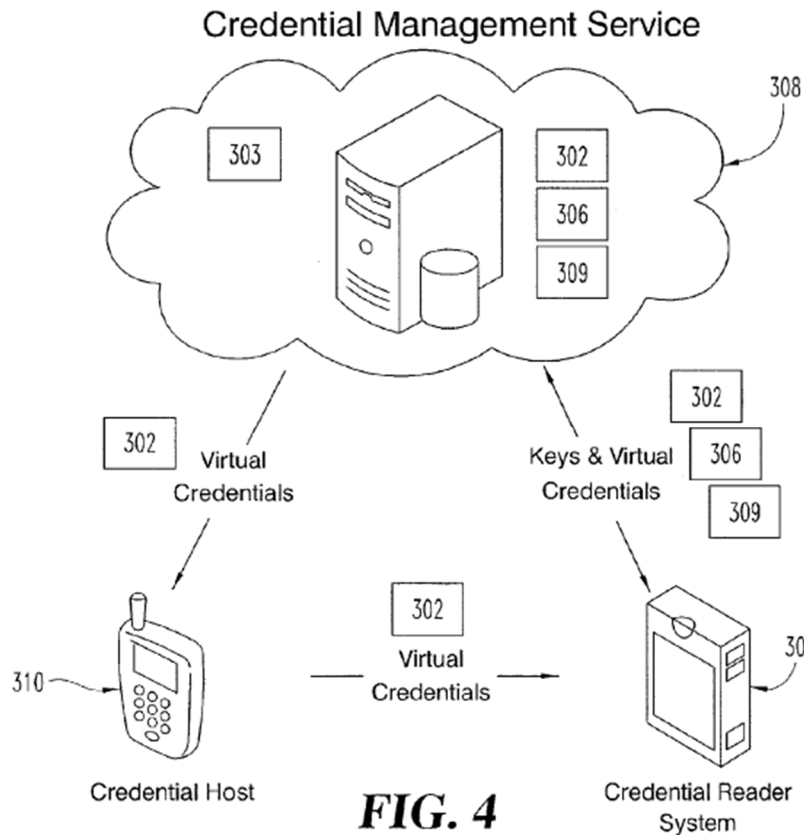
149. **Neafsey Step [1.3]**: The Neafsey provisional discloses “transmitting, with the server, the virtual credential to the mobile device.” For example, the Neafsey provisional teaches that the requested credentials are “hosted and delivered via a mobile device such as a smartphone.” EX1016, 12; *see also id.*, 4 (“The cloud credential management service 102 may generate and deliver credentials 110 to the mobile devices 104, reader devices 106, and other devices such as computers 108.”), Fig. 9 (showing transmission of different types of requested credentials to mobile devices). Accordingly, the Neafsey Provisional discloses Neafsey Limitation 1.3.

150. As I have shown above, the Neafsey Provisional provides a written description of each limitation of claim 1 of Neafsey. The following claim chart

summarizes the locations of relevant support for each limitation of claim 1 of Neafsey:

US20130212248	US61/598,219
1. A method comprising:	EX1016, 2, claims 1-14, 18.
providing, with at least one server, a cloud credential management service including generating credentials of at least two different types;	EX1016, 5, 11-12, Figs. 1, 9.
receiving, with the server, a credential request from a customer computer to assign a virtual credential to a mobile device; and	EX1016, 4, 8, 12.
transmitting, with the server, the virtual credential to the mobile device.	EX1016, 4, 12, Fig. 9.

151. Fig. 4 of Neafsey shows a credential management system in which virtual credentials are issued to a mobile device 310 for presentation to a credential reader 304:



EX1015, Fig. 4; EX1016, Fig. 4.

152. Neafsey also discloses that the credential may include a “unique device identifier” along with a token:

*Once authenticated, at operation 326, the credential host 310 then requests to be enrolled with the credential management service 308 by sending a request along with a specifier such as a **unique device ID**.*

EX1015, [0048]; EX1016, 10.

*At operation 412, the device 402 then sends a **unique device identifier** to the credential management service 406 along with the token.*

EX1015, [0056]; EX1016, 11.

153. Neafsey discloses a credential in the form of a QR code:

*Virtual credentials 502 can be generated by the cloud credential management service 504 in multiple formats (e.g., prox, MIFARE Classic, MIFARE DESFire EV1 [sic, EV1], optical, XceedID [sic, XceedID], elSA, bar code, **QR code**) depending on the requesting host.*

EX1015, [0061]; EX1016, 12.

154. The foregoing passage also discloses sending credentials to different devices in device-specific formats.

155. Neafsey also discloses the “status indicator” of the ’854 Patent as an “authentication status,” for example:

*Process 311 then proceeds from operation 312 to operation 314. At operation 314, the cloud credential management service 308 transmits an **authentication status**, which may include a **token**, to the reader system 304.*

EX1015, [0042]; EX1016, 10.

156. Neafsey is an obviousness reference discussed in more detail beginning at ¶268.

*telecommunications, the server 108 may identify an associated account and encrypt the requested account data by virtue of generating a virtual machine-readable **token** 804 at step 310. Once the virtual machine-readable **token** 804 is generated, it may be transmitted at step 315 to the requesting CPCD 102B.*

*[0091] The CPCD 102B receives the virtual machine-readable **token** 804 at step 320. In step 325, the CPCD 102B renders and presents the virtual machine-readable **token** 804 to a MPCD 102C for payment as illustrated in FIG.1. In some embodiments, one or more of the previously-described steps of 305-315 may take place at the time when the CPCD 102B is being used to offer payment to obtain the virtual machine readable **token** 804.*

160. On June 7, 2012, an application was filed that was published on December 13, 2012, as Osborne U.S. Patent Application Publication 2012/0316992 (“Osborne,” EX1011), entitled “Payment Privacy Tokenization Apparatuses, Methods and Systems.” These apparatuses, methods and systems are referred to in Osborne as “PPT.”

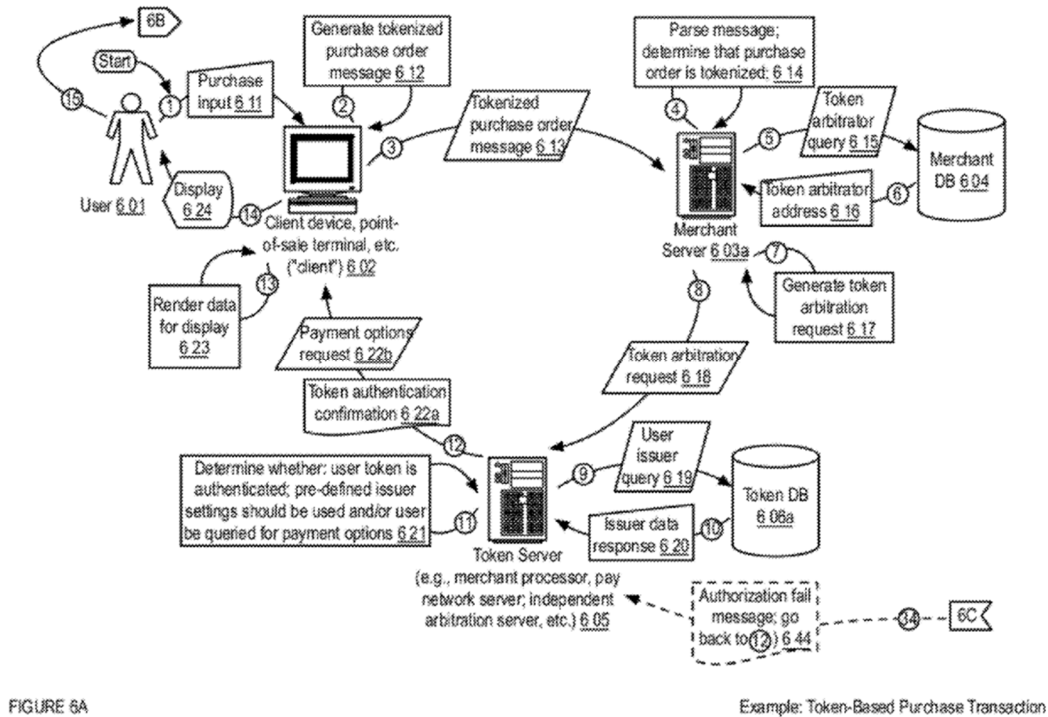
161. The Abstract of Osborne states:

*In one embodiment, the PPT obtains a **token** arbitration request including unique source-neutral universally-resolvable payment **token** information from a merchant for processing a purchase order from a user. The PPT queries a **token** database for issuer information on an issuer using the payment **token***

information, and obtains the issuer information. The PPT also determines that the user should be queried for payment options based on the issuer information, and provides a payment options request to a user mobile device. Upon obtaining a response from the mobile device, the PPT generates a purchase authorization request based on the payment options and pre-defined settings for issuers to be contacted for processing the purchase order, and provides the generated purchase authorization request to the issuer.

162. Osborne discloses tokenization and communication of an OVER file using NFC, which Patent Owner considers a “scan,” and by QR code, which surely is a “scan.”

163. Fig. 6A from Osborne is reproduced below. It depicts an in-store tokenized purchase by a User 6.01, who interacts with a merchant’s point-of-sale terminal 6.02.



164. As described at [0048]:

The user may communicate with a merchant server, e.g., 603a, via a client such as, but not limited to: a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, and/or the like (e.g., 602). For example, the user may provide user input, e.g., purchase input 611, into the client indicating the user's desire to purchase the product. In various implementations, the user input may include, but not be limited to: keyboard entry, card swipe, activating a RFID/ NFC enabled hardware device (e.g., electronic card having multiple accounts, smartphone, tablet, etc.), mouse clicks, depressing buttons on a joystick/game console, voice commands, single/multi-touch gestures on a touch-sensitive interface, touching user interface elements on a touch-sensitive display, and/or the like.

165. Payment by QR code is described by Osborne in several paragraphs:

The price and total payable information may also be displayed, along with a QR code 915k that captures the information necessary to effect a snap mobile purchase transaction. Id. at [0078]

In another example, money may be transferred to Brian S. via QR code as indicated by the QR code icon 917d. Id., [0080]

With reference to FIG. 10D, in one embodiment, the mode tab 1040 may facilitate selection of a payment mode accepted by the payee. A number of payment modes may be available for selection. Example modes include, blue tooth 1041, wireless 1042, snap mobile by user-obtained QR code 1043, secure chip 1044, TWITTER 1045, 13 near-field communication (NFC) 1046, cellular 1047, snap mobile by user-provided QR code 1048, USB 1049 and FACEBOOK 1050, among others. Id. at [0093]

166. In one implementation, a pay card such as a credit card, debit card, pre-paid card, smart card and other pay accounts may have an associated code such as a bar code or QR code. Such a code may have encoded therein pay card information including, but not limited to, name, address, pay card type, pay card account details, balance amount, spending limit, rewards balance, and/or the like, *Id. at [0108]*. The techniques used by Osborne were well-known in the field.

Osborne is an obviousness reference discussed in more detail beginning at ¶IX.A, below.

167. On September 21, 2012, an application was filed that was published on February 28, 2013, as Purves et al. U.S. Patent Application Publication 2013/0054454 (“Purves,” EX1013), entitled “Wallet Service Enrollment Platform Apparatuses, Methods and Systems.”

168. Purves discloses a system for enrolling payment account in a consumer’s virtual wallet. EX1013, Abstract. The issuer of a credit card, for example, can share payment information with a virtual wallet provider. Purves teaches that a user may select a payment credential from their wallet by choosing among visual representations (e.g., images) of the credentials stored in the wallet. EX1013, Fig. 20b. This is also described at [0104]:

In some implementations, the user may be presented to a card management screen (e.g., from an issuer, merchant, and/or like source) that allows the user to select 2012 bank credit cards 2013a and/or debit cards 2013b to be used in the user's virtual wallet. In some implementations, information 2014 related to each card may be displayed with the card selection, including the card number, the card balance, images of the card, and/or like identifying information.

169. Purves also teaches the use of tokens as replacements for actual credentials, and that tokens may be encrypted:

In one implementation, the merchant server may use the user sign as a trigger to request current user information from the wallet server. The merchant server may generate and send a user information request message 926 to the wallet server. The user information request message 926 may include, without limitation, the customer ID that is unique to the customer and the merchant relationship, a token, an API key, a digital certificate, and/or the like. In one implementation, the token may be generated using one or more parameters such as the merchant's API key, customer ID, merchant ID, merchant name, customer name, and/or the like. In a further implementation, the token may be encrypted. In one implementation, the token may be a string that is created by the MD5 Message Digest algorithm hash of one or more of the parameters listed above. Id., [0073]

170. Purves further discloses at [0095] that payment credentials can be communicated by QR code:

As another example, using a quick response (QR) code scan, a near-field communication (NFC) tap or other mobile trigger in lieu of a WSEP button may also trigger a wallet connection or login. As yet another example, using a voice password, repeatable gestures or action, biometrics, and/or the like may trigger a wallet connection or login

171. Harris et al. U.S. Patent Application Publication 2012/0310838 (“Harris,” EX1014), entitled “Local Usage of Electronic Tokens in a Transaction Processing System,” was published on December 6, 2012.

172. Its Abstract discloses:

*A method for the use of electronic transactional tokens includes: generating a plurality of transactional **tokens** including a first token; associating each of the transactional **tokens** with a plurality of users, the first **token** associated with a first user; monitoring usage of the transactional tokens in a plurality of transactions in a local region or network; and in response to receiving transactional data for the first transaction, updating the first **token** from a first state to a second state (e.g., to provide a benefit when the token is applied in the local region or network). The **tokens** may be generated and monitored using a **token** processing system, which uses transaction data received by a transaction handler that is handling transaction processing for the transactions.*

173. I note that the “state” of the tokens in Harris corresponds to the “status indicator” of the ’854 Patent.

174. In view of the foregoing, by December 21, 2012, there was nothing inventive about generating from a credential a tokenized representation of the credential.

C. QR Codes

175. QR codes have been available since 1994 and have found multiple uses in transactions and authentication.

176. In 2009, Starnberger et al. published “QR-TAN: Secure Mobile Transaction Authentication” (“Starnberger,” EX1041) Its Abstract discloses:

QR-TANs are a transaction authentication technique based on two-dimensional barcodes. Compared to other established techniques, QR-TANs show three advantages: First, QR-TANs allow the user to directly validate the content of a transaction within a trusted device. Second, validation is secure even if an attacker manages to gain full control over a user’s computer.

177. Further,

QR-TANs use a method based on transaction-signing that has been adapted to fit the capabilities of commonly used Web-based applications. QR-TANs are based on two-dimensional QR barcodes. Similar to other approaches [2]–[6], QR-TANs authenticate transactions by using a trusted device. This device can be a mobile phone with a display and a camera with a modest resolution. QR-TANs use QR codes for the transmission of information. Id. at 578

178. As discussed above, Neafsey, Purves, and Osborne disclose displaying virtual credentials as QR codes. As discussed below at ¶182, Langley also discloses such use of QR codes.

179. Laracey U.S. Patent Application Publication 2011/0251892

(“Laracey,” EX1042), entitled “Mobile Phone Payment Processing Methods and Systems,” was published on October 13, 2011, more than one year before the Priority Date. It discloses a method of making a purchase from a mobile phone by scanning a token displayed on the phone in the form of a QR code or by transmitting it using NFC:

*Referring first to FIG. 8A, a mobile device 802 is shown which has a display 836 showing an image of a check out **token** (represented as a dynamic two dimensional **bar code image** or “**QR code** 837) which has been captured or imaged by a camera associated with the mobile device 802. The checkout **token** or code has been captured by a customer operating the mobile device 802 during the course of a payment transaction using embodiments of the present invention (e.g., the display shown in FIG. 8A may have been captured during the transaction processing described at Step 430 of FIG. 4B, or step “13 of FIG. 6, etc.).*

Id. at [0163].

*The mobile device 700 can also include one or more wireless communication Subsystems 724. Such as an 802. 11b/g communication device, RFID, **NFC**, and/or a Bluetooth(R) communication device.*

Id. at [0156].

*A number of terms are used herein for convenience and ease of exposition. For example, the term “capture” will be used to refer to the act of scanning, reading or other capturing of a “checkout **token**” (an identifier used to facilitate transactions pursuant to some embodiments). The term “capturing (or “captured) is not intended to be limiting, and is intended to encompass embodiments where a mobile device is operated to receive a checkout **token** (or data associated with a checkout **token**) via key entry, via **image capture**, via RFID reading, and using other **Scanning**, reading, or other techniques described herein.*

Id. at [0019].

180. On August 16, 2012, Hammond et al. U.S. Patent Application Publication 2012/0209749, entitled “Snap Mobile Payment Apparatuses, Methods and Systems” (EX1043) was published. Its Abstract discloses:

*The SNAP MOBILE PAYMENT APPARATUSES, METHODS AND SYSTEMS (“SNAP) transform real-time-generated merchant-product **Quick Response codes** via SNAP components into virtual wallet card-based transaction purchase notifications. In one embodiment, the SNAP obtains a snapshot of a **QR code** presented on a display screen of a point-of-sale device from a mobile device. The SNAP decodes the **QR code** to obtain product information included in a checkout request of the user, and merchant information for processing a user purchase transaction with a merchant providing the **QR code**. The SNAP accesses a user virtual wallet to obtain user account information*

to process the user purchase transaction with the merchant. Using the product information, merchant information and user account information, the SNAP generates a card authorization request, and which the SNAP provides to a payment network for transaction processing. Also, the SNAP obtains a purchase receipt confirming processing of the user purchase transaction.

181. The information communicated by QR code may include a token:

*In some implementations, a first user 121b may desire to pay a second user 121a an amount of money (or a value equivalent, e.g., virtual currency, alternate real currency, rewards, miles, points, etc.), e.g., P2P Snap mobile payment 120. The second user 121a may generate a limited time-validity **QR code**, e.g., 122, including information on the amount of money to be transferred, as well as a privacy **token**/alias linked to a financial account of the second user. The second user may display the **QR code** generated to the first user (e.g., by holding the second user's mobile phone displaying the **QR code** to the first user; sending the **QR code** by email, Social network message, tweet, etc.). The first user may take a snapshot of the **QR code** using the first user's mobile phone, e.g., 123, and utilize the amount of money, the second user's privacy **token**/alias linking to a financial account, and the first user's virtual wallet linked to the first user's mobile phone, to generate a purchase transaction request for processing by the payment network.*

Id. at [0026].

182. Langley (EX1040) also discloses at [0171] the display of a credential using a QR code:

*This diagram is similar to FIG. 10B, however, instead of a one-dimensional bar code being displayed, a two-dimensional barcode 804B is displayed for a merchant using the MPCD 102C to Scan Such a barcode 804B. The 2-D bar code may include, but is not limited to, the following symbologies: Aztec Code, 3-DI, ArrayTag, Small Aztec Code, Chromatic Alphabet, Chromocode, Codablock, Code 1, Code 16K, Code 49, ColorCode, Compact Matrix Code, CP Code, CyberCode, d-touch, DataGlyphs, Datamatrix, Datastrip Code, Dot Code A, EZcode, Grid Matrix Code, High Capacity Color Bar code, HueCode, INTACTA.CODE, InterCode, MaxiCode, mCode, MiniCode, Micro PDF417, MMCC, Nintendo e-ReaderiDot code, Optar, PaperDisk, PDF417, PDMark, **QR Code**, QuickMark Code, Semacode, Smart Code, Snowflake Code, ShotCode, SuperCode, Trillcode, UltraCode, UnisCode, VeriCode, VSCode, WaterCode, for example.*

183. Thus, by December 21, 2012, it was not inventive to use a QR code to communicate an authentication token.

D. Near-Field Communication

184. Near-Field Communication (NFC) permits two-way wireless digital communication between two devices that are in proximity to one another. NFC became a standard for close-range communication on December 8, 2003, when

ISO/IEC standard 21481 was published and adopted by the European Computer Manufacturers Association (ECMA) as Standard ETSI TS 102 312. NFC was available on Nokia smartphones and the Samsung Nexus Android phone in 2010.

185. As discussed above, Neafsey (EX1015-EX1016) and Osborne (EX1011) disclose transmitting virtual credentials using NFC.

186. The Abstract of Langley discloses the use of NFC to communicate a payment token:

*A system and method for remitting payment from a consumer's credit or stored value account by digital presentations of account information are described. A merchant may create one or more merchant account at a point-of-sale service site ("POS service site") and associate one or more merchant portable computing devices ("MPCDs") with one or more of the merchant accounts. Each MPCD may be configured to receive customer data from a customer via one of a visual capture and a wireless communication, such as a near field communication (NFC) or a machine-readable **optical code**. The customer data may be received from an **NFC**-capable physical **token** such as an EMV card, or a virtual **token** presented by a customer portable computing device ("CPCD") using a **NFC** or a machine-readable optical code. Each MPCD may contain a point-of-sale payment application supplied by the POS service site that may capture data representative of a consumer account from the received customer data.*

187. Digital Transactions at 20 discloses:

NFC-enabled handsets contain a special chip that can communicate over a very short range--typically about 4 centimeters--to establish a link with another NFC device, such as a point-of-sale reader. The chip interacts with the phone's operating system and with an electronic wallet in the phone containing card-account details.

188. Harris at [0437] discloses:

In another embodiment, the reader (163) includes a contactless reader, such as a radio frequency identification (RFID) reader, a near field communications (NFC) device configured to read data via magnetic field coupling (in accordance with ISO standard 14443/NFC), a Bluetooth transceiver, a WiFi transceiver, an infrared transceiver, a laser scanner, etc.

189. Laracey at [0156] discloses:

The mobile device 700 can also include one or more wireless communication subsystems 724. Such as an 802. 11b/g communication device, RFID, NFC, and/or a Blue tooth R communication device.

190. Hammad at [0026] discloses:

In alternate implementations, the two users may share the data encoded in the QR code via methods alternate to the QR code, including but not limited to: near-field communications (NFC),

Wi-Fi™, Bluetooth™, cellular network, SMS, email, text messages and/or the other communication protocols.

191. Thus, by December 21, 2012, it was not inventive to use NFC for communication in an authentication transaction.

E. Credential Identifiers

192. It is almost universal for authentication credentials to carry identifiers. A driver's license has a license number. A passport has a passport number. A credit card has a credit card number. This is essential because the name of the holder of the credential may not be unique (e.g., John Smith), while the credential identifier can be unique. This idea is not new – it stands to reason that in order to determine if a credential is valid, there has to be some way to look it up in a database of credentials.

193. Osborne, for example, discloses a credential identifier in the form of a “token identifier” at [0047]:

*For example, the token server may generate a unique and resolvable **token identifier** irrespective of the token requesting channel (e.g., merchant, issuer, acquirer, payment network, user, etc.). In some implementations, the token server keeps track of all generated tokens via **token identifiers**, and as each is created, subsequent requests for creation of a token with the same **token identifier** will be denied.*

194. Langley discloses at [0114]:

*Specifically, the stored value account issuer server 108B is responsible for creating and managing the client unique identifiers 155, **virtual card identification numbers** 167, primary account numbers (“PANs”) 165, and merchant identifiers 170 of FIG. 7AB discussed in greater detail below.*

195. Harris discloses at [0023]:

*In one embodiment, the token processing system maintains data for the tokens of each user (e.g., a **unique identifier for each token** that is associated with that user). The token processing system may, for example, maintain data regarding various attributes for each token and also transaction histories associated with each token.*

196. Thus, by December 21, 2012, it was not inventive to identify a credential using a credential identifier.

F. Device Identifiers

197. It was well-known to use device identifiers to tie electronic representations to particular devices. As discussed above at ¶152, Neafsey discloses using a device identifier as part of a credential.

198. Further, Osborne expressly includes a device “MAC address” in its token. EX1011, table in [0047], excerpted here:

<token>

...

<!-- In some embodiments, client_details are optional and the token may be

tied to a specific client-->

<client_details>

<client_IP> 192.168.23 .126</client_IP>

<client_type>smartphone</client_type>

<client_model> HTC Hero</client_model>

<OS>Android 2.2</OS>

<app_installed_flag>true</app_installed_flag>

*<client_fingerprint>font list, **MAC address**, memory size, hardware chip, screen resolution</client_fingerprint>*

</client_details>

199. Harris discloses at [0075]:

*For example, the above coupon may be entered into a user network that is associated with an iPhone or iPad mobile device. The coupon is associated with this network and is also associated with an **ID for this mobile device**. The **mobile device ID** may be referenced to a specific user or group of users of the mobile device (e.g., this reference may be stored in user device information 422).*

200. Laracey discloses at [0066]:

In some embodiments, where the customer registers from a browser on their mobile device, or by first downloading a payment application having a registration module onto their mobile device, the system may capture unique identifying information associated with the mobile device (e.g., such as a hardware serial number, an ASIN, a UUID or other device identifiers).

201. That is, in Laracey, the registration of the payment application ties the use of that application to the device identifier.

202. Thus, by December 21, 2012, it was not inventive to tie a credential to a particular device using a device identifier.

G. Status Indicators

203. As discussed above at ¶154, Neafsey discloses a credential status indicator. As discussed above at ¶173, Harris also discloses a token status indicator referred to as “state.”

204. On April 30, 2009, Adams et al. U.S. Patent Application Publication 2009/0113543, entitled “Authentication Certificate Management for Access to a Wireless Communication Device” (“Adams,” “EX1044”) was published. It contains extensive disclosures of status indicators associated with token. For example, at [0046] is describes:

*In various embodiments, the **status** represented in the status indicator 45 may be indicated as being “valid”, “revoked”, or “on hold.” A **status** such as “on hold” may be a subcategory of “revoked”; if subcategories of “revoked” **status** are provided, then the **status indicator** may also comprise a reason code as well, which provides a further explanation why the certificate was revoked. The “on hold” **status** may mean that an administrator may have reason to believe that the private key 55 corresponding to the certificate 35 has been compromised for some reason. For example, the user may have reported that he*

*or she had misplaced the security token 108, which may prompt an administrator to change the **status** of the certificate to “revoked” and/ or “on hold”. If the user had reported the security token 108 stolen, then the **status** indicator 45 would indicate “revoked” and the reason code may indicate “stolen”, or may be blank. This **status** information may first be updated at the source CRL or other certificate status source, and would be updated at the user device 100 as described below. Other revocation reasons will be apparent to those skilled in the art. It will also be apparent that the certificate **status** need not literally comprise indicators such as “revoked” or “on hold”; the **status** indicator 45 may be encoded in any appropriate format. For example, the status indicator 45 may comprises numeric codes which may be interpreted by a human with reference to an established information technology policy for that user device 100.*

205. Thus, by December 21, 2012, it was not inventive to provide a token status indicator.

H. Reason for Invalid Credential

206. When a transaction fails because a user credential, such as a token, is found to be invalid, it is natural and expected for the user to be informed of the reason for invalidity, e.g., “Your credit card has expired.” Many references disclose this.

207. For example, Langley discloses at [0097]:

*A transaction declined notice or message may be sent to the MPCD 102C and the method 300 may end. The message may include a **code** or identifier indicating the **reason for declining the transaction**.*

208. CyberSource discloses “reason codes” at p. 88:

*ecAuthenticateReply_reasonCode. Numeric value corresponding to the result of the overall request. See “**Reason Codes** for the Simple Order API” on page 125 for a list of possible values.*

209. The referenced page 125 lists 18 different “reason codes,” some relating to authentication or verification, including the following:

101 The request is missing one or more required fields.

102 One or more fields in the request contains invalid data.

200 The request was declined by CyberSource because it did not pass the eFunds ID Verification check.

388 Error: The routing number did not pass verification as described in “ACH Verification” on page 13.

210. The passage from Adams cited in ¶204 also discloses reason codes.

211. Thus, by December 21, 2012, it was not inventive to provide a reason that a credential was found invalid.

IX. GROUND 1: CLAIMS 1-17 WERE OBVIOUS OVER OBORNE

A. Overview of Ground

212. Osborne discloses or suggests each limitation of independent claims 1, 8 and 15, as well as the limitations of claims 2-7, 9-14, and 16-17, arranged as in each claim. Specifically, Osborne teaches using tokens representing credentials such as credit cards to perform payment transactions. Here I apply constructions of “OVER file” and “scan” as advanced by Patent Owner in the Complaint, EX1018 (i.e., as encompassing a token and an NFC interaction, respectively).

213. As I discuss below, limitation 1.3 requires that the OVER file’s “virtual representation” (which Patent Owner maps to a token) must be verified as an official representation of a credential by an issuer. Osborne teaches or at least suggests that its token server may be operated by the issuer of a user’s credentials. In such a system, it would at minimum have been obvious that the OVER file comprising a virtual representation of the credential has been verified by the issuer as an official representation, since the issuer is the entity issuing the token as well as the credential. As I explained above beginning at ¶109, the use of tokens was well-established and familiar to issuers. *See, e.g.*, EX1033 (Visa publication providing best practices for tokenization). An arrangement where a credential issuer also issued tokens, as taught by Osborne, and thus verified their status as representations of their own credentials, would have been a routine and predictable application of known technology. It was therefore guaranteed that the virtual representation (token) had been verified by the issuer.

B. Claim 1

214. Osborne teaches or suggests each limitation of claim 1.

1. Preamble

1. A computer-implemented method comprising:

215. Whether or not the preamble is limiting, Osborne clearly teaches a computer-implemented method. See, e.g., EX1011 Figs. 1A, 4, 6A-6E, and 15, and [0114]-[0122], which show and describe computer system architectures.

2. Limitation 1.1

accessing, by an officially verifiable electronic representation (OVER) file verifying device, a first OVER file stored on a first OVER file client device, the first OVER file comprising:

a first virtual representation of an original credential of a user that has been verified by an issuing agency to be a first official representation of the original credential of the user for proving the user's identity or qualifications, based on information associated with the original credential of the user, wherein the first OVER file is itself a first new credential of the user;

the first OVER file generated by an OVER engine configured to:

store the information associated with the original credential of the user; and

**transmit the first generated OVER file to the first OVER file
client device;**

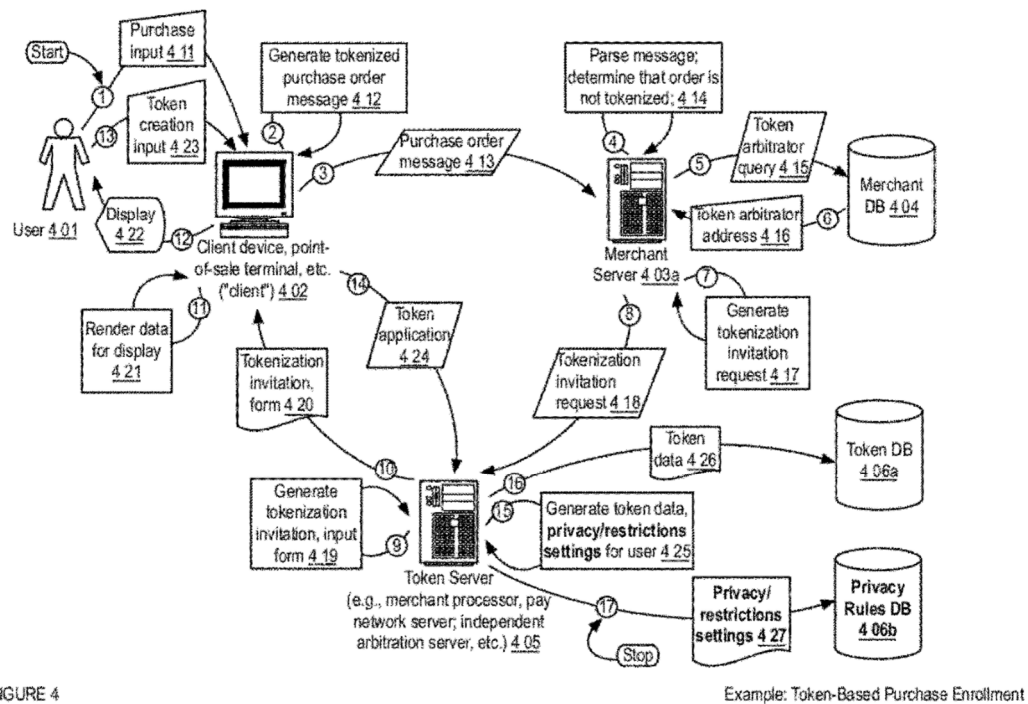
216. I address the various components of this limitation as follows:

217. An “OVER engine” is configured to generate a “*first OVER file*” with characteristics as recited above and transmit it to a “first OVER file client device,” from which it is accessed by an “OVER file verifying device.” Osborne teaches such an arrangement for token-based transactions, as described below.

OVER engine, verifying device, and client device

218. Osborne teaches an OVER engine, in the form of a “payment privacy tokenization apparatus” or “PPT” apparatus to “transform payment token-based purchase orders, via PPT components, into multi-issuer purchase payment funds transfers” is the claimed “(OVER) generation and verification engine.” EX1011, [0022], [0166]. The system includes a “token server,” also referred to as a “token arbitrator,” that may be any entity involved in the PPT, such as “part of the payment network (e.g., a pay network server).” EX1011, [0053]. Osborne states that the “the source of the token” may be the “issuer” (e.g., a funding source for the user’s account). EX1011, [0047]-[0048] (noting in XML comments that the token administrator may be the funding source, or that “alternatively token administrator may be different from funding source”), [0029] (user may obtain token from funding source).

219. The PPT system also includes a “merchant server” in communication with a user via clients, which may include devices such as “a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, and/or the like.” EX1011, [0035]. Osborne depicts the general arrangement of customers, parties, and the pay network server (which can include the PPT apparatus) in Fig. 4, reproduced below.



EX1011, Fig. 4. This system includes the “OVER file verifying device” (e.g., merchant point-of-sale device in communication with merchant server), as well as the “first OVER file client device” (user device, such as a card or mobile device communicating with the verifying device).

220. As I explain below in connection with limitations 1.3 and 1.6, the disclosed apparatus generates and verifies OVER files. Osborne thus discloses the recited OVER engine.

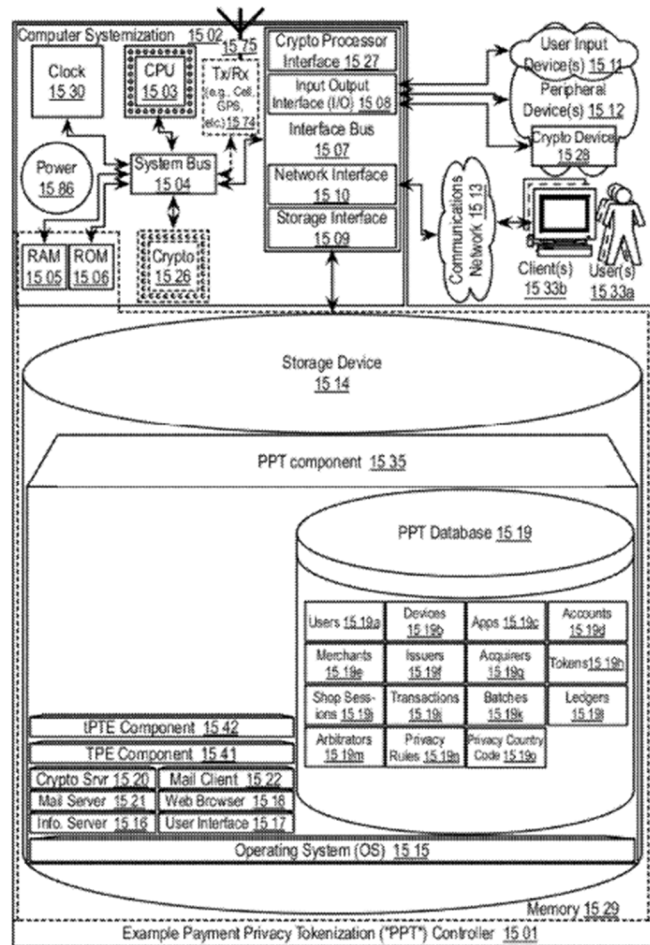
OVER file

221. The PPT apparatus supports the use of tokens for transactions, corresponding to the recited “OVER file,” as discussed below. EX1011, [0025].

222. The PPT apparatus generates tokens in response to receipt from a user of a token application received by a token server of the PPT apparatus. EX1011, [0035], [0040]-[0047], [0054]. Osborne provides an example encoding of a tokenization application form, shown below:

```
POST /purchase.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 1306
<?XML version = "1.0" encoding = "UTF-8"?>
<token_application_form>
  <provisional_token_ID>4NFU4RG94</provisional_token_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <account_params>
    <account_name> John Q. Public </account_name>
    <account_type> credit </account_type>
    <account_num>123456789012345</account_num>
    <billing_address> 123 Green St., City, ST 12345
    </billing_address>
    <phone> 123-456-7890 </phone>
    <sign> /jqp/ </sign>
    <confirm_type> CVV2 456 </confirm_type>
    <contact_info> SAME AS BILLING </contact_info>
    <country> UK </country>
    <privacy_restriction_type> EU DEFAULT
    </privacy_restriction_type>
  </account_params>
  <shipping_info>
    <shipping_address> 123 Green St., City, ST 12345
    </shipping_address>
    <ship_type> Express </ship_type>
    <ship_carrier> FedEx </ship_carrier>
    <ship_account> 0908765432 </ship_account>
    <tracking_flag> ON </tracking_flag>
    <sign_flag> ON </sign_flag>
  </shipping_info>
</token_application_form>
```

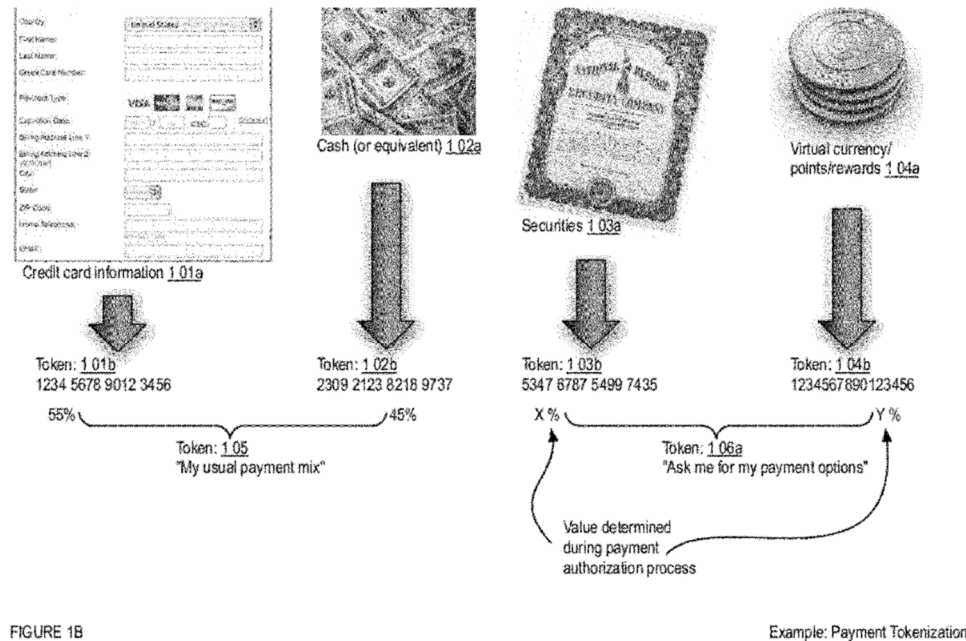
EX1011, [0040]. This form provides “information associated with the original credential of the user” stored by PPT, such as account number, type, billing address, etc., for the user’s credit cards. Osborne’s PPT apparatus includes a storage device (storage device 1514) storing account information in a database, as shown in Fig. 15, below.



EX1011, Fig. 15; *see id.*, [0114], [0146]-[0151]. The database’s “Accounts table 1519d,” includes fields for storing the “information associated with the credential” (e.g., information about the user’s credit cards), such as “account_number,” “issuer_name,” “account_address,” “routing_number,” etc. EX1011, [0147].

223. The token server uses these stored values to generate a data record and data structure for a token (“OVER file”), as well as a “token identifier” representing the token, which is provided to the user. EX1011, [0041], [0047]-

[0048], Fig. 5 (showing process). As depicted in Fig. 1B (below), the token is a virtual representation of a credential, such as a credit card.



EX1011, Fig. 1B. Osborne confirms that the token is “linked to credit card information,” noting that the tokens are used “in lieu of payment information” such as “card information.” EX1011, [0025]. Thus, the token is a “virtual representation of an original credential of a user” that is generated based on the information associated with the credential. Osborne teaches that a user “desir[ing] to utilize a card” may use “tokens in lieu of payment information,” using the token to prove identity to a merchant as a stand-in for credit card or account information. EX1011, [0025]. Thus, the token is a “first new credential” used “for proving the user’s identity or qualifications,” by taking the place of an “original credential.”

...verified by the issuing agency...

224. Osborne teaches, or at least suggests, that the token would be verified by the issuing agency as an official representation. As discussed above for with respect to the OVER engine, Osborne teaches that any entity can operate as the token server, and it specifically identifies that the token may be provided by the credential's "funding source"—that is, by the agency that issued the credential. EX1011, [0029], [0047]-[0048], [0053]; *see also id.*, [0058] ("Issuer server(s), e.g., 609 a-n, of the issuer(s) may maintain details of the user's account linked to the payment token."). By generating the token and providing it to the user to represent the credential it has issued, the issuer would be verifying it to be an official representation of the credential.

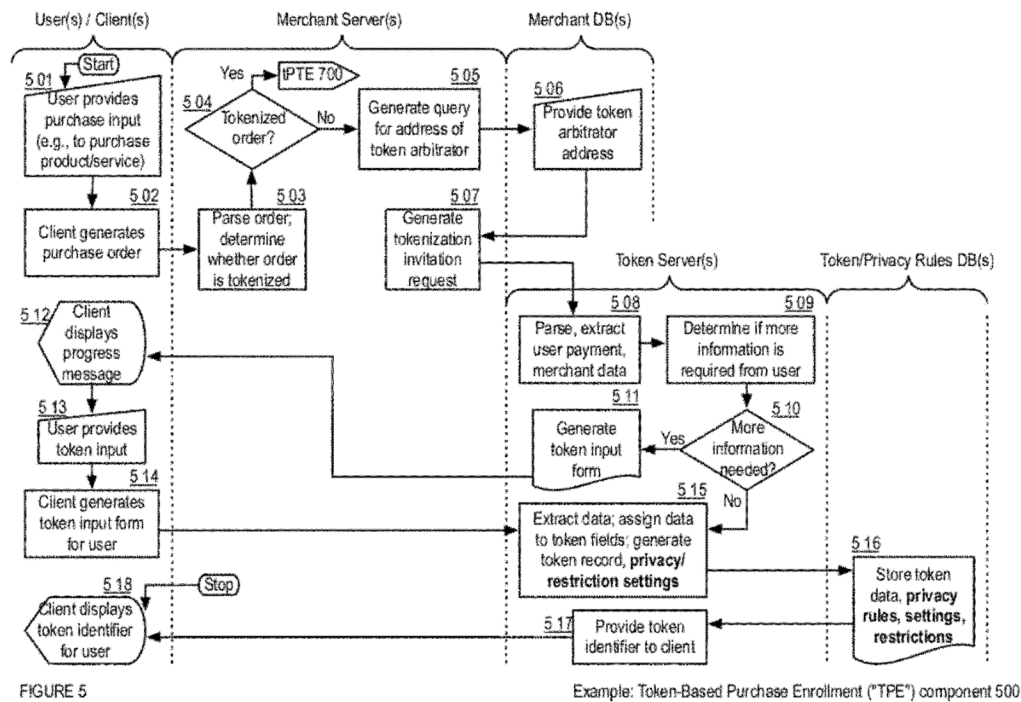
225. Further, a POSITA would have found it obvious for an issuer, upon generating the token, to verify that it was an official representation of the credential, using stored the credential information identified by the token application form when generating the token, since verifying that the token officially represented the credential would be a routine step based on the credential data received and doing so would increase confidence that the token legitimately represented the credential.

226. If Patent Owner argues that the claim requires that the credential, rather than the token, be verified by the issuer, a POSITA would have found it obvious that a credential is verified by virtue of being issued by an official issuer.

Because the purpose of a credential is to be an official representation from the issuer, an issuer would make such a verification as a matter of course when issuing the credential.

transmit[ted] to the client device

227. Osborne teaches that a “token may be provided as a data structure via HTTP(S) POST, as a file, as an attachment (e.g. via email), and/or provided to the client device for later use.” EX1011, [0048]. The transmission to the client device is performed after receiving the token application as shown in Fig. 5, with step 517 occurring after a token generation request is received from the user (steps 508 and 515). *See* EX1011, [0040]-[0041], [0046]-[0047], and Fig. 5 (below). Osborne’s token server sends a token (“OVER file”) to the user’s device (“OVER file client device of the user”).



accessing the OVER file

228. Osborne teaches that the “OVER file verifying device accesses the first OVER file.” Of course, the OVER file verifying device must necessarily access the first OVER file in order to verify it. Osborne teaches that a user may communicate with a merchant server via a client (e.g., “mobile device” or “point-of-sale-terminal”) by “activating a RFID/NFC enabled hardware device.” EX1011, [0049]. This NFC interaction triggers a tokenized purchase with the merchant via a “third-party client verifying device” (the merchant server, alone or in conjunction with the merchant’s point-of-sale device interacting with the user’s device via NFC). EX1011, [0050] (the client provides a “tokenized purchase order message to the merchant server”).

229. Osborne teaches that a “user may be able to pass a token...to a merchant,” and “upon receiving a payment token from the user, the merchant may pass the token to a transaction arbitrator.” EX1011, [0025]. By receiving and passing the token, the merchant device “accesses...a first OVER file stored on a first OVER file client device,” as claimed.

3. Limitation 1.2

transmitting, by the OVER file verifying device, to the OVER engine, a first verifying request to verify that the first OVER file accessed from the first OVER file client device authenticates the user;

230. Osborne teaches this limitation as part of processing a merchant’s token arbitration request (“first verifying request”) triggered by a purchase order request from a user. To process the purchase order request, the merchant server sends a “token arbitration request...to a token server.” EX1011, [0051]-[0052]. This is the verifying request of limitation 1.2. An example of an encoding of such a request, which includes a token_id field representing a token, is reproduced below, with the token_id highlighted.

```
GET /purchase.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 1306
<?XML version = "1.0" encoding = "UTF-8"?>
<purchase_order>
  <order_ID>4NFU4RG94</order_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <merchant_params>
    <merchant_id>3FBCR4INC</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>1NNF484MCP59CHB27365</merchant_auth_key>
  </merchant_params>
  <purchase_details>
    <num_products>1</num_products>
    <product>
      <product_type>book</product_type>
      <product_params>
        <product_title>XML for dummies</product_title>
        <ISBN>938-2-14-168710-0</ISBN>
        <edition>2nd ed.</edition>
        <cover>hardbound</cover>
        <seller>bestbuybooks</seller>
      </product_params>
      <quantity>1</quantity>
    </product>
  </purchase_details>
  <account_params>
    <token_id>1234567890123456</token_id>
  </account_params>
  <shipping_info>
```

Id., [0050]. Osborne teaches that the “token server may parse the token arbitration request message” and “determine whether the user token is authenticated.”

EX1011, [0053]-[0055]; see also *id.*, [0025] (“[A] user may desire to purchase a product....For example, the user may be able to pass a token...to a merchant....For example, upon receiving a payment token from the user, the merchant may pass the token to a transaction arbitrator.”). Osborne thus teaches that the OVER file verifying device transmits first verifying request to verify that the OVER file verifies the user to the OVER engine.

4. Limitation 1.3

receiving, by the OVER file verifying device, a first authentication message comprising a first indication of whether a first scan associated with the first OVER file on the first OVER file client device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine;

231. Osborne teaches that a user communicates with a merchant server via a client (e.g., “mobile device” or “point-of-sale-terminal”) by “activating a RFID/NFC enabled hardware device” EX1011, [0049]. This NFC interaction triggers a tokenized purchase with the merchant, via the “OVER file verifying device” (the merchant server, alone or in conjunction with the merchant’s point-of-sale device interacting with the user’s device via NFC). EX1011, [0050] (client provides “tokenized purchase order message to the merchant server”). As discussed at ¶¶95-96, Patent Owner has argued in district court that transmitting proximity-payment requests such as NFC interactions constitute a scan under the ’854 patent. Applying this interpretation to Osborne, since Osborne’s RFID/NFC activation triggers the purchase to be performed with the token, the RFID/NFC activation would be a scan associated with the first OVER file on the first OVER file client device of the user.

232. As discussed above, a token arbitration request is sent from the merchant server based on the user’s purchase order. EX1011, [0051]-[0052]. In

response, the token server processes the token arbitration request triggered by the scan by extracting the token from the request and looking up the account number in a token database. In particular, the token server “extract[s] the payment token from the message,” then issues a “query to a database, e.g., token database 606, using the payment token as a search term in the query.” EX1011, [0053]. In response, the database produces “instructions for the token server on how to proceed with payment processing.” *Id.* This includes credential information such as user account numbers, as shown in the highlighted XML example reproduced below:

```
<?XML version = "1.0" encoding = "UTF-8"?>
<issuer_data>
  <auto_default>false</auto_default>
  <user_contact>in-app</user_contact>
  <device_id>B17BP927</device_id>
  <default>
    <issuer>
      <issuer_id>A12345</issuer_id>
      <issuer_name>Bank de Tolkien</issuer_name>
      <issuer_IP>123.45.67.891</issuer_IP>
      <account_type>token</account_type>
      <account_number>1234567890123456</account_number>
      <percentage>65</percentage>
    </issuer>
    <issuer>
      <issuer_id>B12345</issuer_id>
      <issuer_name>ABC Credit Union</issuer_name>
      <issuer_IP>223.25.67.091</issuer_IP>
      <account_type>token</account_type>
      <account_number>6543210987654321</account_number>
      <percentage>25</percentage>
    </issuer>
    <issuer>
      <issuer_id>C67890</issuer_id>
      <issuer_name>BNR Bank</issuer_name>
      <issuer_IP>153.65.87.231</issuer_IP>
      <account_type>token</account_type>
      <account_number>1234567890123456</account_number>
      <percentage>10</percentage>
    </issuer>
  </default>
</issuer_data>
```

Id., [0053]. Osborne further teaches that the “token server may determine whether the user token is authenticated”; for example, where “no XML data is available associated with the payment token,” this indicates that the “user has not signed up for payment tokenization services.” EX1011, [0054]; *see also id.*, [0069] (“the token server may determine whether the user token is authenticated”). In other words, the query determines whether the scan (RFID/NFC interaction) “associated with the first OVER file [token] corresponds to the information associated with the original credential” (whether the database query for the token returns the user’s account details or not).

233. Osborne teaches sending an authenticating message comprising an indicator of the authentication determination. For example, if “the token server determines that the user is not authenticated, e.g., 711, option ‘No,’ the token server may generate an ‘authentication fail message.’” EX1011, [0069]. As shown in Fig. 7A, steps 712a-b, this message is sent to the merchant server (“verifying device”), which may then initiate enrollment or error-handling with the user device:

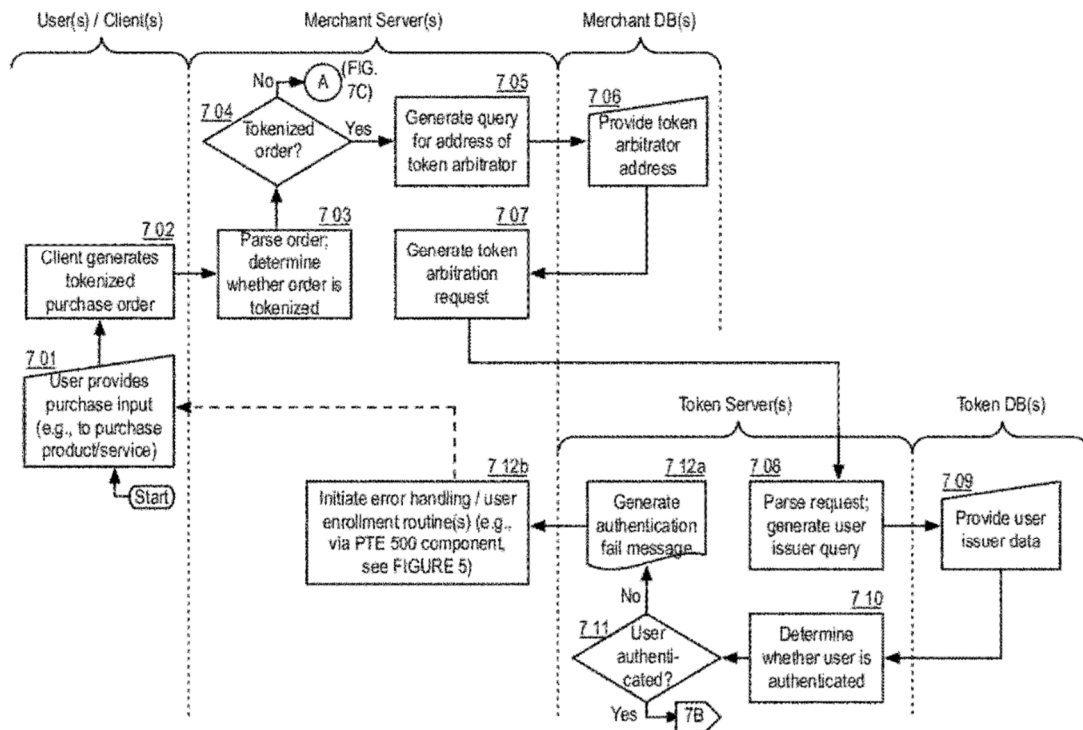


FIGURE 7A

Example: Token-Based Purchase Transaction Execution ("TPE") component 700

EX1011, [0069], Fig. 7A. This indicates that the scan is not associated with the stored user data.

234. If the user token is authenticated, then the “token server may continue processing.” EX1011, [0069]. The stored user account information is then used to procure payment authorization, and a message is sent to the merchant server indicating authorization, non-authorization, and/or “authorization in progress.” EX1011, [0063] (“token server...may in turn forward the authorization success message, e.g., 647, to the merchant server”), [0061] (sending “an ‘authorization fail’ message to the merchant server, token server and/or client”), [0070] (“authorization in progress” message), Figs. 7B-C (showing process). Any of these

messages is an indication that the token was authenticated, and thus that the scan corresponded properly to the stored user credential information.

5. Limitation 1.4

outputting a first status indicator expressing whether the first OVER file authenticates the user;

235. Osborne teaches that an authentication failure message triggers “an error handling routine and/or a user enrollment routine,” which Fig. 7A illustrates may be performed by the merchant server. EX1011, [0069], Fig. 7A. The initiation of these routines would be a status indicator expressing non-authentication (e.g., offering to enroll a user for tokens would indicate the user lacked an authenticated token). On the other hand, after successful authentication and an authorization success, the “merchant server may add a record of the transaction for the user” and also “provide the purchase receipt to the client,” which renders it for the user. EX1011, [0073]. This receipt is a status indicator confirming successful authentication.

6. Limitations 1.5-1.8

236. Limitations 1.5-1.8 repeat limitations 1.1-1.4, with several modifications. First, the “first” OVER file and OVER file client device are replaced, respectively, with a “second” OVER file and OVER file client device. Also, limitation 1.6 recites that the second OVER file is “scanned at the second

OVER file device” instead of “accessed from the first OVER file device.” Further, it is not specified whether the OVER engine generates the second OVER file.

Lastly, limitation 1.5 requires that the second OVER file be a “second new credential” that is “invalid for use in the first OVER file client device for authenticating the user.” Osborne teaches or suggests each of limitations 1.5-1.8 for the following reasons.

237. The existence and use of a second OVER file is met by a user having two devices and receiving respective OVER files to be used on each device. This would have been obvious in view of Osborne. A POSITA would have expected users to use multiple devices: Osborne expressly teaches that the token server may keep a device table with various identifiers for a user’s devices, such as “device_ID,” “device_name,” “device_MAC,” (referring to a MAC address) etc. EX1011, [0148].

238. The second and third differences for limitations 1.5-1.8 are also taught or suggested by Osborne. As discussed for limitation 1.3, Osborne teaches using an NFC interaction to provide a token to a verifying device, which meets Patent Owner’s own interpretation of “scan.” *Supra* ¶¶231-234. It would have been obvious to use such “scans” for tokens provided to each of two different user devices.

239. As to the last difference—that the second OVER file must be a new, device-specific credential that is invalid on the first OVER file client device, this would also have been obvious to a POSITA based on Osborne’s disclosure. For example, Osborne teaches that “device fingerprinting may be utilized” to provide “additional security” for use of Osborne’s tokens. EX1011, [0026]. Similarly, Osborne provides an example token data structure including a “client_fingerprint” field with device-identifying information like the client’s MAC address. EX1011, [0047]. To obtain the additional security taught by Osborne, a POSITA would have been motivated to employ Osborne’s device fingerprinting to tie a given token to a given device, such that the token for a second device would be a new credential, different from the first token (with both being different credentials from the original credential), with the second device’s token being invalid in the first device (since the first device’s fingerprint would not match).

240. Accordingly, claim 1 was obvious over Osborne alone.

C. Claim 8

241. Claim 8 is an apparatus for of claim 1, and was obvious over Osborne for essentially the same reasons as for claim 1.

1. Preamble

**1. An officially verifiable electronic representation (OVER) file
verifying device comprising:**

242. Whether or not the preamble is limiting, Osborne teaches an OVER file verifying device, as discussed for claim 1. See EX1011, [0035], Fig. 4.

2. Limitations 8.1-8.2

a hardware processor;

a memory unit operatively coupled to the hardware processor, the memory unit configured to store information associated with an original credential of a user and a plurality of instructions, wherein the instructions are configured to cause the hardware processor to perform operations comprising:

243. As discussed for claim 1, Osborne teaches a PPT apparatus that communicates with an OVER file verifying device, in the form of a merchant server and associated point-of-sale terminal. EX1011, [0035], Fig. 4. These components are depicted as computers by Osborne. See EX1011, Fig. 4 (showing “client device, point-of-sale terminal” 402 as computer and “Merchant Server” 403a as second computing device); *see also id.*, [0117] (“It should be noted that the term ‘server’ as used throughout this application refers generally to a computer, other device, program, or combination thereof.”).

244. A POSITA would have understood from Osborne that the verifying device would comprise a hardware processor and memory unit. Osborne explains the general understanding of POSITAs includes that “computers employ

processors to process information; such processors 1503 may be referred to as central processing units (CPU).” EX1011, [0115]. Osborne further explains that “stored instruction codes, e.g., programs, may engage the CPU circuit components and other motherboard and/or system components to perform desired operations,” with instructions stored in in various processor accessible and operable areas of memory.” *Id.* A POSITA would have understood that these basic elements of computer systems would apply to each computerized component described by Osborne, including the merchant server and point-of-sale terminal (OVER file verifying device); thus, these components would include a processor coupled to a memory unit storing instructions. The instructions stored in Osborne’s merchant devices would be configured to perform the operations described by Osborne for those devices, which correspond to the steps recited in claim 1 (and repeated in the remaining limitations of claim 8).

245. The verifying device would further be configured to store information associated with an original credential of a user in its memory unit. As discussed above for limitation 1.1, Osborne teaches that such information is received by the PPT apparatus via a token application form and stored by the apparatus. *Supra* ¶¶216-229. Osborne further teaches that the merchant server and point-of-sale terminal (verifying device) may provide the completed application including the original credential information to the token server. See EX1011, [0040] (“The

client may generate a competed [*sic*] application form, and provide, e.g., 424, the token application to the token server (either directly or via the merchant server).”). A POSITA would have understood that Osborne’s client (e.g., point-of-sale device) and the merchant server (collectively, the verifying device) would store the application containing the original credential information at least temporarily to allow the data to be transmitted to the token server. Thus, the verifying device’s memory unit is configured to store information associated with the user’s original credential, as recited in limitation 8.2.

3. Limitations 8.3-8.10

246. Limitations 8.3-8.10 are essentially identical, respectively, to limitations 1.1-1.8. The only changes are that limitations 8.3-8.10 omit “by the OVER file verifying device” (because the preamble and limitations 8.1-8.2 specify that the steps are performed by such a device), and limitation 8.3 recites “the original credential” instead of “an original credential of a user,” as the “original credential” was introduced in limitation 8.2. Neither of these constitute substantive differences relative to the mapping discussed above for claim 1. Accordingly, Osborne teaches limitations 8.3-8.10 for similar reasons as those discussed for 1.1-1.8 above.

247. Therefore, claim 8 was obvious over Osborne.

D. Claim 15

248. Claim 15 is a computer-readable medium form of claims 1 and 8. It recites a “non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to perform operations comprising” a series of steps recited in limitations 15.1-15.8. As discussed above for claim 8, Osborne teaches a verifying device (merchant server and point-of-sale terminal) storing instructions in a memory unit to be executed by a processor to perform the steps of claim 8. *Supra* ¶¶242. These steps (limitations 8.3-8.10) are identical to the steps recited in limitations 15.1-15.8, respectively, with the only differences being that limitation 15.1 recites “an original credential” and “a user,” and it does not expressly recite that the OVER file is a new credential. Thus, claim 15 was obvious over Osborne for similar reasons to claim 8. See *supra* ¶¶241-247; 214; see also *supra* ¶¶214-240 (substantively identical limitations for claim 1).

E. Claims 2, 9, and 16

249. Claims 2, 9, and 16 depend, respectively, from claim 1, 8, and 15. Each contains substantively identical limitations. Claims 2 and 9 recite that the “first OVER file further comprises a device identifier for the original credential configured to limit the first OVER file, for use in authenticating the user using the information of the original credential, to the first OVER file client device.” Claim 15 recites the same limitation, except that it omits two instances of “first” highlighted in bold above. Since claim 15 does not recite an “OVER file” or

“OVER file client device” without the terms “first” or “second,” I assume that claim 16 was intended to encompass at least an embodiment including the two bolded words “first,” paralleling claims 2 and 9. Osborne teaches these limitations.

250. For example, Osborne teaches that the token server may keep a device table with various identifiers for a user’s device, such as “device_ID,” “device_name,” “device_MAC,” (referring to a MAC address) etc. EX1011, [0148]. Osborne further teaches that “device fingerprinting may be utilized” to provide “additional security” for use of Osborne’s tokens and provides an example token data structure that includes a “client_fingerprint” field with device-identifying information like the client’s MAC address. EX1011, [0047]. Osborne further teaches that the “token may be provided as a data structure...to the client device for later use.” EX1011, [0047]; *see also id.*, [0026] (teaching that device fingerprinting may operate using a “client device of a user”). Because the token represents the credential, the device identifier would function as a device identifier limiting the credential to the particular client device via its association with the token (for example, the token would not be authenticated if used with a device having a device identifier not associated with the token). See EX1011, [0047] (including credential account numbers and related information along with device fingerprint in token).

251. Therefore, to obtain the additional security taught by Osborne, a POSITA would have been motivated to include a device identifier in a first OVER file (token) sent to a device of the user to employ Osborne's device fingerprinting to tie a given token to a given device, thus using the device identifier when authenticating the user using the information of the original credential (i.e., when confirming that the authenticity of the token matched to the original credential's information). This would have added an extra layer of security by ensuring the user's token was only being used by someone who also had possession of the user's device (since the device's fingerprint would not match otherwise).

252. Therefore, claims 2, 9, and 16 were obvious over Osborne.

F. Claims 3-4, 10-11, and 17

253. Claims 3 and 10 depend from claims 1 and 8, respectively, reciting that "the first OVER file further comprises user-specific information." Claims 4 and 11 depend from claims 3 and 10, respectively, reciting that "wherein the user specific-information comprises at least one of: biometric information, location information, a password, or a device identifier." Claim 17 depends from claim 15, and recites substantively the same limitations as claims 3-4 and 10-11, namely that "the first OVER file further comprises user-specific information comprising at least one of: biometric information, location information, a password, or a device identifier."

254. Osborne teaches that its PPT system stores user-specific information in a “Users table,” including, for example, the user’s “state, address firstline, address secondline, zipcode,” etc. EX1011, [0148]; *see id.*, Fig. 15 (table in PPT storage device), [0047] (token server stores token data structure comprising user’s address). These entries include at least location information (e.g., address, zip code, ...) about the user. EX1011, [0148] (also storing “device_ID,” “device_GPS,” “password”), 30 (biometric and/or like recognition); *see also id.*, [0047]-[0048], Fig. 3C (client device displaying user-specific information such as user address disclosed as being stored in token data structure, demonstrating inclusion in OVER file). Furthermore, as discussed above for claims 2, 9, and 16, Osborne teaches or suggests including a device identifier in a first OVER file sent to a user’s device to facilitate device fingerprinting for additional security. See EX1012, [0026], [0047]-[0048]. This device identifier would be user-specific information included in the first OVER file as recited in claims 3-4, 9-10, and 17.

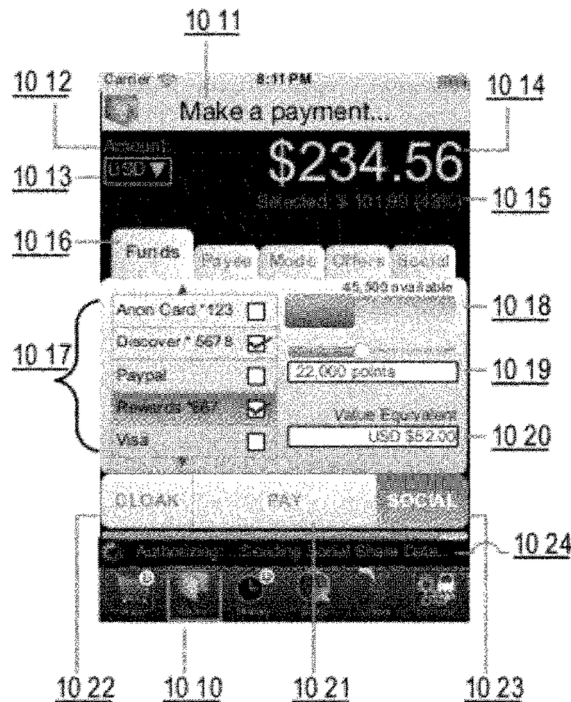
255. Therefore, Osborne renders claims 3-4, 9-10, and 17 obvious.

G. Claims 5 and 12

256. Claims 5 and 12 depend from claims 1 and 8, respectively, reciting that “the first OVER file comprises a portion of the original credential stored by the OVER engine.” This additional limitation was obvious, at least because a

virtual representation of a credential would be expected to contain a portion of the credential itself, e.g., the name of the holder.

257. Further, Osborne teaches that various payment account details (portion of the stored credential) are stored in a token data structure, and thus are included in the token. See EX1011, [0054] (including details such as account numbers). Osborne further teaches that the user device interface may display a portion of a credential, such as part of an account number. EX1011, [0085]; *see id.*, Fig. 10A (excerpted below).



258. In view of this disclosure, a POSITA would have found it obvious to include a portion of the stored credential (e.g., part of an account number) in the OVER file in order to allow disclosed display of portions of credentials.

259. Therefore claims 5 and 12 were obvious over Osborne.

H. Claims 6 and 13

260. Claims 6 and 13 depend from claims 1 and 8, respectively, reciting that “the first authentication message comprises an indication that the first OVER file is expired.” This additional limitation was conventional because in common credit card transactions, when a user attempted to use an invalid card, the merchant would be informed that the card was invalid (e.g., expired). At that point, the merchant would normally ask the user for a different credit card. The same principle would apply to tokens, as reflected by Osborne.

261. Osborne teaches that a user can specify “token attributes” including specifying “activation 227 and expiry 228 dates for the tokens.” EX1011, [0029]. Osborne confirms that a token includes an expiry date, as reflected in the example XML encoding of Osborne’s token data structure. See EX1011, [0047] (“<expiry>2011-02-28 23:59:59</expiry>”). Osborne also teaches that an “authentication fail message” can be sent where the token server determines the user is not authenticated, which may also trigger “an error-handling routine.” EX1011, [0069]. Where the user’s token had expired, the resulting authentication fail message would be an indication that it was expired. Indeed, it would have been obvious to specifically include a reason for rejection of the token (i.e., due to expiry) as part of the authentication fail message to inform the merchant and user

and facilitate the error-handling routine taught by Osborne. Expiration messages were standard for credit card transactions.

262. Therefore, claims 6 and 13 were obvious over Osborne.

I. Claims 7 and 14

263. Claims 7 and 14 depend from claims 1 and 8, respectively. Claim 7 recites that the method further comprises “accessing, by the verifying device, from the first OVER file client device, additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been satisfied.” Claim 14 recites substantively the same limitation, except that it omits claim 7’s reference to “the verifying device.”

264. Osborne teaches that “additional security may be layered by using authentication methods” in combination with tokens. EX1011, [0026]. This can include use of a “user name and password,” “a digital certificate,” and “device fingerprinting.” *Id.* When implementing the additional types of security measures disclosed by Osborne, it would have been readily apparent to a POSITA to do so by accessing additional credential information from the first OVER file client device by the verifying device indicating whether a secondary condition for authorizing the user has been satisfied. In such an implementation, the information (username/password, certificate, or fingerprint) would be accessed from the user’s

device by the verifying device, and the secondary condition would be that the provided information matched the corresponding values associated with the token.

265. For example, Osborne teaches that an “authentication chip may be configured to recognize the user's payment token physical card” using digital fingerprinting, with the user “required to present the payment token physical card to the authentication chip disposed in communication with the client before the user can make a purchase order using the token.” EX1011, [0026]. Specifically, Osborne explains that “the chip may be embedded into the client, come pre-installed in the client, attached as a periphery to the client, and/or the like.” *Id.*

266. As explained above in ¶219, Osborne discloses that the client can take the form of various hardware components such as a point-of-sale terminal or kiosk. EX1011, [0035]. Osborne recognizes this use of an authentication chip as a condition for authorization, stating it “provides an authenticity shield preventing others who may know of the user’s payment token from utilizing the user’s payment token in a fraudulent transaction.” *Id.*, [0026]. In light of Osborne’s disclosure, it would have been obvious for a verifying device to employ additional security measures such as the authentication chip described by Osborne to confirm a device fingerprint of the user’s device providing the token (OVER file client device).

267. Therefore, claims 7 and 14 were obvious over Osborne.

X. GROUND 2: CLAIMS 1-17 WERE OBVIOUS OVER OBORNE IN VIEW OF NEAFSEY

A. Rationale to Combine

268. As discussed in Ground 1, Osborne teaches or suggests each limitation of claims 1-17. For limitations 1.3, 1.6-1.7, 8.5, 8.8-8.9, 15.3, and 15.7-15.8, in Ground 1 I applied a construction of “scan” encompassing NFC interactions. To the extent “scan” is limited to an optical scan (as I believe it should be), this limitation is taught by Neafsey.

269. Neafsey teaches that various formats of virtual credentials may be used for conducting transactions. Among these formats are optically scannable codes, such as QR (quick response) and bar codes. EX1015, [0061]; re optical, *see* EX1016, 12; EX1011, [0032] (describing QR and barcodes that may be scanned with a camera). A POSITA would have been motivated to incorporate an optically scannable code into an OVER file to be used to trigger the use of tokens to purchase goods, in a manner similar to Osborne’s disclosure of using NFC or mag stripe interactions, as Neafsey teaches that such optically scannable codes would serve similar roles. The combination would thus be a simple substitution of known elements to achieve predictable results. Doing so would provide greater flexibility to users, increasing convenience and allowing a greater range of mobile devices to be employed (e.g., devices with screens capable of displaying an optical code could be used even if NFC communication was unavailable).

270. A POSITA would have had a reasonable expectation of success in this combination. Osborne expressly teaches the use of QR and bar codes in conjunction with similar transactions. *See* EX1011, [0080] (QR code for money transfer), [0093] (payment via “user-obtained QR code” alternative to use of NFC). Thus, a POSITA would have expected success in using optically scannable codes to stand in for credentials (e.g., as a scannable part of an OVER file) to trigger a tokenized transaction as taught by Osborne.

271. In this Osborne-Neafsey combination, scanning an optical code would replace the NFC or mag stripe interactions of Osborne, invoking the use of a token in a similar way. Using an optically scannable code in this way would satisfy the “scan associated with a credential” element of claims 1, 8, and 15, even under a (correct) narrower construction of “scan.” The remaining claim limitations for claims 1-17 would have been obvious for the same reasons discussed above for Ground 1.

272. Accordingly, claims 1-17 were obvious over Osborne in view of Neafsey

XI. GROUND 3: CLAIMS 1-17 WERE OBVIOUS OVER STAFFORD IN VIEW OF PURVES FURTHER IN VIEW OF NEAFSEY

A. Overview and Rationale to Combine

273. The combination of Stafford, Purves and Neafsey renders each of claims 1-17 obvious.

274. Stafford teaches a system for “validating and disseminating credential information” that discloses almost all limitations of the independent claims as well as many dependent claim limitations. EX1012, Abstract. Stafford’s system does not use tokens, but rather uses key signatures (e.g., hash values for encrypted files) to verify users’ identity and provide credential information to a third party. *See* EX1012, Fig. 3, [0107]-[0121].

275. Stafford discloses methods for providing credentials to third parties that parallel those described and claimed in the ’854 patent. Stafford’s system stores credential information for a user (“entity”) in a credential database, provides users with key signatures representing those credentials, and allows a third party (“IdBus1”), with which the user has shared the key signatures, to receive verification of a credential from the system. *See* EX1012, [0010], [0097]-[0102], [0108], [0115], [0118]-[0126], Figs. 2-3.

276. Stafford teaches that the key signatures and other information may be provided to a third party “online or in person,” and that the “delivery process may vary” based on the information provided and the recipient. EX1012, [0106]-[0113]. Stafford thus expressly suggests including other information with its key signatures and employing various known delivery processes as using an optical scan in the and including an image as a virtual representation of a credential in an OVER file. Such known processes and information would include using an optical scan in the

delivery process, including an image as a virtual representation of a credential in an OVER file, and using device identifiers to make such files unique to a given user device.

277. These limitations are taught by Purves and Neafsey. In particular, Purves teaches providing issuer-verified representations of credentials (such as credit card images). EX1013, [0085], [0102], [0108]-[0112]. A POSITA would have been motivated to incorporate such representations with Stafford's key signatures to provide user devices convenient images of the credentials that may be selected by the user.

278. Neafsey also teaches that scannable codes may be used to convey virtual credential information. EX1015, [0061], [0022] (credential encode strings of bits in different formats); EX1016, 4, 12. Such optical codes would include QR and bar codes, as taught by Purves. *See* EX1013, [0064] (QR code may be used to trigger wallet connection), [0095] (describing "a QR code 1508, bar code, or other visual element suitable for scanning by a mobile device"). Neafsey further teaches that clients may have different devices, and that credentials may be provided in different formats appropriate to a particular device. EX1015, [0061]; EX1016, 12. For example, these different credentials may be generated based on a "unique device ID" of the recipient device. EX1015, [0048]-[0049]; EX1016, 9-10.

279. A POSITA would have been motivated in light of these teachings to provide OVER files (such as files comprising the hash codes and credential representation of Stafford and Purves) to client devices in formats appropriate to each client device, e.g., by tying the OVER files to a given device's unique device ID. In particular, a POSITA would have understood that different client devices would sometimes require using different formats appropriate to each device, as certain formats could not be used on certain devices. For example, a first device may be able to process a QR code but not a bar code, while a second may permit the opposite, or more generally, different devices may support distinct sets of code formats, including optical codes, such that code formats supported by a first device could not be used in a second, and vice versa. See EX1015, [0061] (multiple different devices and formats possible); EX1016, 12. In such a case, each OVER file would be valid in one user device but invalid for use in the other.

280. As discussed in detail below for the independent claims, it would have been obvious to use these features as part of Stafford's credential-distribution system (1) to provide user devices convenient images of the credentials they are showing to third parties and (2) to use the scannable code formats such as QR and bar codes to transfer Stafford's key signatures to the third party by providing device-specific, encoded key signatures to the user.

281. A POSITA would have been motivated to combine Stafford, Purves, and Neafsey with a reasonable expectation of success to arrive at the claimed invention. All three references are directed to similar applications (electronic use of credentials replacing physical credentials typically carried in physical wallets, such as driver's licenses, credit cards, etc.). Further, incorporating features such as credential images and device-specific, optically-scannable codes into a credential management system like Stafford's would have been straightforward, as the use of these features would have been familiar to the POSITA and their application would have been predictable.

282. A POSITA would have recognized various benefits from incorporating Purves's credential images into Stafford's system. For example, the images would improve ease-of-use and reduce user error by providing users images matching the credentials the user seeks to provide to third parties.

283. Similarly, a POSITA would have viewed the device-specific, optically-scannable codes taught by Neafsey as a convenient way to convey key signatures to third parties in a more efficient and reliable manner than reading or typing a code manually, both of which are slow and error-prone. By adapting Stafford's credential management system to provide optically encoded key signatures, a POSITA would reasonably have expected to achieve these benefits for users.

284. The discussion of claims 1-17 below provides further detail regarding POSITA's rationale to combine Stafford, Purves, and Neafsey to arrive at the claimed invention with a reasonable expectation of success.

B. Claim 1

285. The combination of Stafford, Purves and Neafsey teaches each limitation of claim 1, as discussed below.

1. Preamble

1. A computer-implemented method comprising:

286. Whether or not the preamble is limiting, Stafford, Purves and Neafsey all teach a computer-implemented method. See, e.g., EX1012, [0054], Fig. 1; EX1013, [0130]-[0146]; EX1016, 4-8, Figs. 1-2.

2. Limitation 1.1

287. As discussed above in ground 1, limitation 1.1 involves an OVER engine that is configured to generate a first OVER file with certain specific characteristics and transmit it to a first OVER file client device, from which it is accessed by an OVER file verifying device. Stafford, Purves, and Neafsey teach such an arrangement, as described below.

OVER engine, verifying, and client devices

288. Stafford teaches a system ("OVER engine") that stores credential information for proving users' identity or qualifications. EX1012, [0054] ("FIG. 1 illustrates a system 100 for storing, validating and disseminating credential

information about an entity.”), Fig. 1; *see also id.*, claim 1 (“method of compiling a credential database including” receiving and verifying credential information, generating data representations of credential information and document, and storing them in encrypted form).

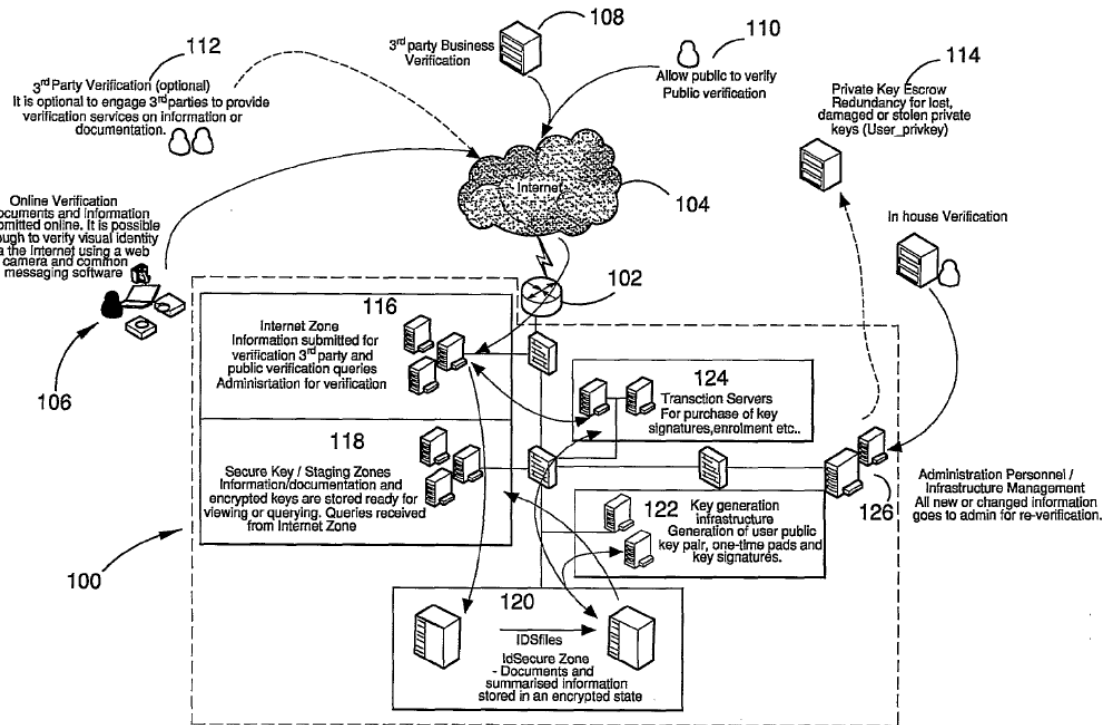


FIGURE 1

289. Stafford uses the terms “entity” or “IdMember” to refer to the user whose credentials are stored. Stafford’s system stores “credential information,” such as “name, address, date or birth, as well other information.” EX1012, [0053]-[0054]. This includes memory (a “data store”) hosting a “database of encrypted credential information.” EX1012, [0057]. Credential information is encrypted using the user’s public key, and further encryption (e.g., using a one-time-pad) is also employed to securely store the user’s credential information. EX1012, [0058],

[0071], [0089]. Stafford teaches that any of a variety of credentials may be used, such as driver's licenses, professional memberships, a degree (such as Ph.D.), etc. EX1012, [0004], [0065], [0131], [0139].

290. Stafford also teaches an entity client terminal ("first OVER file client device") operated by an entity/IdMember and that communicates with Stafford's system to store credentials, with the entity/IdMember providing and setting the sensitivity of credential information. EX1012, [0054], [0081]. Sensitive credential information requires use of "highly secure symmetric or similar encryption process e.g. a one time pad" when being released. EX1012, [0088]; *see id.*, [0073]-[0074], Fig. 2 (showing credential release process).

291. Stafford teaches that users can request release of sensitive credentials, and this request satisfies limitation 1.2. See EX1012, [0074] ("To release data, in a first example the entity (IdMember) logs on to the website and elects to 'release' information using the appropriate interface."). The request/release process is shown in Fig. 2, reproduced below.

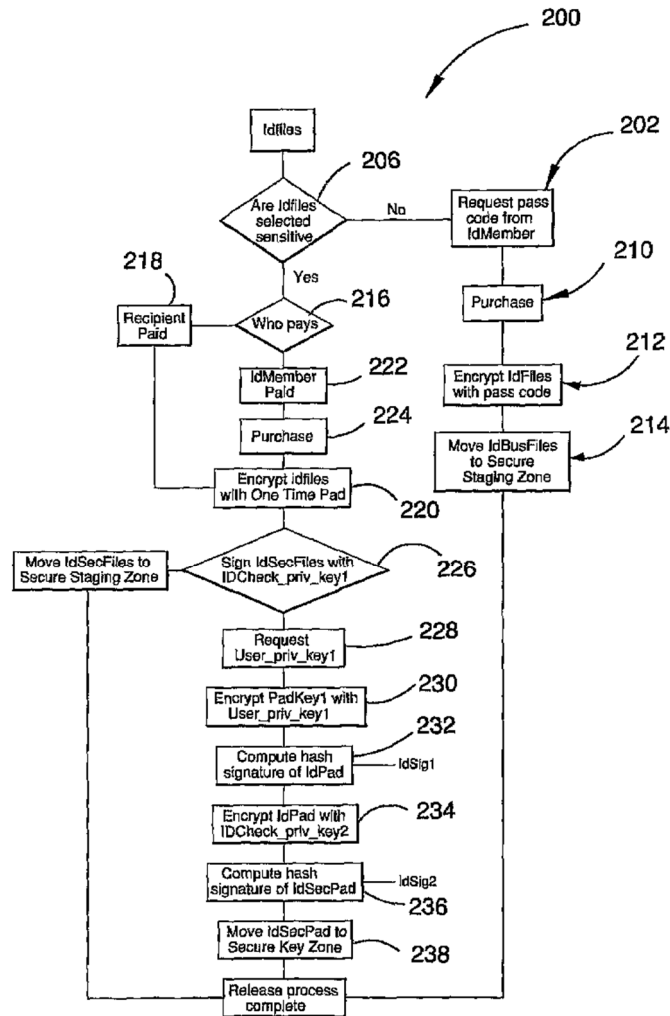


FIGURE 2

EX1012, Fig. 2. As shown in Fig. 2, when sensitive files are selected for release, the recipient or IdMember purchases a “key signature” that includes “a hash value or similarly secured...encrypted passwords or one-time pads” that identify and authorize release of encrypted credentials (IdFiles). EX1012, [0075]-[0079]; *see id.*, [0038], [0088], [0093]-[0095]. As discussed below, these key signatures would be provided in an “OVER file.”

292. Stafford also teaches an “OVER file verifying device.” As illustrated in Fig. 3, Stafford teaches that a third-party OVER file verifying device (referred to as IdBus1 at EX1012, [0108]) sends a request for release of information to the credential-database system. EX1012, [0115]; Fig. 3 (marked-up below).

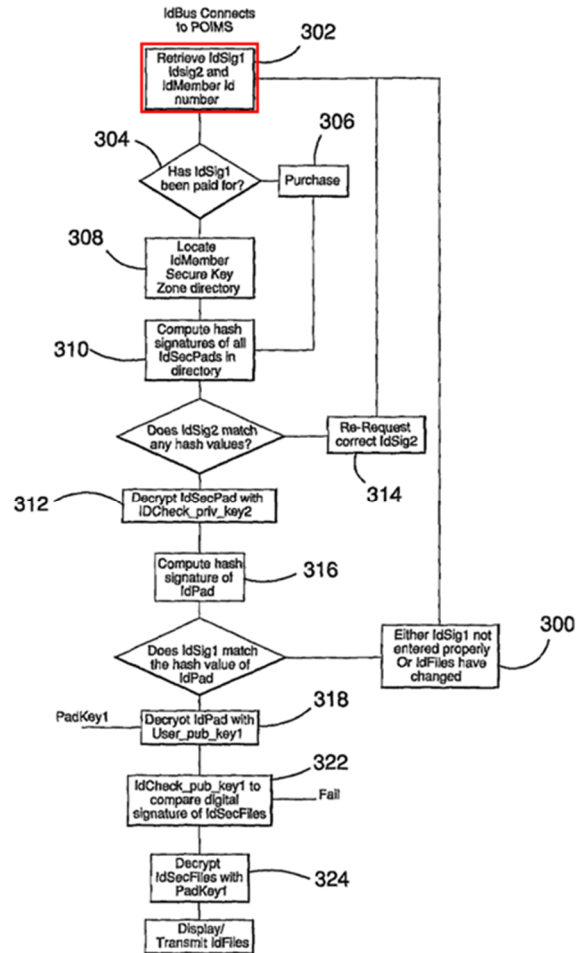


FIGURE 3

The request includes the key signatures IdSig1 and IdSig2, which are used to verify that the OVER file (encoding the signatures) authenticates the user, as only if the key signatures match the hash values of the encrypted credential file are the credential files transmitted. *See* EX1012, [0119]-[0122].

**OVER file comprising a first virtual representation of the original
credential that has been verified by an issuing agency...and
transmit[ted] to the client device**

293. Stafford's system generates key signatures to release sensitive files. These signatures can comprise hash values (IdSig1 and IdSig2), which can either be displayed to the user or transmitted electronically to the user's device (e.g., by email). EX1012, [0097]-[0099]. The credential to be released is stored in an encrypted format using one-time pads (referred to as IdSecPad and IdPad), and the hash values are of the credential's one-time pads, thereby identifying the encrypted credential. EX1012, [0116]-[0022]. The release of the credential is authorized by comparing the hash values to the IdSecPad and IdPad corresponding to the credential, with a match indicating that release is authorized. A hash value acts as a virtual representation of the stored credential, and is derived based on the information associated with the credential, so generating the hash values or similar key signature corresponds to the step of generating the OVER file.

294. Stafford teaches that its encrypted credentials may be verified by the issuer and may include storing an image of the credential (e.g., a scanned copy). EX1012, [0062], [0065], [0067]. However, to the extent that Stafford does not expressly teach that the files sent to the user (e.g., containing hash values) include

a virtual representation verified by the issuing agency, this portion of the limitation is disclosed by Purves.

295. Purves teaches that a user device (e.g., a device implementing a digital wallet) may be sent an image of a credential (e.g., an image of a credit card provided by an issuer) to conveniently represent a real credential. EX1013, [0102], [0108]-[0109]. The image of a card may expressly be “from an issuer.” EX1013, [0085]. The server may also generate an on-the-fly image of the credential to be used to represent the credential on the user’s device, optionally with “confidential information ... obscured.” EX1013, [0122]; see also *id.*, [0111]-[0112] (“multiple versions of the card” may be used in various formats). A representative image provided “from an issuer” would be “verified by the issuing agency” as an official representation, as would an image produced from an actual credential, since an actual credential naturally represents itself.

296. In view of Purves’s teaching to provide user devices with images representing a credential (such as a credit card), it would have been obvious to use similar credential images in the context of Stafford. For example, the system would provide an image of the user’s credential (e.g., a generally-representative, issuer-provided image provided by the issuer or a real image of the credential with optionally-obscured confidential information) along with the encoded key signature to remind users which credential the key signature represents and enable

quick selection from among a plurality of options available on the user's device.

See EX1013, [0085], [0122]. Such an image would be a virtual representation verified by the issuer as being an official representation of the credential.

accessing the OVER file

297. Stafford teaches that the key signatures and other information may be provided to a verifying device (IdBus1) "online or in person," and that the "delivery process may vary" based on the information provided and the recipient. EX1012, [0106]-[0113]. Stafford thus expressly suggests including other information with its key signatures and employing various known delivery processes. Such known processes and information would include using an optical scan in the delivery process, as taught by Neafsey, in addition to the virtual representation of a credential taught by Purves, as discussed above. In particular, Neafsey teaches that credentials may be provided in varying formats specific to user devices, including by keying formats to unique device IDs. EX1015, [0048]-[0049], [0061]; EX1016, 9-10, 12. Such formats include optically-scannable formats, such as QR and bar codes. EX1015, [0061]; EX1016, 12. As discussed above, in ¶280, it would have been obvious to use such optically-scannable codes to encode Stafford's key signatures, allowing them to be transferred to the recipient (IdBus1) in a simple, reliable manner. Such a scan of the OVER file would

constitute “accessing of the OVER file by the OVER file verifying device” recited in limitation 1.1.

298. Stafford, Purves, and Neafsey thus teach or suggest each limitation of element 1.1.

3. Limitation 1.2

299. Stafford, Purves, and Neafsey teach limitation 1.2. As illustrated in Fig. 3, Stafford teaches that a third-party client verifying device (referred to as IdBus1, see EX1012, [0108]) sends a request for release of information to the credential-database system. EX1012, [0115]; Fig. 3 (as marked up above in ¶292).

300. The request includes the key signatures IdSig1 and IdSig2, which are used to verify that the OVER file (encoding the signatures) authenticates the user, as only if the key signatures match the hash values of the encrypted credential file are the credential files transmitted. See EX1012, [0119]-[0122].

301. As discussed above in ¶292, it would have been obvious to provide the key signatures encoded as an optically scannable code in light of the teachings of Neafsey and Purves. See EX1015, [0065]; EX1016, 12; EX1013, [0064]. Doing so would allow the user to more easily transmit the key signature to a third party using an optical scan. The optical encoding would be scanned by the third-party device to provide the key signatures used in step 302 of Stafford’s Fig. 3. The

scanning of this code by the OVER file verifying device corresponds to the recited accessing of the OVER file.

4. Limitation 1.3

302. Stafford in view of Purves and Neafsey teaches this limitation.

Stafford's system responds to the request discussed for limitation 1.2 (and thus the associated scan of the code taught by Neafsey) by comparing the encoded hash values IdSig1 and IdSig2 of the key signature. EX1012, [0115]-[0121], Fig. 3 (marked up below).

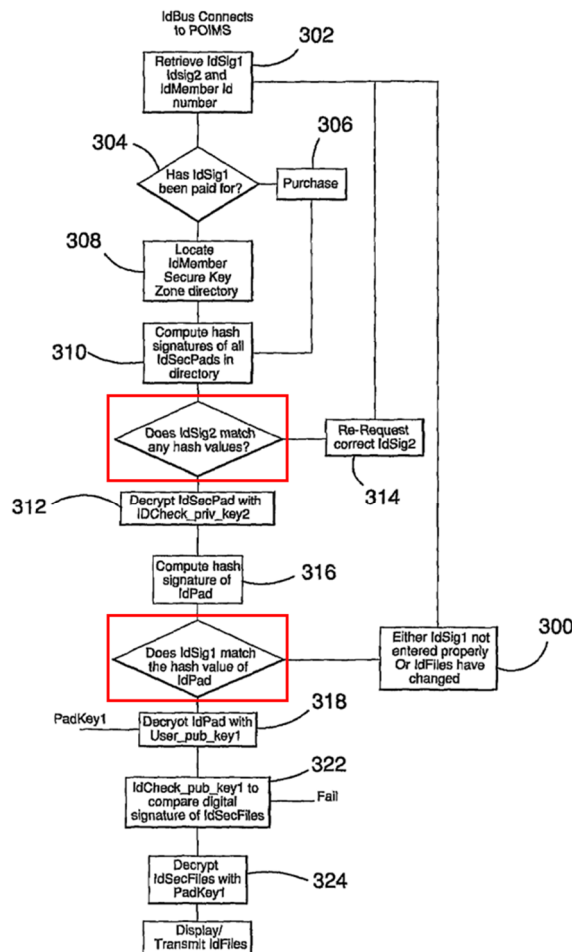


FIGURE 3

303. This comparison verifies that the scan (which provides the key signatures) corresponds with the information associated with the credential (since it matches the encrypted credential's hash values). See EX1012, [0093] (IdFiles (credentials) encrypted with one-time pad) [0115]-[0122] (hash values match credential's one-time pad).

304. Stafford teaches that an authenticating message is received by the third-party device with a first indication of whether the scan corresponds to the first OVER file. For example, where either key signature fails to match, an appropriate message is sent to re-request the non-matching hash value. EX1012, [0120]-[0022]. Fig. 3 (see blocks 314 and 300 in Fig. 3 at ¶302). Alternatively, if the key signatures match, a decrypted copy of the IdFiles is transmitted to the third-party device. EX1012, [0120]-[0126]. These alternatives, indicated in Fig. 3, both correspond to the recited authentication message, since a re-request message indicates a lack of correspondence and the sending of the IdFiles indicates a successful correspondence between the credential information and the recited scan.

5. Limitation 1.4

305. Stafford in view of Purves and Neafsey teaches “outputting a first status indicator expressing whether the first OVER file authenticates the user,” as recited in limitation 1.4. For example, when “IdSig does not match the hash value... request for re-entry of IdSig1 is made and the process retried.” EX1012,

[0122]. This request for re-entry is an indicator expressing that the first OVER file did not authenticate the user. In the alternative, if the key signatures match, “decrypted and released IdFiles can then be transmitted or displayed to IdBus1 for use in the necessary data comparison and credential verification,” which is an indicator that the OVER file authenticates the user. EX1012, [0126].

6. Limitations 1.5-1.8

306. As discussed above in Ground 1, limitations 1.5-1.8 repeat, respectively, limitations 1.1-1.4 as applied to a second OVER file that is a second credential on a second client device scanned by the OVER file verifying device, with the second OVER file being invalid for use on the first client device. *Supra* ¶¶236-237. These limitations would have been obvious over the combination of Stafford, Purves, and Neafsey.

307. It would have been obvious to provide a second OVER file comprising a second encoded key signature to a second device of the user, as Neafsey teaches that different devices may receive different virtual credentials in different formats corresponding to the particular device. See EX1015, [0061]; EX1016, 12. As Neafsey discloses, each such virtual credential would be generated using the “unique device ID” of the recipient device, meaning that each credential would be limited to being used on a particular device matching the device ID. EX1015, [0048]-[0049]; EX1016, 10-11. A POSITA would have understood that

different client devices would sometimes require using different formats appropriate to each device. See ¶279. In such a case, by limiting each type of format to a particular device according to the device ID, the encoded key signatures of a first device would be invalid for use on a second device, and the encoded key signatures of the second device would be invalid for use on the first device.

308. In such a combination, the “second OVER file” (second encoded key signature) would be present on and accessed and “scanned at the second client device” by the recipient’s verifying device, and it would constitute a “second new credential” that is “invalid for use in the first OVER file client device for authenticating the user.” The remainder of limitations 1.5-1.8 would have been obvious for the same reasons as limitations 1.1-1.4.

309. Accordingly, claim 1 was obvious over the combination of Stafford, Purves, and Neafsey.

C. Claim 8

310. Claim 8 is an apparatus form of claim 1, and was obvious over the combination of Stafford, Purves, and Neafsey for essentially the same reasons as for claim 1.

1. Preamble

311. Whether or not the preamble is limiting, Stafford, Purves, and Neafsey teach an OVER file verifying device (Stafford's IdBus1 configured as taught by Stafford, Purves, and Neafsey).

2. Limitations 8.1-8.2

312. Stafford, Purves, and Neafsey teach the processor and memory recited in limitations 8.1-8.2.

313. Stafford discloses a computer-implemented "system 100 for storing, validating and disseminating credential information about an entity," which may be connected "to a computer network such as the Internet." EX1012, [0054]; *see id.*, Fig. 1 (depicting system 100 as a system comprising computers). Thus, Stafford discloses a computer apparatus that stores credential information. A POSITA would have understood that such a system would include a processor coupled to a memory unit storing instructions and the user's credential information.

314. Stafford further describes that the recipient (IdBus1) is a computer-based device that would include the recited processor and memory. For example, Stafford repeatedly refers to the systems of IdBus1 interfacing with the credential system and other computer components, including allowing "IdBus1 systems to interface with the system 100 i.e. a common interface" and placing data "into a format parseable by IdBus1's systems (e.g. XML)." EX1012, [0110]-[0012]; *see also id.*, [0128] (IdBus1 computes and compares hash values). A POSITA would

have understood that such a device would be a computing device comprising a processor and memory storing instructions and other data. Among this stored data would be information associated with an original credential of a user—for example, IdBus1 not only receives the key signatures (which are directly associated with the original credential) but also receives “decrypted and released IdFiles” (i.e., copies of the original credential images stored by Stafford’s system). EX1012, [0115], [0126].

315. Purves confirms that such a computer system would include a processor and memory. For example, Purves teaches that “computers employ processors to process information,” which “may be referred to as central processing units (CPU),” and which operate on “instructions and data in various processor accessible and operable areas of memory.” EX1013, [0127]; *see also id.*, [0132] (CPU “execute[s] stored instructions (i.e., program code) according to conventional data processing techniques”). Purves details components present in typical computer systems, including CPUs and memory to store information and instructions. EX1013, [0131]-[0149]; *see also* EX1015, [0030]-[0034] (similar components for virtual credential-receiving device); EX1016, 6-8.

3. Limitations 8.3-8.10

316. Elements 8.3-8.10 are almost verbatim copies of elements 1.1-1.8, respectively, with no substantive differences relative to the mapping discussed

above for claim 1. *See supra* ¶¶287-308. Accordingly, Stafford, Purves, and Neafsey teach elements 8.3-8.10 for similar reasons as those discussed for 1.1-1.8 above.

317. Therefore, claim 8 was obvious over the combination of Stafford, Purves, and Neafsey.

D. Claim 15

318. Claim 15 recites a “non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to perform operations comprising” a series of steps recited in elements 15.1-15.8. As discussed above for claim 8, Stafford, Purves, and Neafsey teach a verifying device (merchant server and point-of-sale terminal) storing instructions in a memory unit to be executed by a processor to perform the steps of claim 8. *Supra* ¶¶311-317. These steps (elements 8.3-8.10) are identical to the steps recited in limitations 15.1-15.8, respectively, with the only differences being that limitation 15.1 recites “an original credential” and “a user,” and does not expressly recite that the OVER file is a new credential. Thus, claim 15 was obvious over Stafford, Purves, and Neafsey for similar reasons to claim 8. See also *supra* ¶¶285-308 (substantively identical elements for claim 1).

319. Therefore, claim 15 was obvious over the combination of Stafford, Purves, and Neafsey.

E. Claims 2, 9, and 16

320. As discussed in ground 1, claims 2, 9, and 16 are materially identical, requiring the use of device identifiers for use in authenticating the user. The combination of Stafford, Purves, and Neafsey renders these claims obvious.

321. As discussed above for claim 1, Neafsey teaches generating different credentials for different devices based on a “unique device ID” of the recipient device. EX1015, [0049], [0061]; EX1016, 9, 12. A POSITA would have used such device IDs to tie encodings of Stafford’s key signatures to a given device, to ensure that each device received an appropriately encoded key signature. Doing so would limit a given encoded key signature to a given device by including such device IDs in a first OVER file containing Stafford’s encoded key signatures. In particular, this would limit the first OVER file to the first device. Moreover, this step would be performed “for use in authenticating the user using the information of the original credential,” since the purpose of Stafford’s key signatures is to authenticate the user by matching the information of the original credential (via the hashes of the one-time pads used to encrypt it), which would be furthered by the use of device IDs to ensure the encoded key signatures were used by the devices configured to display them appropriately.

322. Therefore, claims 2, 9 and 16 were obvious over the combination of Stafford, Purves, and Neafsey.

F. Claims 3-4, 10-11, and 17

323. Stafford teaches storing user-specific information, including the specific categories listed in claim 3-4, 10-11, and 17. For example, associated with its stored credentials, Stafford stores location information (addresses) as well as encrypting a private key that is stored “using a biometric such as a fingerprint or password.” EX1012, [0053], [0071]. Further, as discussed above for claims 2, 9, and 16, it would have been obvious to include a device identifier in Stafford’s OVER file to limit encoded key signatures to appropriate devices, which would specifically constitute user-specific information included in a first OVER file, as recited in claims 3-4, 10-11, and 17.

324. Therefore, claims 3-4, 10-11, and 17 were obvious over the combination of Stafford, Purves, and Neafsey.

G. Claims 5 and 12

325. Stafford teaches storing scans of a credential. EX1012, [0062], [0067]. As discussed for claim 1, it would have been obvious in view of Purves to include an image of a portion of a stored credential in an OVER file. Supra ¶277; EX1013, [0122] (credential image with confidential information obscured).

326. Therefore, claims 5 and 12 were obvious over the combination of Stafford, Purves, and Neafsey.

H. Claims 6 and 13

327. Stafford teaches that certain information “has a validity date associated” and “remains current only for a pre-determined set of time before it requires revalidation.” EX1012, [0135]. It would have been obvious to a POSIA to send an authentication message comprising an indication that the OVER file was expired, either because the credential itself had expired or because elements of the OVER file (e.g., the key signatures) had expired. This was a conventional practice in credit card transactions.

328. For example, Stafford contemplates a credential including a driver’s license, which a POSITA would have known would generally include an expiration date; for such a credential, an issuer would respond that the credential was not valid if it had expired. EX1012, [0004]; *see id.*, [0135] (“Certain IdMember information remains current only for a pre-determined set of time....”). In such a case, it would have been obvious to receive a corresponding status indication (such as “not verified,” “expired,” etc.) from the issuer and send it to the recipient along with the credential authorized for release by the user.

329. Stafford further teaches that the key signatures themselves may expire. For example, Stafford teaches that an IdSig may not match the hash value of an IdPad if the “IdPad has changed since the hash key signature was created.” EX1012, [0122]. This would be an example of Stafford’s key signature expiring due to passage of time. As a further example, Stafford teaches that the key

signatures may be limited by a “set amount of attempts” before becoming invalid.

If the keys do not match despite a re-attempt, the transmission of data is aborted. It would have been obvious to a POSITA, considering this discussion of Stafford, that it would be advantageous to send an authentication message to the third-party verification device that the key signatures of the OVER file had expired.

330. Therefore, claims 6 and 13 were obvious over the combination of Stafford, Purves, and Neafsey.

I. Claims 7 and 14

331. Stafford teaches accessing, by the verifying device, from the first OVER file client device, additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been satisfied. For example, Stafford teaches that the “first OVER file client device” (IdMember’s device) may provide the “verifying device” (IdBus1) with a member identification number (MIN) in addition to the key signatures. EX1012, [0052], [0108]-[0113]. This MIN is sent with the key signatures by its IdBus1 to the system, which uses the MIN (1) to confirm that payment for data release was received, and (2) to locate the user’s credential information for release. EX1012, [0115]-[0116], [0118]. Each of these is a secondary condition for authorizing the user. Thus, the MIN is “additional credential information associated with the first

OVER file indicating whether a secondary condition for authorizing the user has been satisfied.”

332. Therefore, claims 7 and 14 were obvious over the combination of Stafford, Purves, and Neafsey.

XII. CONCLUDING STATEMENT

333. Relying on my education, experience, skill, and training in the relevant field of art, and after reviewing the materials identified above, it is my opinion that each of the Challenged Claims is invalid.

XIII. JURAT

334. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination remotely within the United States during the time allotted for such cross-examination at a time and place agreed by counsel.

335. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false

Declaration of Michael I. Shamos

U.S. Patent 9,954,854

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.

Executed January 26, 2024 at Pittsburgh, PA

By: Michael Ian Shamos
Michael Ian Shamos