UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

Case No. IPR2024-00490
U.S. Patent No. 11,329,973

DECLARATION OF SAM MALEK

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND AND QUALIFICATIONS 2

III. MATERIALS CONSIDERED 7

IV. SUMMARY OF ASSERTED GROUNDS 9

V. RELEVANT LAW 10

VI. LEVEL OF ORDINARY SKILL IN THE ART 15

VII. CLAIM CONSTRUCTION 16

A. "OVER file" 16

B. "verified by an issuing agency" 16

VIII. OBORNE GROUNDS 1-2 17

A. "verified by an issuing agency to be an official representation of the credential" 17

1. Issuing Agency Verification In The '973 Patent 18

2. Oborne Does Not Teach A Token "verified by an issuing agency to be an official representation of the credential" 18

B. Complexity of Digital Payment Systems Technology 25

C. User Authentication in Oborne 35

D. Claims 2, 9, and 17: "second OVER file" 42

1. Oborne Does Not Suggest "generating… a second over file comprising a second virtual representation of the credential" 44

2. Oborne Does Not Suggest "a second OVER file" That Is "invalid for use in the first over file storage client device" 49

IX. STAFFORD GROUNDS 3-4 52

A. Public/Private Key Encryption in Stafford 52

B. Stafford Does Not Teach Or Suggest An "OVER File" That Is "based on the information associated with the credential of the user" 54

C. Stafford's Key Signatures Do Not Meet The Claimed "OVER file comprising a virtual representation of the credential that has been verified by an issuing agency" 63

D. Security Risks of Sending Credential Images 66

X. CONCLUSION 77

XI. APPENDIX: LIST OF CHALLENGED PATENT CLAIMS 78

I, Sam Malek, hereby declare as follows:

I. INTRODUCTION

1. I have prepared this Declaration in connection with Patent Owner's Response to Visa's Petition for *Inter Partes* Review challenging U.S. Patent No. 11,329,973 ("the '973 Patent").

2. I have been retained by Cortex MCP, Inc. ("Cortex" or "Patent Owner") as an expert in the field of electronic authentication, credentialing systems, and mobile security. I have been asked to provide testimony about Cortex's U.S. Patent No. 11,329,973 challenged by Visa in this IPR and to respond to selected opinions of Visa's expert Dr. Michael Shamos. The full text of the challenged claims appears in Appendix A to this Declaration.

3. I understand that Visa filed a challenge to the '973 Patent in IPR2024-00490. I will address selected aspects of this challenge in this Declaration.

4. I am being compensated at my normal consulting rate for my time and reimbursement for expenses incurred in the course of my work. My compensation is not dependent on the outcome of this case, and in no way affects the substance of my statements in this Declaration. I have no financial interest in Cortex, the '973 Patent, or the owner of the '973 Patent.

II. BACKGROUND AND QUALIFICATIONS

5. My background, experience, and qualifications are set forth in my *curriculum vitae*, which I understand is submitted as Exhibit 2010.

6. I am currently a Full Professor of Software Engineering with tenure in the School of Information and Computer Sciences at the University of California, Irvine ("UCI"). I am the Director of UCI's Software Engineering and Analysis Laboratory (SEAL). Previously, I was the Director of the Institute for Software Research at UCI from 2018-2022. Prior to my time at UCI, I was an Associate Professor at George Mason University from 2007-2015 and a graduate researcher at the University of Southern California from 2003-2007.

7. I have approximately 25 years of experience in the fields of computer and software technology including mobile payment systems and electronic credentials in a variety of roles: from software engineer, software architect, and programmer at various companies to researcher and professor at several universities.

8. I have extensive education in the general field of computing technology. I received a Bachelor of Science degree in Information and Computer Science from the University of California, Irvine in 2000, a Master of Science in Computer Science from the University of Southern California in 2004, and a Ph.D. in Computer Science from the University of Southern California in 2007.

9. I have received numerous awards for my scientific contributions to the field of Computer Science, including the Test of Time Award in 2020 from the Association for Computing Machinery, CAREER award from the National Science Foundation in 2013, Emerging Researcher/Scholar/Creator award from GMU in 2013, and Computer Science Department Outstanding Faculty Research award from GMU in 2011.

10. Software systems and results produced in my research lab have been adopted for use by various organizations in both private (e.g., Boeing, Bosch) and public (e.g., NASA, DHS, FBI) organizations.

11. I am a member of numerous professional organizations, including the Association for Computing Machinery ("ACM"), ACM Special Interest Group on Software Engineering ("SIGSOFT"), and the Institute of Electrical and Electronics Engineers ("IEEE").

12. My research is in the field of software engineering, and to date my focus has spanned the areas of software design and architecture, distributed and embedded systems, smartphone and mobile computing, internet and web technologies, middleware, service-oriented computing, autonomic computing, software testing and analysis, and software dependability and security. I have undertaken substantial research on the security of mobile platforms, resulting in dozens of publications. I highlight a few examples below. I led a team of researchers in a project sponsored

by the United States Defense Advanced Research Projects Agency (DARPA) to develop a novel approach for protecting Android applications from Inter-Process Communication (IPC) security attacks. The project resulted in the development of a tool called COVERT. I have published extensively on this work, including a highly cited manuscript that appeared in the IEEE Transactions on Software Engineering in 2015. I also led a team of researchers in a project sponsored by the United States Department of Homeland Security (DHS) to detect Android malware through the use of program analysis and machine learning techniques. This work resulted in a tool called RevealDroid, which was adopted for use by the DHS and FBI for vetting the security of mobile applications. I published the results of this work in the ACM Transactions on Software Engineering and Methodology in 2018. In another project, I developed DelDroid, which is the first approach for automated determination and enforcement of least privilege architecture in Android. This work was published in the Journal of Systems and Software in 2019.

13. I have authored over 130 research papers that have been published in peer-reviewed scientific journals and conferences. These publications have been highly cited: more than 11,000 times, according to Google Scholar (scholar.google.com).

14. I have received approximately $12 million in research grants from a variety of organizations, including the National Science Foundation (NSF), Federal

Bureau of Investigation (FBI), Air Force Office of Scientific Research, Department of Homeland Security (DHS), National Security Agency (NSA), Defense Advanced Research Projects Agency (DARPA), Office of the Director of National Intelligence, and Army Research Office, among others.

15. I also teach graduate- and undergraduate-level software engineering and computer science courses at UCI. For example, I taught a mobile software engineering class to graduate level software engineering M.S. and Ph.D. students where I covered topics related to mobile computing, including state-of-the-art solutions for achieving software security in mobile applications. I also taught a course on Internet Applications Engineering, as part of which I covered technologies for building e-commerce applications, including various ways in which customer payments can be processed in mobile and web e-commerce applications. I also taught a course on Distributed Software Architecture, as part of which I covered topics related to electronic credential management, encryption techniques, and authentication methods.

16. I also have professional experience as a software engineer, software architect, and programmer at numerous companies from 1998-2007, including the Boeing Company, PricewaterhouseCoopers Consulting (later acquired by International Business Machines (IBM) Corporation), FieldCentrix, and Neural Computing Systems Lab. With respect to the subject matter of the technology at

issue in this case, namely mobile software and payment technology, my experience in this area goes back to the late 1990s when I was employed as a software engineer at FieldCentrix. FieldCentrix developed mobile applications for field technicians (e.g., service personnel of utility companies). These mobile applications provided a variety of capabilities, including the ability to dispatch service requests, retrieve information about service jobs, collect payments, and create invoices.

17. I have served as an expert witness in approximately 80 prior litigation matters, many of which involved mobile or payment processing technologies. For example, in a litigation matter involving two banks, USAA v. PNC Bank, my testimony helped the jury determine USAA's check processing functionality was not infringing certain patents asserted by PNC Bank.

18. I have been a frequent speaker at scientific conferences, symposia, workshops, and gatherings of software engineering academics and professionals on topics related to the technologies at issue in this case. For example, I was invited by the Association for Computing Machinery to give a talk in 2020 titled, "*The Threat in Your Pocket: Trends, Challenges, and Solutions in Mobile Application Security*."

19. On more than 150 occasions, I have served as a chair, editorial board member, organizer, and reviewer for leading computer science journals, magazines, and conferences that publish cutting-edge advancements in the field. In these roles, I have refereed hundreds of articles submitted by the scientific community for their

novelty and contribution to the existing body of knowledge. Many of these submissions have dealt with topics that are directly related to the technologies at issue in this case, namely mobile computing, payment processing, and authentication and verification of credentials.

III. MATERIALS CONSIDERED

[Paragraphs 20-21 reserved.]

22. I reviewed the following materials from IPR2024-00490 in preparing this Declaration:

a. Petition for *Inter Partes* Review (Paper 2);

b. Patent Owner Preliminary Response (Paper 6); and

c. Decision Instituting *Inter Partes* Review (Paper 7).

23. I reviewed the following exhibits, as well as any documents cited or referenced in this Declaration:

Exhibit No.	Description
1004	U.S. Patent No. 11,329,973
1005	Declaration of Dr. Michael Ian Shamos
1019	File history for ’973 Patent
1011	U.S. Patent Application Publication No. 2012/0316992 (“Oborne”)
1012	U.S. Patent Application Publication No. 2009/0271321 (“Stafford”)
1013	U.S. Patent Application Publication No. 2013/0054454 (“Purves”)

Exhibit No.	Description
1014	U.S. Patent Application Publication No. 2012/0310838 ("Harris")
1015	U.S. Patent Application Publication No. 2013/0212248 ("Neafsey")
1016	U.S. Provisional Patent Application No. 61/598,219 ("Neafsey Provisional")
1017	U.S. Patent Application Publication No. 2008/0270166 ("Morin")
1019	Steiner et al., *Kerberos: An Authentication Service for Open Network Systems*, Usenix Winter (1988)
1020	Cross River, *Tokenization in Card Networks,* (May 2023)
1021	U.S. Patent No. 7,014,107 ("Singer")
1022	Heather Mark, *Shift4: Secure Payment Processing*, (2006)
1023	Tom Arnold, *Credit Card Information Surrogate: A Method and System for using surrogates to integrate PCI-level security for legacy information systems*, (2007)
1024	Brown et al., *Microsoft Code Name "Geneva" Framework Whitepaper for Developers*, (2008)
1025	Thakar et al., *PCI Compliance for Dummies*, (2009)
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)
1028	U.S. Patent Application Publication No. US20090249082 ("Mattsson")
1031	Richard J. Sullivan, *The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy*, (2010)
1034	U.S. Patent No. 8,458,487 ("Palgon")
1042	U.S. Patent Pub. No. US 2011/0251892 ("Laracey")
2001	U.S. Patent No. 9,996,835 to Visa
2002	U.S. Patent Publication No. 2007/0208665 to Ohara ("Ohara")

Exhibit No.	Description
2003	U.S. Patent No. 8,540,149 to Chu ("Chu")
2004	Defendant Visa Inc.'s Invalidity Contentions, *Cortex MCP, Inc. v. Visa Inc.*, Case No. 5:23-CV-05720 (N.D. Cal. Mar. 15, 2024)
2005	U.S. Patent Publication No. 2009/0307756 to Kang ("Kang")
2006	U.S. Patent Publication No. 2012/0240204 to Bhatnagar et al., ("Bhatnagar")
2013	Cortex's Reply Claim Construction Brief, *Cortex MCP, Inc. v. Visa Inc.*, Case No. 5:23-CV-05720, Dkt. No. 105 (N.D. Cal. July 19, 2024)
2016	Transcript of September 25, 2024 Deposition of Dr. Michael Shamos
2017	Martin E. Hellman, *An Overview of Public Key Cryptography*, IEEE Communications Society Magazine (Nov. 1978)
2018	Christian Boyce, *iOS 8 Tip #8: Make and Answer Phone Calls From Your iPad* (Apr. 13, 2020), https://christianboyce.com/ios-8-tip-8-make-and-answer-phone-calls-from-your-ipad/#google_vignette

IV. SUMMARY OF ASSERTED GROUNDS

24. The 490 Petition only alleges the claims are unpatentable for obviousness under 35 U.S.C. § 103. The grounds and challenged claims are summarized in the following table:

Ground	490 Claims Challenged	References
1	1-2, 4-7, 16-17	Oborne
2	3, 8-15	Oborne and Purves

Ground	490 Claims Challenged	References
3	1, 3, 5-8, 10, 12-15	Stafford and Purves
4	2, 4, 9, 11, 16-17	Stafford, Neafsey, and Purves

V. RELEVANT LAW

25. I am not an attorney. For the purposes of this Declaration, I have been informed about certain aspects of the law that are relevant to my opinions. My understanding of the law is summarized below.

26. I have been informed and understand that determining whether a patent claim is valid requires a two-step analysis. First, the claim must be construed. Second, the properly construed claim must be compared to the prior art.

27. I have been informed and understand that claim construction is a matter of law and that the final claim constructions for this proceeding will be determined by the Patent Trial and Appeal Board.

28. I have been informed and understand that in the context of an *inter partes* review, claims are construed from the perspective of a person of ordinary skill in the art at the time of the purported invention (which is approximated based on the earliest priority date of the patent). I understand that absent disclaimer or express definition, claim terms are given their plain and ordinary meaning to a person of

ordinary skill in the art in view of the specification, file history, and knowledge of a person of ordinary skill in the art.

29. I have been informed and understand that a patent claim is obvious and therefore invalid if the claimed subject matter, as a whole, would have been obvious to a person of ordinary skill in the art as of the priority date of the patent based on one or more prior art references and/or the knowledge of one of ordinary skill in the art. I understand that an obviousness analysis must consider (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) secondary considerations, if any, of non-obviousness (such as unexpected results, industry praise, commercial success, long-felt but unmet need, failure of others, copying by others, and skepticism of experts).

30. I understand that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. § 103. I understand that a reference may also be combined with the knowledge of a person of ordinary skill in the art, and that this knowledge may be used to combine multiple references. I further understand that a person of ordinary skill in the art is presumed to know the relevant prior art. I understand that the obviousness analysis may take into account the inferences and creative steps that a person of ordinary skill in the art would employ.

31. In determining whether a prior art reference could have been combined with other prior art or other information known to a person having ordinary skill in the art, I understand that the following principles may be considered:

a. A combination of familiar elements according to known methods is likely to be obvious if it yields predictable results;

b. The substitution of one known element for another is likely to be obvious if it yields predictable results;

c. The use of a known technique to improve similar items or methods in the same way is likely to be obvious if it yields predictable results;

d. The application of a known technique to a prior art reference that is ready for improvement, to yield predictable results;

e. Any need or problem known in the field and addressed by the reference can provide a reason for combining the elements in the manner claimed;

f. A person of ordinary skill often will be able to fit the teachings of multiple references together like a puzzle; and

g. The proper analysis of obviousness requires a determination of whether a person of ordinary skill in the art would have a "reasonable expectation of success" – not "absolute

predictability" of success – in achieving the claimed invention by combining prior art references.

32. I understand that an obviousness analysis can consider common sense and common knowledge if explained with sufficient reasoning. I have been informed that to avoid impermissible use of hindsight, common sense cannot be used to fill a missing limitation or provide a motivation to combine without reasoned analysis and evidentiary support. I have also been informed that even with reasoned analysis and evidentiary support, courts have only permitted common sense to fill a missing limitation when the missing limitation was unusually simple and the technology was particularly straightforward, such as where the missing limitation was merely repeating earlier steps already taught by the prior art.

33. I am informed that whether a prior art reference invalidates a patent claim as obvious is determined from the perspective of a person of ordinary skill in the art. There is no requirement that the prior art contain an express suggestion to combine known elements to achieve the claimed invention, and a suggestion to combine known elements to achieve the claimed invention may come from the prior art as a whole or individually, as filtered through the knowledge of one skilled in the art. In addition, the inferences and creative steps a person of ordinary skill in the art would employ are also relevant to the determination of obviousness.

34. When a work is available in one field, design alternatives and other market forces can prompt variations of it, either in the same field or in another. If a person of ordinary skill in the art can implement a predictable variation and would see the benefit of doing so, that variation is likely to be obvious. In many fields, there may be little discussion of obvious combinations, and in these fields market demand – not scientific literature – may drive design trends. When there is a design need or market pressure and there are a finite number of predictable solutions, a person of ordinary skill in the art has good reason to pursue those known options.

35. It is my understanding that there is no rigid rule that a reference or combination of references must contain a "teaching, suggestion, or motivation" to combine references, but I understand that the "teaching, suggestion, or motivation" test can be a useful guide in establishing a rationale for combining elements of the prior art. This test poses the question as to whether there is an express or implied teaching, suggestion, or motivation to combine prior art elements in a way that realizes the claimed invention, and it seeks to counter impermissible hindsight analysis.

36. It is also my understanding that to render a claim obvious, the prior art, taken as a whole, must enable a skilled artisan to make and use the claimed invention. I understand that if an obviousness case is based on a non-self-enabled reference and no other prior art reference or evidence would have enabled a skilled artisan to make

the claimed invention without undue experimentation, then the invention cannot be said to have been obvious.

VI. LEVEL OF ORDINARY SKILL IN THE ART

37. Dr. Shamos opines that:

> one of ordinary skill in the art of the ’973 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.

EX1005 (Shamos Declaration) ¶78.

38. The Board adopted this definition of the level of skill in the art, with the additional requirement that a person of ordinary skill in the art could have less education but significant professional experience in one of these fields. 490 Institution Decision at pages 14-15.

39. I agree with this definition of the level of skill in the art for the ’973 Patent. I also agree with the additional requirement that more work or industry experience could offset less educational training, and more educational training could offset less work or industry experience.

40. As of the December 21, 2012 provisional date of the ’973 Patent, I had at least the background of one of skill in the art.

41. I have applied the Board's definition of the level of skill in the art throughout my analysis in this Declaration.

VII. CLAIM CONSTRUCTION

42. I have not been asked to provide an opinion on the construction of the following claim terms. For the purposes of this Declaration, I have been asked to review the Board's constructions in the Institution Decision and apply them in my analysis.

A. "OVER file"

43. In the Institution Decision, the Board found "that the term 'OVER file' encompasses a virtual representation of one or more credentials, to be used for verification of those credentials." Institution Decision at page 11. I applied this construction in my analysis.

[Paragraph 44 reserved.]

B. "verified by an issuing agency"

45. In the Institution Decision, the Board also interpreted "verified by an issuing agency" to require that "an issuing agency have verified a *virtual representation* in an OVER file as being an official representation of a credential." Institution Decision at page 13 (emphasis in original). I understand that this means that the claim language a "virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential"

requires that the issuing agency has verified the "virtual representation" (and not the "credential") to be "an official representation of the credential." I understand that the parties agree to this definition in substance. EX2013 (Cortex's reply claim construction brief) at pages 10-11. I also applied this construction and understanding in my analysis in this Declaration.

VIII. OBORNE GROUNDS 1-2

A. "verified by an issuing agency to be an official representation of the credential"

46. Every claim of the '973 Patent requires an "OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential." *See* EX1004 at cols. 22:1-4, 23:23-25, 24:44-47 (independent Claims 1, 8, 16). Because each of the independent claims requires this limitation, every dependent claim does as well.

47. As I explained in Paragraph 42 of this Declaration, I applied the Board's claim construction of these claim terms. In other words, the claim language "a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential" requires that the issuing agency has verified the "virtual representation" (and not the "credential") to be "an official representation of the credential."

48. As explained in this section of my Declaration, I disagree that Oborne teaches or suggests this claim limitation.

1. Issuing Agency Verification In The ’973 Patent

49. By way of background, the ’973 Patent teaches verification by an issuing agency. It discloses that an OVER file generation request may be sent to an OVER engine. EX1004 (’973 Patent) at col. 6:37-43. After the OVER engine receives this OVER file generation request, it may then “contact an issuing agency datastore, such as, for example, an issuing agency database 130, to verify the information contained in the OVER File generation request and to obtain additional credential information.” EX1004 (’973 Patent) at col. 6:48-53. In one example embodiment, the ’973 Patent describes the process for a user that requests an OVER file “representative of a driver’s license.” It explains:

> The OVER File database 128 may contact the issuing agency database 130, such as a state DMV database, and provide the driver’s license identification number to the issuing agency database 130. The issuing agency database may respond by indicating the validity of the requested credential containing the driver’s license identification number and may provide the legal name, address, and birth date of the person associated with the driver's license identification number.

EX1004 (’973 Patent) at col. 7:3-11.

2. Oborne Does Not Teach A Token “verified by an issuing agency to be an official representation of the credential”

50. I understand that Visa and Dr. Shamos are relying on Oborne’s “token… ‘linked to credit card information’” as being the claimed “OVER File

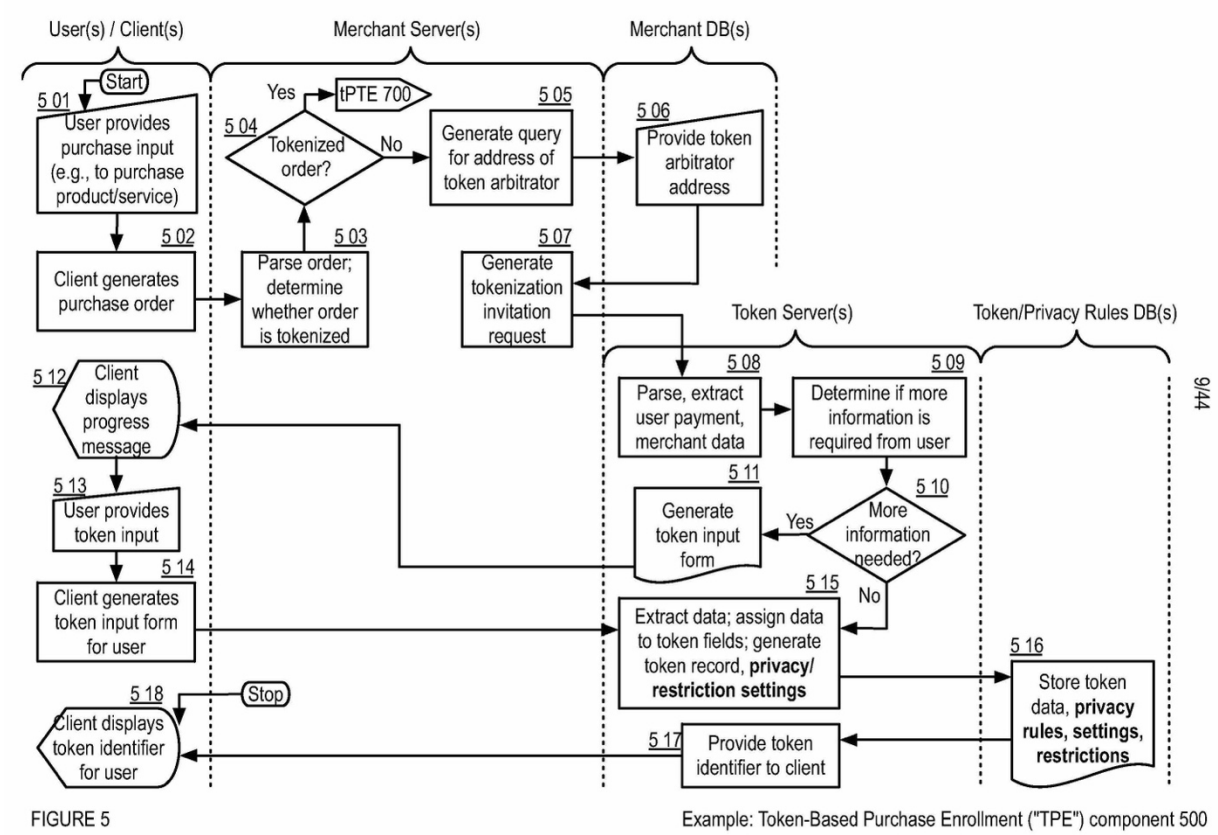
comprising a virtual representation of the credential." IPR Petition at pages 20-21; EX1005 (Shamos Declaration) ¶210. The Petition cites Oborne's Figure 5 and its accompanying descriptions in paragraphs 47-48 as teaching the process for generating Oborne's token. IPR Petition at page 20. Further, Dr. Shamos opines that "Oborne teaches or suggests that the token is verified by the issuing agency as an official representation." EX1005 (Shamos Declaration) ¶211. I disagree that Oborne discloses verification by the issuing agency.

51. Oborne (EX1011) explains its process of generating tokens in Figure 5. I've reviewed Oborne in general and, in particular, Oborne's Figure 5 and paragraphs 45-48 describing Figure 5, to determine whether Oborne teaches any verification by an issuing agency when its token is generated. Oborne does not.

52. Oborne's published figures have a low resolution. My declaration uses the higher-resolution images that Oborne submitted to the Patent Office during prosecution. *See* File History of Application No. 13/491,591 to Oborne; EX1011 (Oborne) at page 1 (item 21) (listing "Appl. No. 13/491,591"). These file history images should be and do appear to be identical to the images in Oborne (EX1011).

53. Oborne described Figure 5 as "a logic flow diagram illustrating example aspects of enrolling in a token-based purchase payment program in some embodiments of the PPT." EX1011 (Oborne) ¶10.

54. As shown in Figure 5 below, Oborne shows steps performed by different entities: "User(s) / Client(s)," "Merchant Server(s)," "Merchant DB(s)" or database(s), "Token Server(s)," and "Token/Privacy Rule DB(s)" or database(s):



EX1011 (Oborne) at Fig. 5.

55. To summarize: Oborne's process began with a user "enrolling in a token-based purchased payment program." EX1011 (Oborne) ¶45. The user used a "client" device "to purchase a product" or "service" and sent "a purchase order message to the merchant server" with a "client." EX1011 (Oborne) ¶45 (describing steps 501-502 in Figure 5). The "merchant server" may contact a "token server"

with "a tokenization invitation request on behalf of the user." EX1011 (Oborne) ¶45 (steps 503-507 in Figure 5). "If additional information is needed… the token server may generate a token input form" and send it to the user. EX1011 (Oborne) ¶46 (steps 508-511 in Figure 5).

56. "The client may generate a completed form, and provide, [in step] 514, the form to the token server…." EX1011 (Oborne) ¶¶46-47 (steps 512-514 in Figure 5). Then Oborne explains:

> The token server may obtain the form, and parse the form to extract data fields and values from the form to generate a token data record, e.g. [step] 515. For example, the token server may generate a unique and resolvable token identifier irrespective of the token requesting channel….

EX1011 (Oborne) ¶47 (step 515 in Figure 5).

57. After determining a set of privacy rules in step 516, Oborne's "token server may also provide a token identifier, e.g., [step] 517 to the client." EX1011 (Oborne) ¶48 (steps 516-517 in Figure 5).

58. Those are the required steps that Oborne describes to generate a token. In short, after the user completes a form to request a token in step 514, the token server simply "generate[s a] token data record" in step 515, as shown in Oborne's Figure 5 below:

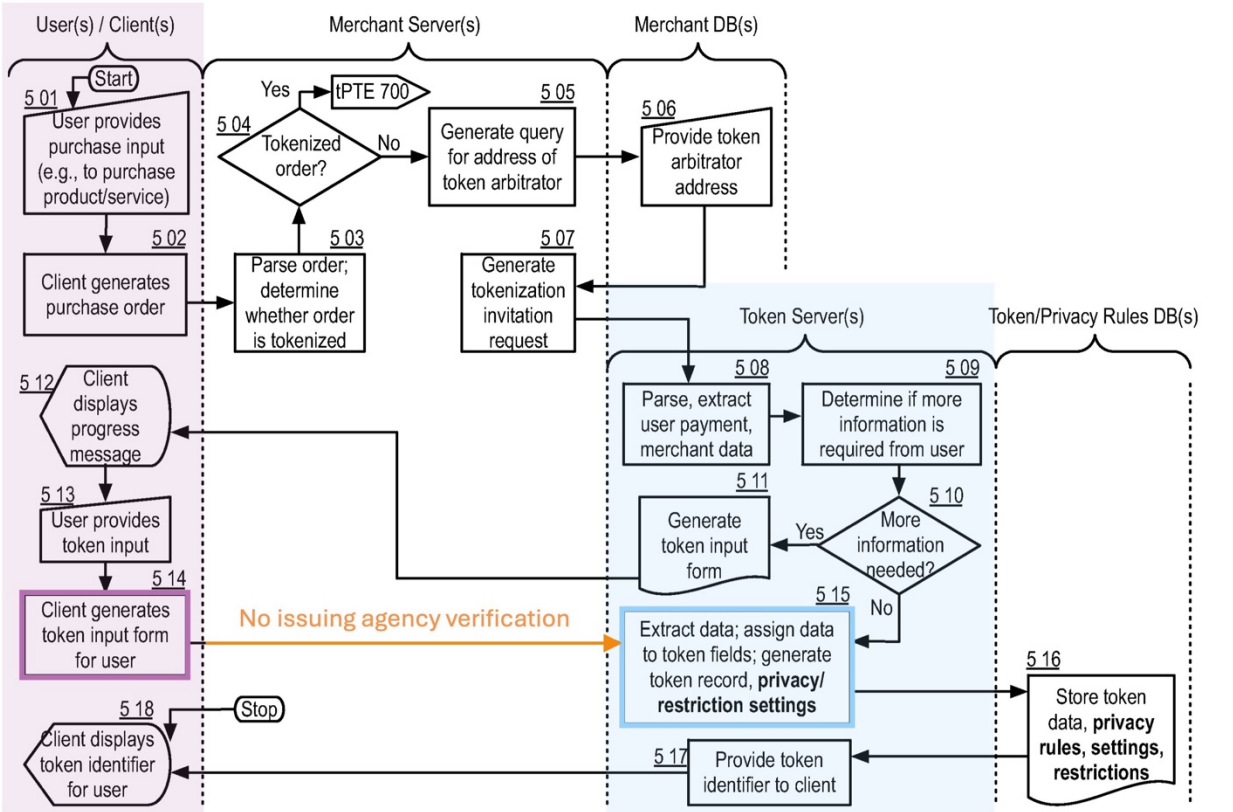


FIGURE 5 Example: Token-Based Purchase Enrollment ("TPE") component 500

EX1011 (Oborne) ¶¶46-47, Fig. 5 (annotated). There is no disclosed intermediate step between the user sending the form and the token server creating a "token data record."

59. In summary, when the token server (which Visa and Dr. Shamos identify as the claimed "OVER engine") generates the token in Figure 5 (which Visa and Dr. Shamos identify as the claimed "OVER file"), it has not been "verified by an issuing agency to be an official representation of the credential" as required by the claims of the '973 Patent. EX1011 (Oborne) ¶¶46-47, Fig. 5. Oborne contains no teaching of an issuing agency participating in the token server's token generation

process shown in Figure 5, let alone verifying the token. That claim limitation is absent from Oborne's disclosure.

60. Dr. Shamos appears to contend that issuing agency verification is implied by Oborne because "the token may be provided by the credential's 'funding source,' e.g., by the bank that issued the credit card (credential)." EX1005 (Shamos Declaration) ¶211 (citing EX1011 (Oborne) ¶¶29, 47-48, 53, 58). Dr. Shamos then asserts that "[b]y 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." EX1005 (Shamos Declaration) ¶211. Thus, Dr. Shamos reasons that in the event the issuer operates the token server and by virtue of operating the token server issues the token, it has somehow verified it to be an official representation of the credential. I disagree.

61. First, Dr. Shamos' opinion essentially reads the verification step out of the claims. All the independent claims require some form of "generating, by a processor of an OVER engine, an OVER file." EX1004 ('973 Patent) at cols. 22:1-2, 23:23 (Claim 8: "generate an OVER file"), 24:44-45 (Claim 16: same as Claim 1). The claims separately require that the OVER file comprise "a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential." EX1004 ('973 Patent) at cols. 22:1-4 (Claim 1), 23:23-25 (Claim 8), 24:44-47 (Claim 16). If, as Dr. Shamos contends,

simply generating the OVER file also verifies it as an official representation of the virtual credential, then the verification limitation is superfluous and has been effectively read out of the claims.

62. Second, a person of ordinary skill in the art would understand verification to require something more than generating a token. Verification indicates some kind of formal approval or confirmation by the issuing agency that what has been issued will act in place of the credential in the issuer's eyes when presented instead of the credential. Dr. Shamos points to nothing in Oborne indicating any kind of verification by an issuing agency that could correspond to this requirement. *E.g.*, EX1005 (Shamos Declaration) ¶211. Dr. Shamos' single paragraph containing only two sentences of explanation asserts that the issuer could operate the token server, but neither Oborne nor Dr. Shamos explains what this scenario would look like other than the same example of Figure 5 with its accompanying disclosure in Oborne. As I explained above, there is no indication in Oborne that the process of generating a token involves anything more than simple token generation as Oborne described. A person of ordinary skill in the art would not view generating a token as inherently or impliedly verifying the token as an official representation of a credit card absent some formal indication of approval or confirmation by the issuing agency. Oborne simply does not disclose any such formal indication of approval or confirmation by the token generator, much less the

issuing agency. Verification and generation are two separate acts, and a person of ordinary skill in the art would not understand them to be the same.

B. Complexity of Digital Payment Systems Technology

63. I understand that even if Oborne did disclose issuing agency verification (which it did not for the reasons I explained above), Visa and Dr. Shamos have argued that including issuing agency verification in Oborne would have been obvious. IPR Petition at page 22; EX1005 (Shamos Declaration) ¶211. Dr. Shamos argues that verification "would be a routine step." EX1005 (Shamos Declaration) ¶212. I understand this to mean that Dr. Shamos believes that verification was "routine," or a simple exercise of common sense.

64. As explained in Paragraph 32 of this Declaration, I understand that to use common sense to find a claim limitation obvious, the limitation must be unusually simple and the technology particularly straightforward. Having reviewed the Petition and Dr. Shamos' declaration, I do not see either of them assert, much less back up by evidence, that the verification limitation at issue in the '973 Patent is unusually simple or that the technology of the '973 Patent is particularly straightforward, even though my understanding is that they must show both to prevail. Thus, under the law as it has been explained to me, I do not see how Dr. Shamos or Visa have shown that the addition of the verification step would be "routine."

65. Nevertheless, I have been asked to provide an opinion about whether the verification limitation is unusually simple or whether the technology described in the ’973 Patent is particularly straightforward. The implementation of payment systems security is not unusually simple or particularly straightforward. As one of Visa’s exhibits explains: “When a merchant accepts a payment card, a complex system of devices, software, networks, service providers and the card acquirer is required to process the payment and get the money.” EX1025 (PCI for Dummies) at page 7. Instead, the ’973 Patent addresses a complex and evolving set of technical challenges. And the implementation and usefulness of verification in the context of the ever-evolving world of payment system fraud depends on the particular system being implemented and the extent to which it solves specific problems in the particular system at issue.

66. The ’973 Patent describes its technical field as “electronic transactions, and more particularly to systems, methods, and apparatuses for securely storing and displaying user credentials.” EX1004 (’973 Patent) at col. 1:31-33. The patent explains that:

> The rapid growth and evolution of traditional and electronic commerce markets has resulted in a wide-spread demand for monetary payments by digital transactions. However, currently payment systems are highly fragmented and insecure, which creates a threat of data compromise and theft during the transfer and use of electronic

> commerce data. This threat may result in losses for corporations as well as users of such systems, and these losses factor into escalating fees and client costs.

EX1004 ('973 Patent) at col. 1:37-45.

67. Electronic payment and related systems have long faced significant and complicated security challenges. EX1021 (Singer) at col. 1:46-47 ("The biggest challenge facing any card payment system is security of the credit card information."); EX1022 (Shift4) at page 2 ("Since 2001, issues of data security in the Payment Services Industry have garnered ever-increasing attention.").

68. In particular, banking and payment processing systems are known to be among the most, if not the most, difficult systems to secure. "Personal consumer information has been under siege for years." EX1025 (PCI for Dummies) at page 4. A paper submitted by Visa as an exhibit called "[p]rotecting [c]ardholder [d]ata" a "[d]aunting [c]hallenge." EX1027 (First Data) at page 4. This paper sought to explain "why" protecting consumer financial data was so difficult:

> One reason cardholder data is hard to protect is that it is so desirable to criminals; they will do almost anything to get this data, and for good reason. Security vendor Symantec's research reveals that cardholder information can be easily sold in the underground economy, sometimes for as much as $25 per record….

> With so much money at stake, cybercriminals are devising ever more sophisticated methods to access the data they desire.

EX1027 (First Data) at page 5; *see also* EX1031 (Sullivan) at page 1 ("[C]riminals have a strong incentive to steal that information" to commit "payment fraud.").

69. It is widely known, including in "the popular press," that "private consumer identification information can be stolen and used to commit numerous types of fraud and crime. There is little argument about the value of this information when obtained by an attacker." EX1023 (Arnold) at page 3. As Visa's Exhibit 1020 explains: "Over the past 20 years, the card payment system has seen data breaches exposing millions of customer records." EX1020 (Cross River) at page 2; *see also* EX1031 (Sullivan) at pages 4-9 (providing data on data breaches).

70. Because these systems are so widespread and offer easy access to money, hackers and bad actors have focused their efforts on trying to attack, compromise, and find vulnerabilities. *See, e.g.*, EX1031 (Sullivan) at page 1 ("[A] recent data breach at Heartland Payment Systems exposed 130 million records of payment cards—the largest in a succession of security failures that have exposed growing numbers of payment records."); EX1020 (Cross River) at page 2 (noting large-scale hacks and data breaches of credit card information in 2008 and 2015); EX1022 (Shift4) at pages 1-2 (describing "high-profile security breaches in 2005," including "the most publicized security breach in which at least 40 million credit

card account numbers were compromised"); EX1042 (Laracey) ¶3 ("There have been a number of highly publicized incidents where cardholder data was stolen from merchant systems. In other incidents, employees directly skimmed or copied cardholder data and used it for fraudulent transactions."); EX1031 (Sullivan) at Abstract ("Especially damaging are large data breaches, which are often the result of criminals gathering information useful to committing payment fraud.").

71. The challenge has been creating systems that are easy to use while remaining secure and resilient to intrusion and fraud. EX1034 (Palgon) at col. 1:47-50 (noting "a long-felt but unresolved need exists for a system or method that provides secure access to sensitive data, while maintaining the data format for easy utilization by existing systems"). For example, a paper by Shift4 noted the tension between the (1) needs of customers who enjoy the convenience of charging items to their hotel room, or making a recurring payment for a monthly membership, with (2) the security "constraints placed on the storage of cardholder data" by merchants participating in electronic payment networks. EX1022 (Shift 4) at page 5. Indeed, conventionally "not all merchants are able to properly secure the user information that is read from a payment card." EX1042 (Laracey) ¶3.

72. In this industry, there are numerous security challenges a skilled artisan must address. These challenges are constantly evolving as scammers and bad actors become ever more sophisticated. Visa's Sullivan exhibit explained:

> criminals have a strong incentive to steal that information, leading to attacks on computer systems, data breaches, and ultimately payment fraud. Such criminal efforts are increasing in organization and scale.

EX1031 (Sullivan) at page 1; *see also* EX1031 (Sullivan) at Abstract ("The rapid transition to card payments has sparked a search for effective countermeasures to those who exploit card payment security vulnerabilities to commit payment fraud."). Another Visa exhibit agreed: "With so much money at stake, cybercriminals are devising ever more sophisticated methods to access the data they desire." EX1027 (First Data) at page 5; *see also* EX1025 (PCI for Dummies) at page 4 ("The people behind successful attacks are professional thieves… [and] organized criminal groups…. Their skill and intent demand your utmost vigilance and response!"). They are "shift[ing] techniques again" and again to target different vulnerabilities. EX1027 (First Data) at page 5. Sullivan likewise noted that "a complex and developing chain from data breach to payment fraud is developing." EX1031 (Sullivan) at Abstract; *see also* EX1031 (Sullivan) at pages 3-4 (describing emergence of organized crime committing "electronic payment fraud").

73. Here are some examples of security challenges:

74. **Phishing attacks** tricking consumers into disclosing financial or other sensitive information. *E.g.*, EX1031 (Sullivan) at page 3 ("Criminals also exploit the Internet, such as by sending out millions of email messages that trick a small number

of recipients into revealing sensitive account or card information (phishing)."); EX1024 (Microsoft Whitepaper) at page 3 ("The rampant use of passwords has lead [sic] to a cottage industry for phishers.").

75. **Intrusions in payment processing systems**. *E.g.*, EX1020 (Cross River) at page 2 (noting large-scale hacks and data breaches of credit card information in 2008 and 2015); EX1022 (Shift4) at pages 1-2 (describing "high-profile security breaches in 2005" including "the most publicized security breach in which at least 40 million credit card account numbers were compromised"); EX1031 (Sullivan) at Abstract, page 1 (noting "[c]riminals particularly target nonbank payment processors" and describing "a recent data breach at Heartland Payment Systems exposed 130 million records of payment cards."); EX1027 (First Data) at page 5 (describing "directed attacks against specific companies that processed lots of sensitive data—banks, ATM operators, data processing companies").

76. **Hacks of merchant databases**. *E.g.*, EX1042 (Laracey) ¶3 ("There have been a number of highly publicized incidents where cardholder data was stolen from merchant systems."); EX1031 (Sullivan) at Abstract ("[R]etailers" are particularly targeted by criminals in data breaches.).

77. **Dishonest employees**. *E.g.*, EX1042 (Laracey) ¶3 (describing "incidents" where "employees directly skimmed or copied card holder data and used

it for fraudulent transactions"); EX1031 (Sullivan) at page 3 & n.7 (describing skimming credit card numbers).

78. **Compromising user systems**. *E.g.*, EX1031 (Sullivan) at page 3 ("Some consumers… do not sufficiently protect their personal computers."); EX1027 (First Data) at page 5 (criminals targeting data "in the computer's running memory because it's not encrypted").

79. **Intercepting communications**. *E.g.*, EX1012 (Stafford) ¶8 ("The possibility for fraud and lapses in security are further increased in situations where credential information is shared over a computer network such as the Internet."); EX1027 (First Data) at page 5 (criminals intercepting "data in transit" to commit fraud).

80. **Stolen encryption keys**. *E.g.*, EX1034 (Palgon) at col. 1:40-46 (Because "encryption keys must be distributed to all systems that need to decrypt the information[, i]t is possible for even such a distributed system to be compromised by a sophisticated hacking attack.").

81. **Replay attacks** where "a message is stolen off a network and resent later" to impersonate a user, or to obtain access to a secure system. EX1019 (Steiner) at page 3.

82. Indeed, Visa's primary references acknowledge the challenge of providing a secure system. Oborne sought to create a token system "for securing

user data and preventing fraud." EX1011 (Oborne) ¶8. Stafford also explained the challenge: "The possibility for fraud and lapses in security are further increased in situations where credential information is shared over a computer network such as the Internet." EX1012 (Stafford) ¶8.

83. Given this backdrop of understanding of a skilled artisan of the longstanding need and complexity of the technology involved, verification by an issuing agency is also neither unusually simple nor routine. First, Oborne did teach conventional forms of verification, but not verification of tokens by an issuer. For example, Oborne taught that its system could "[i]n some implementations" provide "additional security," such as (1) requiring a user "to provide a user name and password to activate a payment token," (2) requiring a user "to provide a digital certificate to verify the user's identity prior to utilization of a payment token," (3) using "device fingerprinting," (4) using a "custom hardware authentication chip… in communication with the client," and (5) requiring a user to "perform an authentication procedure with the client and a user's card linked to the user's payment token." EX1011 (Oborne) ¶26. None of these involve the issuer in any way. If issuer verification at the time of token generation were unusually simple or "routine," Oborne would be expected to mention it in its laundry list of "additional security" options, but Oborne did not mention it here or anywhere else.

84. Second, Dr. Shamos' inability to find disclosure of issuer verification of a virtual credential at the time of generation in the prior art suggests that it is not "routine" at all.

85. Third, Dr. Shamos does not explain how or why issuer verification at the time of credential generation could avoid his hypothetical "unofficial, forged or altered tokens in the marketplace." EX1005 (Shamos Declaration) ¶212. Given the complexity of this technology as demonstrated above, more than a simple assertion is required to demonstrate the "routine" use of such a feature to prevent unexplained and imprecise problems, such as Dr. Shamos' "unofficial, forged or altered tokens in the marketplace."

86. Fourth, given that Dr. Shamos opines that this problem had already been solved using a different technique, EX1005 (Shamos Declaration) ¶97 (explaining that this problem was solved "starting in 1967" by requiring "the presenter of the credential to furnish additional information to prove that they are the person named in the credential"), as I explain in more detail below, Dr. Shamos fails to explain why it would have been "routine" to implement a different technique to solve this problem. Indeed, if Dr. Shamos' opinion regarding the solution to this problem is correct, it is difficult to imagine why a skilled artisan would consider it "routine" to solve the problem using a technique other than the accepted solution.

87. Designing a system that can be widely and cost-effectively deployed and that is resilient to constant attacks and an ever-evolving range of security threats is a daunting technological challenge. The technological solutions necessary to address sophisticated and wide-ranging security challenges are by no means easy or straightforward, as is evident from the long-running efforts to address the longstanding need for this technology.

C. User Authentication in Oborne

88. I understand that Visa and Dr. Shamos have argued that including issuing agency verification in Oborne would have been obvious. IPR Petition at page 22; EX1005 (Shamos Declaration) ¶212. Dr. Shamos says issuing agency verification would be obvious because:

> The existence of unofficial, forged or altered tokens in the marketplace would create problems for both issuers and users.

EX1005 (Shamos Declaration) ¶212.

89. I disagree that one of skill in the art would be motivated to add issuing agency verification at the time of token generation to Oborne. Oborne already taught a solution for addressing the "unofficial, forged or altered tokens in the marketplace," which was a user authentication step. In fact, Dr. Shamos himself opines that the problem of "copied, forged, or altered" digital credentials was solved "starting in 1967" by "requir[ing] the presenter of the credential to furnish additional

information to prove that they are the person named in the credential." EX1005 (Shamos Declaration) ¶¶95, 97. Dr. Shamos opines that "requiring the user to enter a PIN at an ATM machine" was an example of implementation of this strategy. EX1005 (Shamos Declaration) ¶97. This type of authentication at the time of use of a virtual credential is the type of "additional security" taught by Oborne as well. *E.g.*, EX1011 (Oborne) ¶26 (providing various "additional security" layers, such as requiring "a user name and password to activate a payment token" and requiring "a digital certificate to verify the user's identity prior to utilization of a payment token for a purchase transaction"). One of skill in the art, understanding what Dr. Shamos alleges that person would understand, would have no motivation to solve a problem that according to Dr. Shamos had already been solved.

90. Additionally, Dr. Shamos does not explain why the allegedly solved problem of "unofficial, forged or altered tokens" would motivate one of ordinary skill in the art to implement issuing agency verification at the time of token generation. *See* EX1005 (Shamos Declaration) ¶212. Dr. Shamos does not explain what benefit issuing agency verification of the token in Oborne would provide to help mitigate "unofficial, forged or altered tokens in the marketplace." *See* EX1005 (Shamos Declaration) ¶212. It is unclear why, for example, if a token is verified to be an official representation of the credential, it could not be forged or altered or even what forging or altering a token means in this context. Nor does Dr. Shamos

explain why Oborne's recommendations—and the understanding of one of ordinary skill in the art that adding security ***at the time of use of the token*** solves the problem of "copied, forged, or altered tokens"—would motivate one of ordinary skill to implement any additional security measures ***at the time of token generation***, much less specifically issuer agency verification at the time of token generation. Dr. Shamos' proposed addition of issuer agency verification at the time of token generation in this context contradicts his own assertions regarding a skilled artisan's knowledge and motivations and appears to be nothing more than hindsight, which I understand is impermissible under the law of obviousness.

91. In addition to these "additional security" measures, Oborne teaches user authentication at the time of token use as part of its Figure 7 embodiments. I explain Oborne's use of authentication in the following paragraphs.

92. For example, Oborne's Figure 7A describes and depicts how it authenticates transactions in "executing a token-based purchase transaction" in its "Token-Based Purchase Transaction Execution ('tPTE') component 700." EX1011 (Oborne) ¶68. Figure 7A is reproduced below:

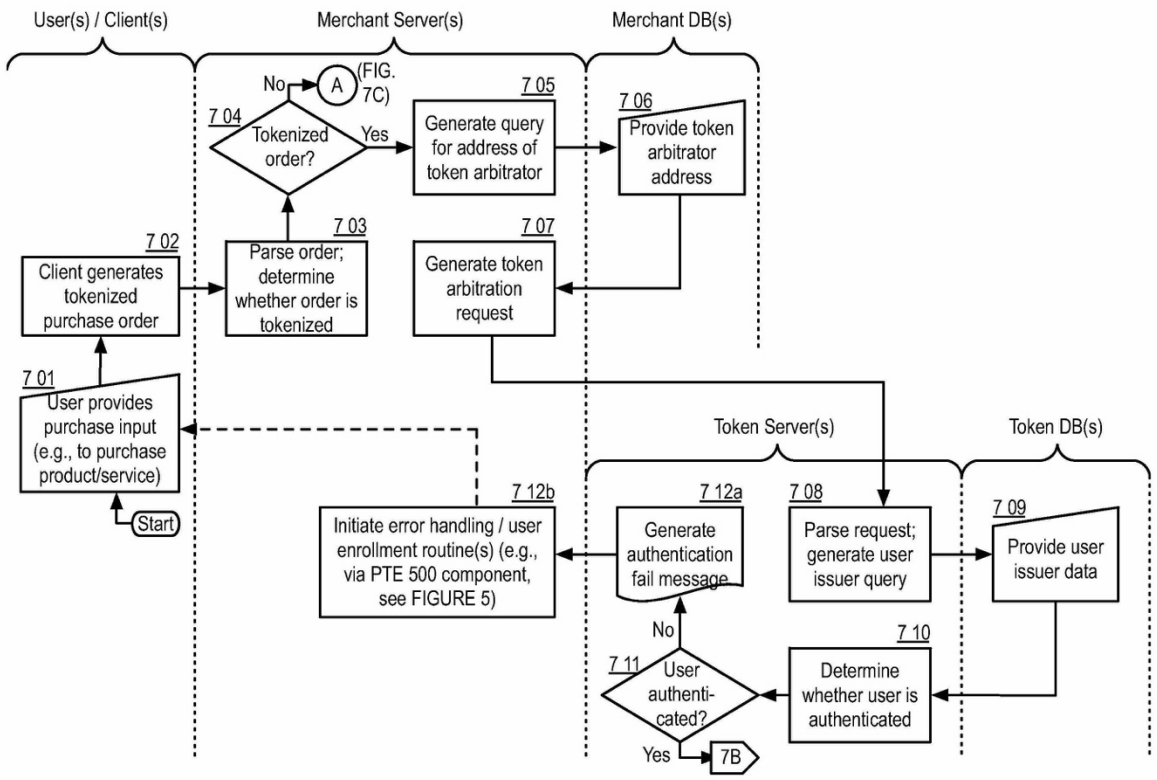


FIGURE 7A Example: Token-Based Purchase Transaction Execution ("tPTE") component 700

EX1011 (Oborne) at Fig. 7A.

93. In Figure 7A, "the user may provide purchase input, e.g. [step] 701, into the client indicating the user's desire to purchase the product." EX1011 (Oborne) ¶68. For a tokenized purchase, "[t]he merchant server may generate a token arbitration request, e.g. 708, and provide the token arbitration request to a token server." EX1011 (Oborne) ¶68.

94. Oborne explains that "the token server may determine whether the user token is authenticated, e.g., [step] 710." EX1011 (Oborne) ¶69, Fig. 7A. Oborne explains that the purpose of this authentication step is to prevent fraud in tokenized

transactions: "[T]he system 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." EX1011 (Oborne) ¶26. Step 710 is shown below:

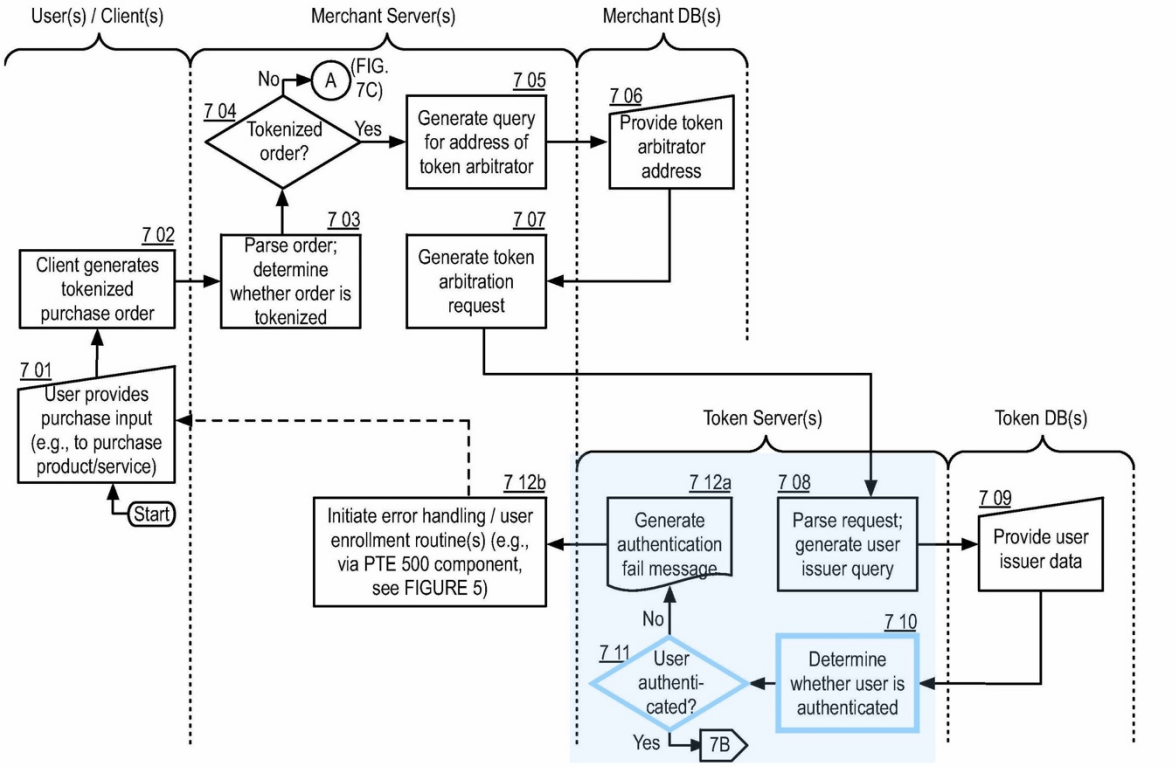


FIGURE 7A

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

EX1011 (Oborne) at Fig. 7A (annotated).

95. At authentication step 710, Oborne teaches that "[i]f the token server determines that the user is not authenticated, e.g. 711, option 'No,' the token server may generate an 'authentication fail message,' e.g. 712a." EX1011 (Oborne) ¶69. This prompts "an error-handling routine." EX1011 (Oborne) ¶69. Otherwise, if

Oborne's system "determines that the user is authenticated… the token server may continue processing at [step] 713a." EX1011 (Oborne) ¶69.

96. Oborne described a variety of techniques for user authentication to prevent fraud.

97. For example, Oborne teaches "the app executing on the user's device may provide a 'VerifyChat' feature for fraud prevention." EX1011 (Oborne) ¶30; *see also* EX1011 (Oborne) ¶54 (describing "verification of authentication" of a user with "VerifyChat"). Oborne's system "may utilize the VerifyChat feature to communicate with the user, and verify the authenticity of the originator of the purchase transaction." EX1011 (Oborne) ¶30. Oborne teaches VerifyChat could use electronic messaging: "electronic mail message, text (SMS) messages, Facebook® messages, Twitter™ tweets, [or] text chat." EX1011 (Oborne) ¶30.

98. Oborne also teaches that VerifyChat's user authentication may include "voice chat" or "video chat (e.g. Apple FaceTime) and/or the like to communicate with the user." EX1011 (Oborne) ¶30. Oborne explains:

> For example, the PPT may initiate a video challenge for the user, e.g., 301. For example, the user may need to present him/her-self via a video chat, e.g., 302. In some implementations, a customer service representative, e.g., agent 304b, may manually determine the authenticity of the user using the video of the user.

EX1011 (Oborne) ¶30; *see also* EX1011 (Oborne) ¶54 (describing "video chat" user authentication using VerifyChat). This allows the customer service agent "to determine the identity of the user." EX1011 (Oborne) ¶30. Oborne shows how this would work in Figure 3A, reproduced below. If "the transaction is fraudulent," Oborne's "PPT may then cancel the transaction, and/or initiate fraud investigation procedures on behalf of the user." EX1011 (Oborne) ¶30.

FIGURE 3A

Example: Token-Based Purchase Payment: Security / Fraud Prevention

EX1011 (Oborne) at Fig. 3A.

99. Oborne extensively describes user authentication at the time of token use to address the problem of fraudulent tokens. That is the same procedure Dr.

Shamos alleges solved the problem of "copied, forged, or altered" digital credentials starting in 1967. EX1005 (Shamos Declaration) ¶¶95, 97. One of ordinary skill in the art with this understanding would have no reason to depart from the known techniques for addressing this problem, and Dr. Shamos offers no explanation or reason for any such departure other than hindsight. *See* EX1005 (Shamos Declaration) ¶212.

D. Claims 2, 9, and 17: "second OVER file"

100. I understand that Claim 2 depends from Claim 1 and adds multiple limitations, including the following:

- "a second OVER file generation request" "from a second OVER file storage client device of the user,"
- "generating… a second OVER file comprising a second virtual representation of the credential… that is invalid for use in the first OVER file storage client device for authenticating the user; and"
- "transmitting, to the second OVER file storage client device of the user, the second OVER file…."

EX1004 at col. 22:35-53. Claims 9 and 17, which depend from independent Claims 8 and 16, respectively, also include these requirements. EX1004 at cols. 23:54-24:6, 25:11-29.

101. The language of Claims 2, 9, and 17 refers to "the user" and "the credential." *See* EX1004 ('973 Patent) at cols. 21:35-53 (Claim 2), 23:54-24:6 (Claim 9), 25:11-29 (Claim 17). Based on the language of Claim 2, I understand "***the*** user" in the limitations (e.g., a "second OVER file storage client device of ***the user***") refers to the same "user" in the Claim 1 limitations (e.g., "information associated with a credential of ***a user***"). I similarly understand that "***the*** credential" in Claim 2 (e.g., "a second virtual representation of ***the credential***") refers to the same "credential" in the Claim 1 limitations (e.g., "information associated with ***a credential*** of a user"). Similarly, I have the same understanding regarding Claim 9 as it relates to Claim 8 and Claim 17 as it relates to Claim 16. Accordingly, Claims 2, 9, and 17 require two different "OVER file storage client device[s]" of the same "user," each of which requests and receives an "OVER file" comprising a "virtual representation" of the same "credential." EX1004 ('973 Patent) at cols. 22:41-53 (Claim 2), 23:61-24:6 (Claim 9), 25:17-29 (Claim 17). In this context, the two OVER files are different from each other, each containing a virtual representation of the credential that is different from the virtual representation in the other OVER file. I further understand that the "second OVER file" is "invalid for use in the first OVER file storage client device for authenticating the user." EX1004 ('973 Patent) at cols. 22:45-50 (Claim 2), 23:65-24:3 (Claim 9), 25:21-26 (Claim 17).

102. I understand that Visa and Dr. Shamos argue that the claim limitations were "obvious in view of Oborne." IPR Petition at pages 33-35 (Claim 2), 48 (Claim 9), 39 (Claim 17); EX1005 (Shamos Declaration) ¶¶226-29 (Claim 2), 268 (Claim 9), 246-47 (Claim 17). Specifically, Visa and Dr. Shamos argue that applying Oborne to a user with two devices "would have been obvious" as a "POSA would have expected users to use multiple devices," IPR Petition at pages 34, 39, 48, and that it would also have been obvious for "the second OVER file" to be "invalid for use in the first device," IPR Petition at pages 34-35, 39, 48; EX1005 (Shamos Declaration) ¶¶227 ("A POSITA would find it unnatural to be restricted to using only a single device."), 228, 246, 268.

1. Oborne Does Not Suggest "generating… a second over file comprising a second virtual representation of the credential"

103. I understand that Visa and Dr. Shamos contend that it would have been obvious to one of skill to adapt Oborne's system to allow users to receive tokens on multiple devices. IPR Petition at pages 34-35, 39, 48; EX1005 (Shamos Declaration) ¶¶227, 246, 268.

104. Oborne does not describe a scenario in which a user seeks to receive tokens on multiple devices and thus does not provide or suggest a solution to this scenario. Dr. Shamos points to no such disclosure in Oborne, and I have not found one. *See* EX1005 (Shamos Declaration) ¶¶227, 246, 268. Instead, Dr. Shamos

asserts that "[a] POSITA would find it unnatural to be restricted to using only a single device" without any explanation or support for this assertion. EX1005 (Shamos Declaration) ¶¶227, 246, 268. However, consumers in 2012 were very accustomed to having a single device on which they could receive cellular telephone calls. For example, in 2014, Apple introduced iOS version 8, which provided the ability to hand off cellular calls to other devices, which took some "by surprise." *See* EX2018 (Boyce) at page 1 ("Turns out the ringing was coming from my iPad. *My iPad!*"). It is not surprising that Dr. Shamos cites no support for his assertion that a skilled artisan in 2012 would have found it "unnatural" to be limited to using only a single device for certain functionalities because it is incorrect.

105. Dr. Shamos next asserts that "Oborne 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." EX1005 (Shamos Declaration) ¶¶227 (citing EX1011 (Oborne) ¶148), 246, 268. Dr. Shamos' assertion, however, adds something Oborne does not disclose. Oborne does state in the context of "the database component 1519[, which] includes several tables 1519a-n" that "[a] Devices table 1519b may include fields, such as, but not limited to: device_ID, device_name, device_IP, device_GPS, device_MAC, device_serial, device_ECID, device_UDID, device_browser, device_type, device_model, device_version, device_OS, device_apps_list, device_securekey,

wallet_app_installed_flag, and/or the like." EX1011 (Oborne) ¶148. What Oborne does not say is that the Devices table 1519b reflects "a user's devices" as Dr. Shamos asserts. Instead, "Users table 1519a" "support[s] and/or track[s] multiple entity accounts on a PPT." EX1011 (Oborne) ¶148. Because the database component 1519 includes the ability to support multiple entity accounts (i.e., multiple users), Oborne does not disclose that multiple devices in the Devices table 1519b are "a user's devices" rather than multiple user**s**' devices. As I mentioned above, I have not found any disclosure or suggestion in Oborne of the use of multiple devices by a single user.

106. Dr. Shamos next cites Oborne's disclosure of storing device IDs and Oborne's teaching that "device fingerprinting may be utilized" for "additional security" to assert that "[t]o obtain the additional security taught by Oborne, a POSITA would have been motivated to employ Oborne's device fingerprinting to tie a given token to a particular device, such that the token for a second device would be invalid if used in a first device (since the device's fingerprint would not match)." EX1005 (Shamos Declaration) ¶¶228, 246, 268. But again, Dr. Shamos' premise is not supported by Oborne and is contradicted by his own testimony.

107. First, Oborne does mention device fingerprinting a single time along with two mentions of "fingerprint" in an XML code sample. EX1011 (Oborne) ¶¶26 ("As another example, device fingerprinting may be utilized. For example, a client

device of a user may be a device that is used exclusively by the user, such as a smartphone, tablet computer, laptop computer, and/or the like."), 47 (XML code sample for a token). But Oborne does not disclose that "device fingerprinting" would be used "to tie a given token to a particular device" as Dr. Shamos asserts. A skilled artisan would understand that "device fingerprinting" merely refers to identifying a particular device as a device of a particular user and says nothing about what is done with that identification once it has occurred. *E.g.*, EX1011 (Oborne) ¶26 ("As another example, device fingerprinting may be utilized. For example, a client device of a user may be a device that is used exclusively by the user, such as a smartphone, tablet computer, laptop computer, and/or the like."). Dr. Shamos does not account for his assertion that it would have been obvious to use device fingerprinting "to tie a given token to a particular device," which Oborne does not teach. In the absence of some teaching or reasoned explanation as to why one of ordinary skill in the art would be motivated to tie a given token to a particular device, Dr. Shamos cannot show that the claims would have been obvious.

108. Second, Dr. Shamos' own opinion is that one of ordinary skill in the art would instead tie a single token to multiple devices if multiple devices were going to be used. As I explained above, Dr. Shamos has shown no reason a user would expect to use a token on multiple devices, and Oborne did not disclose or suggest that. But even if he had shown that or Oborne had disclosed or suggested that, Dr.

Shamos has not shown why one of ordinary skill in the art would choose to generate an entirely new token when a user requested a token on a second device rather than simply re-using the original token. In fact, Dr. Shamos testifies that:

> It was conventional to not [] repeat generating a representation of a credential if the representation had previously been generated and stored. It is simply logical not to waste resources generating something that has already been generated.

EX1005 (Shamos Declaration) ¶58. In light of this alleged understanding of one of ordinary skill in the art, Dr. Shamos has offered no explanation why such a skilled artisan would create an entirely new token (representation of a credential) if a token were requested for a second device. In such a scenario, as Dr. Shamos himself asserts, it would be entirely logical "not to waste resources generating something that has already been generated." EX1005 (Shamos Declaration) ¶58. Doing so would simply require adding a second set of client_details in the XML code sample in paragraph 47 of Oborne, much like the three different accounts shown in that same XML code sample. *See* EX1011 (Oborne) ¶47.

109. However, if a second device token were requested and if the "logical" path according to Dr. Shamos were taken such that the same token were used on both devices, the claims' requirement that the second OVER file be "invalid for use in the first OVER file storage client device" would not be met, and thus, the claims would

not be obvious even assuming all these premises for which Dr. Shamos has shown no basis.

2. Oborne Does Not Suggest "a second OVER file" That Is "invalid for use in the first over file storage client device"

110. I also understand that Visa contends that it would have been obvious to one of skill that the "second OVER file" would be "invalid for use in the first device." IPR Petition at pages 34-35, 39, 48. Visa relies on Oborne's disclosure of "device fingerprinting" as an "additional security" measure to support its argument. IPR Petition at pages 34-35, 39, 48. But Oborne is silent on the use of multiple devices associated with a single user or how "device fingerprinting" would be used in such a scenario. Neither Visa nor Dr. Shamos has presented any indication, suggestion, or reason that a hypothetical second device in Oborne would receive a token that would be invalid for use in the first device.

111. As I explained above, device fingerprinting simply refers to identifying a device and the user associated with that device. As I also explained above, Oborne has only three mentions of "device fingerprinting" or even "fingerprint," none of which refer to use of device fingerprinting in the context of multiple user devices. EX1011 (Oborne) ¶¶26 ("As another example, device fingerprinting may be utilized. For example, a client device of a user may be a device that is used exclusively by the user, such as a smartphone, tablet computer, laptop computer, and/or the like."),

47 (XML code sample for a token). Thus, the mere mention of "device fingerprinting" in Oborne does not disclose or suggest how "device fingerprinting" would be used in the context of multiple devices associated with a single user.

112. Dr. Shamos testified that implementing Oborne's "device fingerprinting" would mean tying "a given token to a particular device, such that the token for a second device would be invalid if used in a first device" of the user. EX1005 (Shamos Declaration) ¶¶228 ("There would be no purpose to device fingerprinting if a token could be used on any device."), 246, 268. However, several other possibilities easily come to mind.

113. For example, device fingerprinting could be used to limit a token to a ***set*** of fingerprinted devices, such as each device belonging to the user. For example, the user could use the same token on any of his or her devices that had been registered with Oborne's system, but not on any other device. In fact, according to Dr. Shamos, this would be the "conventional" and "logical" approach because using the same token on a second device avoids "repeat[ing] generating a representation of a credential if the representation had previously been generated and stored." EX1005 (Shamos Declaration) ¶58. According to Dr. Shamos, "[i]t is simply logical not to waste resources generating something that has already been generated." EX1005 (Shamos Declaration) ¶58. By implementing Oborne's device

fingerprinting to allow the same token to be used on ***two*** of the user's devices, Oborne would be following Dr. Shamos' "conventional" and "logical" approach.

114. As another example, device fingerprinting could be used as one of a number of non-exclusive options for the user to be authenticated. In other words, device fingerprinting could be used to allow for a simpler authentication process on the user's device or devices, but the protocol could require some additional authentication step on other non-fingerprinted devices, similar to how a secure website can be set to remember a user's device for faster login. For example, Oborne's token server could allow a token-based transaction to proceed immediately if it recognized the user's device. If, however, Oborne's token server did not recognize the device, it could ask for additional authentication such as "login and password" or by utilizing the "VerifyChat" feature. EX1011 (Oborne) ¶¶26, 54.

115. Assuming there was some reason or suggestion to use Oborne's system with multiple devices of a single user, which Dr. Shamos has not shown, I disagree with Dr. Shamos' opinion regarding obviousness of the claims. Because Dr. Shamos' assertion that "device fingerprinting" in Oborne could only be implemented with unique tokens for each device is incorrect, as both I and Dr. Shamos himself have shown, I disagree that Dr. Shamos has shown that Oborne's system would be implemented by a skilled artisan with unique tokens for each device such that a token for a second device would be invalid for use on a first device.

[*Paragraphs 116-124 reserved.*]

IX. STAFFORD GROUNDS 3-4

A. Public/Private Key Encryption in Stafford

125. Encryption uses mathematical algorithms to secure sensitive content. This is how it works at a high level. To encrypt data, a sender uses encryption algorithms to convert readable text into an unreadable ciphertext and protect it with an encryption key. EX2017 (Hellman) at page 26. A decryption key is required to convert the ciphertext back into readable text by the recipient. EX2017 (Hellman) at page 26.

126. There are many types of encryption. Stafford uses a conventional public/private key system to encrypt sensitive data. EX1012 (Stafford) ¶¶68-69.

127. Public/private key systems are asymmetric encryption. They were described in a 1978 paper by Martin Hellman (EX2017), then a professor at Stanford University. At a high level, a public/private key system uses paired keys: a public key and a private key. EX2017 (Hellman) at pages 25-26; EX1012 (Stafford) ¶68. Typically, the paired keys are generated by a specific recipient using a cryptographic algorithm. EX1012 (Stafford) ¶68.

128. The public key is not secret and is available to anyone. EX2017 (Hellman) at pages 25-27. To send an encrypted message to the private key holder, the sender can use the public key to encrypt the data. EX2017 (Hellman) at pages

25-27; *see also* EX1012 (Stafford) ¶70. The private key is kept secret by its holder and can be used to decrypt the encrypted message. EX2017 (Hellman) at pages 25-26; EX1012 (Stafford) ¶69. Once encrypted, the data can be shared freely with the expectation it cannot be read by anyone except the private key holder. EX2017 (Hellman) at page 27; *see also* EX2017 (Hellman) at pages 25-26; EX1012 (Stafford) ¶69.

129. Stafford names the keys in his "asymmetric or public key pair for the entity" or specific user as "User_pub_key_1" and "User_priv_key_1". EX1012 (Stafford) ¶68. His "system private key" is called "IDCheck_priv_key1." EX1012 (Stafford) ¶69. He also references a system public key named "IdCheck_pub_key1." *E.g.*, EX1012 (Stafford) ¶36.

130. Stafford also mentions "using One Time Pad or similar highly secure algorithm that provides 'perfect secrecy.'" EX1012 (Stafford) ¶94. One of skill knew that one-time pads are an encryption technique using single-use pre-shared keys that cannot be cracked. One-time pads have long been known. They were famously used by the Allies during World War II and later described by Claude Shannon in a famous 1949 paper titled "Communication Theory of Secrecy Systems."

B. Stafford Does Not Teach Or Suggest An "OVER File" That Is "based on the information associated with the credential of the user"

131. Each of the claims of the '973 Patent requires an "OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, *based on the information associated with the credential of the user*." *See* EX1004 at cols. 22:1-5, 23:23-27, 24:44-48 (independent Claims 1, 8, 16) (emphasis added).

132. Dr. Shamos says that "the key signatures taught by Stafford correspond to the recited OVER files." EX1005 (Shamos Declaration) ¶293. I understand that Dr. Shamos and Visa read Stafford's key signature, "hash values (IdSig1 and IdSig2)," as the claimed "OVER file comprising a virtual representation" and assert that "[a] hash value acts as a virtual representation of the stored credential, and is derived based on the information associated with the credential." EX1005 (Shamos Declaration) ¶295; IPR Petition at pages 57-58 (same).

133. I have been asked to provide an opinion on whether Stafford's key signatures teach or suggest the claimed "OVER file comprising a virtual representation of the credential…, based on the information associated with the credential of the user." They do not.

134. The Board's Institution Decision stated that its "preliminary view at this juncture is that Stafford's hash values are not a virtual representation associated with

the credential because it does not appear that its hash values are derived based on information associated with the credential." Institution Decision at page 40. Specifically:

> At this juncture and on a preliminary basis, we do not agree with Petitioner that Stafford's hash values IdSig1 and IdSig2 "act[] as a virtual credential representation of the stored credential." Our reading of Stafford is that hash signatures are derived values from one-time pads, which may be used to encrypt the credential, but the pads do not appear to include any information related to the credential or its contents. Further, comparisons of derived hash values may lead to a location where a credential is stored in a secure location—but, our preliminary view is that any alleged "association" with the credential appears to be extremely attenuated, at best.

Institution Decision at page 41 (internal citation omitted). I agree with the Board's findings.

135. Dr. Shamos maps Stafford's IdSig1 and IdSig2 to the claimed "OVER file comprising a virtual representation of the credential…." EX1005 (Shamos Declaration) ¶295. He says that IdSig1 and IdSig2 are "hash values" and these "hash value[s] act[] as a virtual representation of the stored credential, and [are] 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." EX1005 (Shamos Declaration) ¶295. This is inaccurate because Stafford never

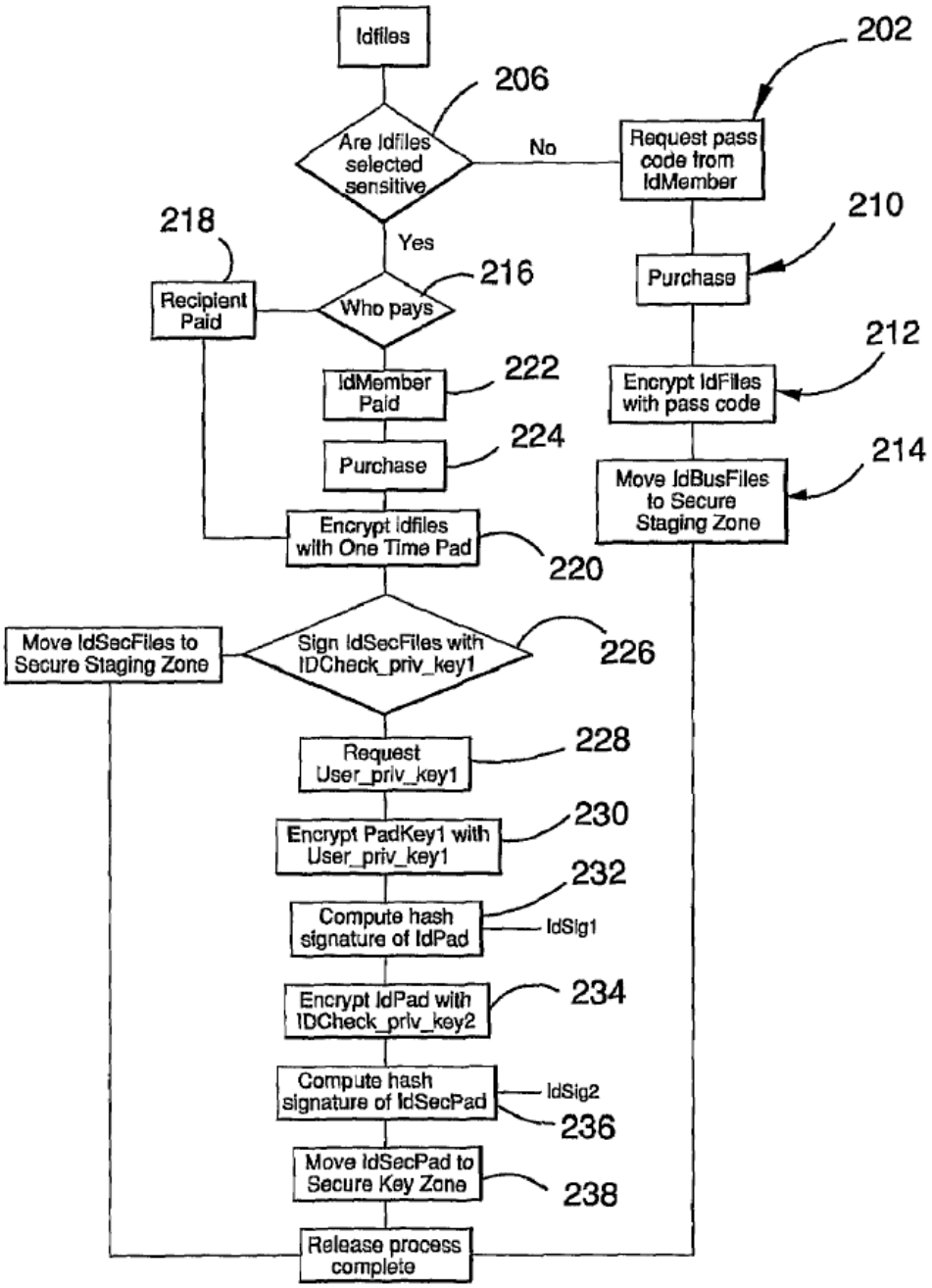
teaches that IdSig1 and IdSig2 are in any way based on information associated with the credential, as the Board pointed out.

136. Stafford teaches a "system [and] methods which enable information relating to an entity, such as an individual or business, to be securely shared across a computer network." EX1012 (Stafford) ¶8. Stafford calls the "unencrypted credential information" stored in its system the "**IdFiles**." EX1012 (Stafford) ¶38 (emphasis added).

137. For increased security, Stafford advises that "[i]nformation of a sensitive nature cannot be released by use of a pass code." EX1012 (Stafford) ¶81. Instead, such "[s]ensitive data is not able to be released without the purchase of key signatures. Typically key signatures are provided and released as a paid service." EX1012 (Stafford) ¶81. Stafford explains that these key signatures required for releasing "sensitive files" are "a one time pad." EX1012 (Stafford) ¶88. Stafford calls its one-time pad the "**IdPad,**" which is an "encrypted one-time pad or symmetric key." EX1012 (Stafford) ¶42 (emphasis added). Stafford teaches that its one-time pads are purchased for single use and "[a]dvantageously… involve[] multiple controls to ensure that the release of sensitive information is intentional, secure and ensures data is delivered to the intended recipient." EX1012 (Stafford) ¶81. Stafford does not teach that its one-time pads can be reused. *See, e.g.*, EX1012 (Stafford) ¶142 ("This form of 'release' [using a pass code] is not as secure as the

previous embodiments, *since data can be transmitted multiple times*." (emphasis added)).

138. Stafford teaches the release of sensitive information using its one-time pad. EX1012 (Stafford) ¶93. This process is shown in Stafford's Figure 2, reproduced below:



EX1012 (Stafford) at Fig. 2 (excerpted).

139. Following along with Stafford's process shown in Figure 2 (above), neither hash value that Dr. Shamos relies on, IdSig1 or IdSig2, is based in any way on Stafford's credentials (IdFiles).

140. First, a user "select[s] files or information for release." EX1012 (Stafford) ¶84. Stafford determines "who pays for the transaction": the sender or recipient. EX1012 (Stafford) ¶93; EX1012 (Stafford) ¶84. After that is worked out, the IdFiles (credentials) are encrypted in step 220 using a one-time pad. EX1012 (Stafford) ¶93; EX1012 (Stafford) ¶94. Stafford calls the encrypted credential file the "**IdSecFiles2**." EX1012 (Stafford) ¶94 (emphasis added) ("[T]he unencrypted IdFiles… are symmetrically encrypted using One Time Pad or similar highly secure algorithm that provides 'perfect secrecy,' to create IdSecFiles2.").

141. The IdSecFiles2 "are then digitally signed using IdCheck_priv_key1" (Stafford's system private key) and "moved to the Secure Staging Zone 118… to enable collection, or transmission to the recipient." EX1012 (Stafford) ¶94; EX1012 (Stafford) ¶69 (IDCheck_priv_key1 is the "system private key.").

142. Stafford describes how its public and private keys are exchanged between the system and the user. The user's private key, "User_priv_key1" is transmitted over a network to Stafford's "system 100." EX1012 (Stafford) ¶96. To securely transmit the user's private key, Stafford teaches "[t]he local control module encrypts User_priv_key1with IdCheck_pub_key2 and transmits it to the system 100 where it is unencrypted with IdCheck_priv_key2." EX1012 (Stafford) ¶96.

143. The single-use "One Time Pad" needed to decrypt IdSecFiles2, "is encrypted with User_priv_key1… to create **IdPad** in step 230." EX1012 (Stafford)

¶95 (emphasis added) ("The key or pad (PadKey1) used for the One Time Pad is encrypted … to create IdPad in step 230."); *see also* EX1012 (Stafford) ¶42 ("IdPad" is the "encrypted one-time pad or symmetric key by User_priv_key_1."). In other words, IdPad is created with the user's private key. EX1012 (Stafford) ¶95.

144. Stafford explains: "Next, in step 232 a hash value of IdPad is created, called **IdSig1**" using the user's private key. EX1012 (Stafford) ¶97 (emphasis added). IdSig1 is the first of two key signatures "required by a recipient to collect/obtain the released information" from Stafford's system. EX1012 (Stafford) ¶¶97, 103; *see also* EX1012 (Stafford) ¶47 ("**IdSig1** is a hash value of the IdPad i.e. OTP key which has been encrypted by User_priv_key 1." (emphasis added)). IdSig1 is one of the hash values that Dr. Shamos identifies as an "OVER file comprising a virtual representation of the credential." EX1005 (Shamos Declaration) ¶295. Stafford teaches that IdSig1 is a hash value of the IdPad or encrypted one-time pad. EX1012 (Stafford) ¶¶95, 97. This hash value is not generated based on Stafford's credentials (IdFiles) at all. *See* EX1012 (Stafford) ¶¶95, 97. Dr. Shamos acknowledges that Stafford's "hash values are of the credential's one-time pads." EX1005 (Shamos Declaration) ¶295.

145. Stafford also teaches creating a second hash value: "Next, IdPad is encrypted with IdCheck_pub_key2 to generate **IdSecPad** in step 234. A hash value of IdSecPad is created at 236, which is referred to as **IdSig2**…" EX1012 (Stafford)

¶¶99, 103 (emphases added). IdSecPad uses the same IdPad but performs a second encryption with the system public encryption key IdCheck_pub_key2. EX1012 (Stafford) ¶¶37, 99; *see also* EX1012 (Stafford) ¶48 ("**IdSig2** is a hash value of IdSecPad i.e. OTP key which has been encrypted firstly by User_priv_key1 and secondly by IdCheck_pub_key2." (emphasis added)). IdSig2 is the second hash value that Dr. Shamos identifies as an "OVER file comprising a virtual representation of the credential." EX1005 (Shamos Declaration) ¶295. Again, Stafford teaches that IdSig2 is a hash value of the IdSecPad, another encrypted one-time pad. EX1012 (Stafford) ¶¶99, 103. This second hash value is also not generated based on Stafford's credentials (IdFiles) at all. *See* EX1012 (Stafford) ¶¶99, 103. Again, Dr. Shamos acknowledges that Stafford's "hash values are of the credential's one-time pads." EX1005 (Shamos Declaration) ¶295.

146. Finally, Stafford teaches both IdSig1 and IdSig2 are sent to the user for releasing the credentials. EX1012 (Stafford) ¶¶97, 99.

147. As can be seen in Figure 2 of Stafford below, Dr. Shamos' asserted OVER file (**IdSig1** and **IdSig2**), which includes hash values of one-time encryption keys, is not based on information associated with Stafford's **IdFiles** (which Dr. Shamos says are the credentials):

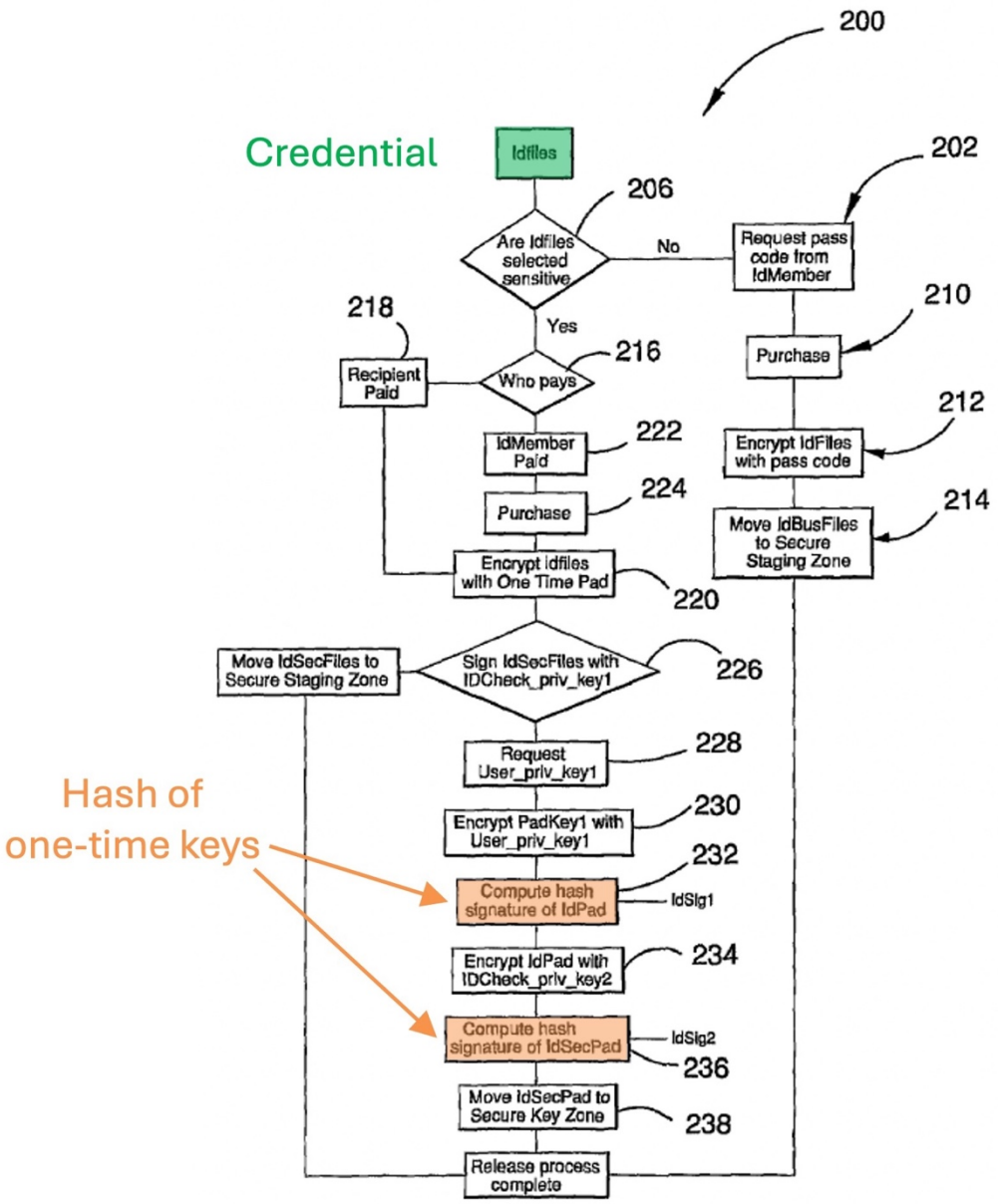


FIGURE 2

EX1012 (Stafford) at Fig. 2 (annotated). The hash values are simply random numbers generated to facilitate release of one or more credentials and are not

associated with any specific credential. Instead, they are associated with a specific one-time release of information that may or may not contain any specific credential.

148. The Board, in my opinion, correctly found that Stafford's key signatures (IdSig1 and IdSig2) are not "derived based on information associated with the credential." Institution Decision at page 40. Thus, Stafford's IdSig1 and IdSig2 plainly do not satisfy the claim requirements of an "OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user" as required by all claims of the '973 Patent. *See* EX1004 at cols. 22:1-5, 23:23-27, 24:44-48 (independent Claims 1, 8, 16).

C. Stafford's Key Signatures Do Not Meet The Claimed "OVER file comprising a virtual representation of the credential that has been verified by an issuing agency"

149. As I explained for the Oborne grounds, all claims of the '973 Patent require an "OVER file comprising a virtual representation of the credential that *has been verified by an issuing agency to be an official representation of the credential*." *See* EX1004 at cols. 22:1-5, 23:23-27, 24:44-48 (independent Claims 1, 8, 16).

150. As I explained in Paragraph 43 of this Declaration, I applied the Board's claim construction of these claim terms. In other words, the claim language "a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential" requires that the issuing agency has

verified the "virtual representation" (and not the "credential") to be "an official representation of the credential."

151. Dr. Shamos and Visa argue that "Stafford teaches that its encrypted credentials may be verified by the issuer." EX1005 (Shamos Declaration) ¶296; IPR Petition at pages 58-59. In support, Dr. Shamos cites Stafford's paragraphs 62, 65, and 67. EX1005 (Shamos Declaration) ¶296.

152. As I explained in paragraph 132, Dr. Shamos says that the IdSig1 and IdSig2 "key signatures taught by Stafford correspond to the recited OVER files" containing a virtual representation of the credential. EX1005 (Shamos Declaration) ¶¶293, 295.

153. I also disagree with Dr. Shamos that Stafford's paragraphs 62, 65, and 67 teach verification of a virtual representation of the credential by an issuing agency. I see nothing in Stafford where an issuing authority has verified the IdSig1 and IdSig2 that Dr. Shamos opines are the OVER files. EX1005 (Shamos Declaration) ¶¶295-96.

154. Paragraph 62 of Stafford only mentions "scan[ning] or upload[ing] hard copy documents into the system" before "perform[ing] tasks such as verification." EX1012 (Stafford) ¶62. This paragraph describing scanning and uploading documents does not mention, and has nothing to do with, the hash values of one-time pads IdSig1 and IdSig2. EX1012 (Stafford) ¶62. It certainly does not teach

any issuing agency verification of IdSig1 and IdSig2, nor would any such issuing agency verification of hash values of one-time pads make any sense. Asking third parties such as issuing agencies to verify one-time pads would require that they be communicated to third parties, thwarting the security of the system, which requires maintaining IdSig1 and IdSig2 confidential between only Stafford's system operator and the intended recipient of the credentials.

155. Stafford's paragraph 65 is part of "an initial step in the enrol[l]ment" where a user "submits their credential information or documentation" and it is verified. EX1012 (Stafford) ¶64. Stafford provides options to perform "[v]erification of the information conveyed by the documentation." EX1012 (Stafford) ¶65. Again, verifying hardcopy or scanned documents has nothing to do with the hash values of the one-time pads (IdSig1 and IdSig2), let alone showing issuing agency verification of IdSig1 and IdSig2. *See* EX1012 (Stafford) ¶65.

156. Finally, paragraph 67 describes that "[t]he original documents are also electronically scanned" and "information derived from a document or supplied by an entity is summarised into a separate text based object," which are Stafford's IdFiles. *See* EX1012 (Stafford) ¶67. Again, creating the IdFiles has nothing to do with IdSig1 and IdSig2, let alone showing issuing agency verification of IdSig1 and IdSig2. *See* EX1012 (Stafford) ¶67.

157. Notably, each of these paragraphs 62, 65, and 67 refers to the initial steps Stafford describes culminating in the creation of IdFiles. These preliminary steps Dr. Shamos points to occur long before IdSig1 and IdSig2 hash values of the one-time pads have been created. As explained in Paragraphs 140-145 of my Declaration, IdSig1 and IdSig2 hash values of the one-time pads (IdPad and IdSecPad, respectively), EX1012 (Stafford) ¶¶97, 99, are only created after the user had "select[ed] files or information for release" and "determin[ed] who pays for the service," EX1012 (Stafford) ¶84. The disclosures in paragraphs 62, 65, and 67 plainly do not teach any verification of the IdSig1 and IdSig2 hash values, much less by an issuing agency.

D. Security Risks of Sending Credential Images

158. I understand that Dr. Shamos opined it would be obvious to one of skill in the art to send "credential images" like those taught in Purves "in the context of Stafford." EX1005 (Shamos Declaration) ¶298. Dr. Shamos and Visa propose sending card images with Stafford's hash values of encrypted single-use keys:

> [Stafford's] 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.

EX1005 (Shamos Declaration) ¶298; *see also* IPR Petition at pages 59-60 (same).

159. One of ordinary skill in the art would not be motivated to adopt Dr. Shamos' proposal of sending card images with Stafford's hash values of encrypted single-use keys from a security perspective. In the following paragraphs, I explain why sending the credential images Dr. Shamos proposes along with Stafford's hash values of single-use encrypted keys open up serious security vulnerabilities.

160. But the difference in the systems and purposes of Stafford and Purves precludes the combination proposed by Visa and Dr. Shamos in the first place. Stafford is a distributed system for sending documents securely to another person or entity over the internet. EX1012 (Stafford) ¶2. Purves discloses a wallet service enrollment platform for enrolling in a digital wallet service. EX1013 (Purves) at Abstract. These two systems are not related in any way. Stafford is not a payment system and does not involve any type of payment system other than receiving payment for providing its services. *E.g.*, EX1012 (Stafford) at Fig. 2 (items 216 (decision "Who pays"), page 218 (step "Recipient Paid"), page 222 (step "IdMember Paid")). Stafford does not disclose any user interface for interacting with its system. Thus, one of ordinary skill in the art would not propose using Purves' credit card images with Stafford's document distribution system.

161. Dr. Shamos' assertion that "[Stafford's] 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" does not describe a practical scenario in the use of Stafford's system, when this might actually be useful. *See* EX1005 (Shamos Declaration) ¶298. Dr. Shamos does not explain, for example, why a user would want Stafford's system to provide images of the user's highly confidential documents, which are intended to be securely stored in encrypted form on Stafford's servers with its IdSig1 and IdSig2 hash values. The level of security used in this system, including using one-time pads and providing only hash values of the one-time pads, suggests that one of skill in the art would not thwart the entire regime by providing an image of much or all of a secured document along with the secret keys meant to convey that secured document securely.

162. Additionally, Purves itself does not disclose sending card images to a user device. Purves is a Wallet Service Enrollment Platform (WSEP) that facilitates the enrollment of payment accounts in a consumer's virtual wallet. EX1013 (Purves) at Abstract. Purves' virtual wallet system is run on a server, not on a user's device. For example, as shown in Figure 23b of Purves below, when a credit card is enrolled

in a virtual wallet, the display of the card enrollment form with card image and available data (step 2325) occurs on Wallet Server 2301. The user "clicks 'Save' button to enroll card" in step 2326. The card is then registered in the wallet in step 2327. All of this occurs on the Wallet Server 2301. Nothing in Purves indicates that any portion of the virtual wallet, card images, or card account information is stored beyond transient storage on a client or user device.

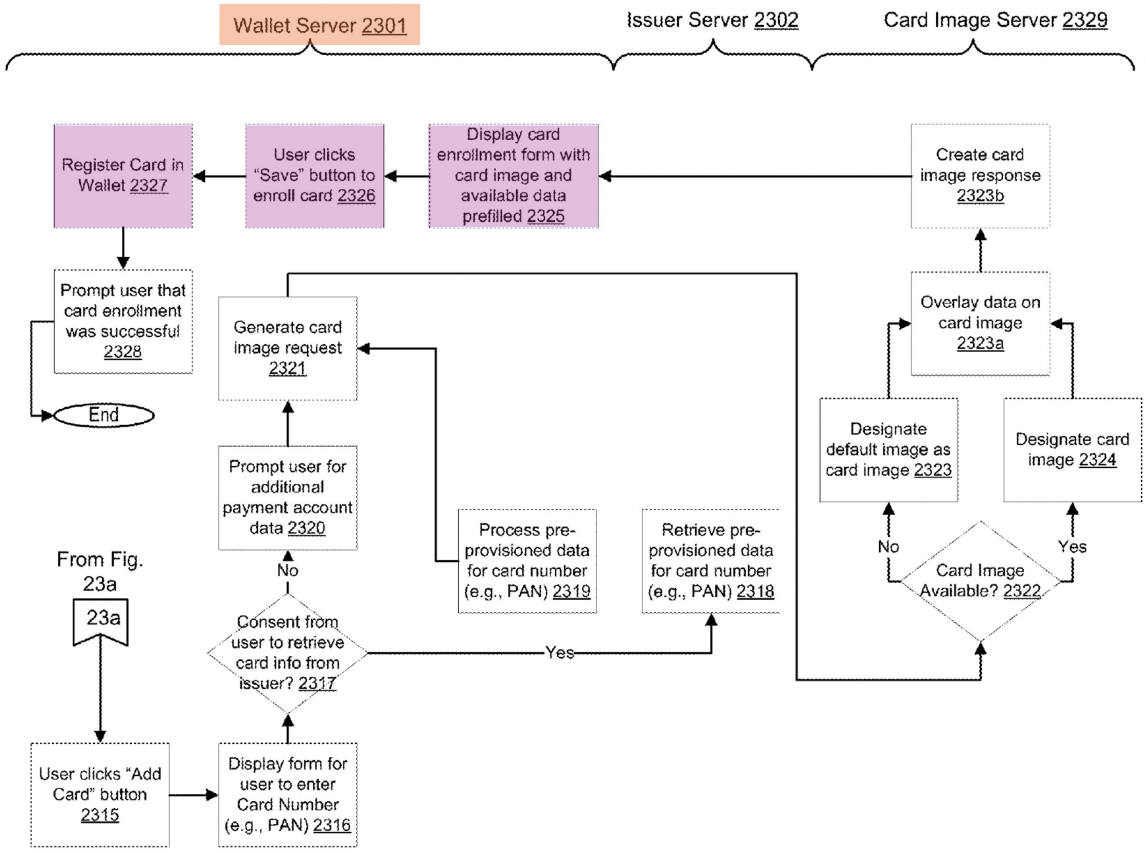


Figure 23b: Exemplary Wallet and Card Enrollment Logic Flow

EX1013 (Purves) at Fig. 23b (annotated), ¶122 (describing this process depicted in Figure 23b). Dr. Shamos confirmed this understanding at his deposition, and I agree with his testimony. EX2016 (Shamos Deposition Tr.) at pages 111:15-22, 114:5-11.

163. Moreover, even if defeating the entire security protocol was not problematic enough, Dr. Shamos provides no example from Stafford of how or when a user might need to choose among multiple sets of hash values in any user interface of Stafford. Stafford teaches that "[t]he IdMember can be presented with a listing of personal or sensitive information objects (e.g. a generic profile created earlier with a list of information objects and personal configurations or preferences of IdMember) from which he/she can select which data (or preselected set of data) to release." EX1012 (Stafford) ¶74. Stafford continues, "[t]he selected information to be released is extracted from the IdFiles. These are then moved to the staging area, using the method 200 of FIG. 2." EX1012 (Stafford) ¶74. Thus, document selection for disclosure occurs before any of the process of Figure 2 occurs, including creation of the hash values IdSig1 and IdSig2. EX1012 (Stafford) ¶84 ("Turning now to the release process 200, this process begins with the IdMember selecting files or information for release").

164. And Stafford describes seeking confirmation of the actions to be taken from the user (and possibly payment) before any such actions are taken. EX1012 (Stafford) ¶87 ("Prior to any potentially sensitive action or process of data storing

an entity's credential information, a message such as an email or webpage is generated which summarises the actions being taken by IdMember. This message requests approval for the sensitive action or process of data or release of the information. The message can be used to direct the IdMember eg using a web link embedded in an email, to a payment screen and then on to the rest of the release process."). Because the documents for release have already been selected and confirmed before any hash values are created, there is no reason in Stafford to remind a user what documents are represented by IdSig1 and IdSig2. Additionally, the IdSig1 and IdSig2 hash values are intended to be single use by the user, indicating that a user would not be selecting these values in the future for use beyond the instant transaction for which they were generated. EX1012 (Stafford) ¶¶98 (explaining that IdSig1 is "sent to payment server for use in verifying that payment for the information release has been received"), 116 ("The transaction subsystem 124 uses the MIN and IdSig1 to confirm payment for the release of the data has been made at 304."), 142 ("This form of 'release' [using pass codes] is not as secure as the previous embodiments, ***since data can be transmitted multiple times***." (emphasis added)).

165. On top of the differences in the systems of Stafford and Purves, one of skill in the art would not have sent images of encrypted credentials with the hash values of Stafford's one-time pads because doing so would thwart the purpose of

Stafford's system: securing the credentials. As I explained in Paragraph 137 of this Declaration, Stafford used encrypted one-time pads (single-use keys) for securely transmitting sensitive user information. EX1012 (Stafford) ¶¶81, 88. Sending an unencrypted card image along with them is very risky and would largely defeat the entire purpose of using Stafford's encryption methods in the first place.

166. First, Dr. Shamos' proposal of sending an unencrypted, "real image of the credential," EX1005 (Shamos Declaration) ¶298, (similar to the example shown below) over a network is ridiculously insecure.

As I explained in Paragraph 68 of this Declaration, cardholder data, including the primary account number (PAN), is very "desirable to criminals" and "they will do almost anything to get this data." EX1027 (First Data) at page 5. Electronic payment industry participants take a lot of precautions and spend a considerable amount of money to encrypt and safeguard cardholder information. As one of Visa's cited

white papers observed, "serious threats from data breaches still exist, despite the billions of dollars that merchants have already spent toward improving cardholder data security." EX1027 (First Data) at page 5. Sending that information in an unencrypted image over the internet where it could easily be intercepted and stolen, to put it mildly, is foolhardy. EX1027 (First Data) at page 5 (criminals targeting "softer targets" where data is "not encrypted"). Further, the same security risks I describe in Paragraphs 168-170 of this Declaration would also apply here.

167. Dr. Shamos also proposes sending "a real image of the credential with optionally-obscured confidential information." EX1005 (Shamos Declaration) ¶298. Below is a conceptualization of what a credit card with the confidential information obscured might look like:

That is also risky. Even if the PAN or other confidential information is obscured from the image, deconvolution techniques could be used to recover or reconstruct

the blurred information. Deconvolution is particularly effective at recovering card numbers because there are only a limited number of card numbers, and they can be guessed even if the blur is not fully removed. *See* EX1028 (Mattsson) ¶3 (Because "there are simply not enough possible credit card numbers," this opens the door to "allowing an attacker routine measures to test them all using simple brute force techniques."). Further, the same security risks I describe below in Paragraphs 168-170 of this Declaration would also apply here.

168. Finally, Dr. Shamos proposes sending a "generally-representative, issuer-provided image" of the credential. EX1005 (Shamos Declaration) ¶298. This is also risky from a security perspective. An example of what Dr. Shamos is proposing is shown below:

Consider the above image above of a Capital One® Venture Card. Even with the PAN, expiration date, and cardholder name removed, the above unencrypted image

of the credit card provides valuable information: that a user has an active credit account; that the account is with a specific card issuer (Capital One® bank); and even specifies the type of account (Venture credit card account).

169. Sending the above unencrypted image with Stafford's hash values of encrypted keys as Dr. Shamos proposes provides a security vulnerability. It would risk revealing to attackers the payload of the credential that Stafford's key is trying to securely transmit. Using the above image of the Capital One® Venture Card as an example, sending this unencrypted image would inform attackers that the credential Stafford's system is trying to securely transmit is a Capital One® Venture credit card and all of the information I have described in the previous paragraph 168. That provides the attacker with a considerable head start in using brute force techniques to guess or decrypt the payload. EX1028 (Mattsson) ¶3 (Because "there are simply not enough possible credit card numbers," this opens the door to "allowing an attacker routine measures to test them all using simple brute force techniques."). For example, the attacker would easily surmise Stafford's credential was: (1) a credit card with a 16-digit primary account number (PAN), (2) the PAN uses only digits and no characters, and (3) at least the first six-digits of the account number because "[t]he first 6 digits of a card number is devoted to the Bank Identification Number (BIN)" specific to the card issuer (here, Capital One®). EX1028 (Mattsson) ¶3. Knowing the first six digits of a credit card number reduces

the number of guesses in a brute force attack "from 10^12 to 10^6 guesses," which "[o]n a modern desktop that calculation would take 4 seconds or less." EX1028 (Mattsson) ¶3.

170. Knowing a consumer has a specific active account opens up a number of other security vulnerabilities. Most consumers have much of their sensitive data easily and publicly available, both through public records and by the large number of data breaches that have occurred over the last two decades, as I've described in Paragraphs 69-70 of this Declaration. Combining this personal information with the knowledge that a consumer has a specific open account could easily allow criminals to access that account through a variety of means, including: impersonating the user, brute force methods similar to those described above, and spear-phishing attacks. Because of all these security concerns, a person of ordinary skill in the art simply would not send images of a credential in Stafford's system with its hash values of one-time pads.

[*Paragraphs 171-179 reserved.*]

X. CONCLUSION

180. 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 called upon to testify in deposition or before the Patent Trial and Appeal Board. If called upon to testify, I would testify truthfully and competently to all matters stated in this Declaration.

181. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner raises and to take into account new information as it becomes available to me.

182. I hereby 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 that such statements are made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: 10/22/204

Sam Malek

XI. APPENDIX: LIST OF CHALLENGED PATENT CLAIMS

The bracketed numbers added to the claims below corresponds to the numbering provided in Visa's IPR petitions.

1.[Preamble] A computer-implemented method comprising:

[1.1] storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user's identity or qualifications;

[1.2] receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential;

[1.3] generating, by a processor of an OVER engine, an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user;

[1.4] transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;

[1.5] 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 Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user;

[1.6] verifying that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request; and

[1.7] transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the NFC protocol-based communication associated with the OVER file on the OVER file storage client device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine;

[1.8] requesting, by the processor of the OVER engine to the issuing agency, an agency authentication to validate the credential, wherein the issuing agency issued the credential of the user;

[1.9] receiving, by the OVER engine, a status indicator and credential information associated with the credential; and

[1.10] storing, by the OVER engine, the status indicator.

2. The computer-implemented method of claim 1, wherein the OVER file is a first OVER file, the OVER file storage client device of the user is a first OVER file storage client device of the user, the virtual representation is a first virtual representation, the official representation is a first official representation, and the method further comprises:

[2.1] receiving, from a second OVER file storage client device of the user, a second OVER file generation request to provide authentication of the user based on the information associated with the credential;

[2.2] generating, by the processor, a second OVER file comprising a second virtual representation of the credential that has been verified by the issuing agency to be a second official representation of the credential that is invalid for use in the first OVER file storage client device for authenticating the user; and

[2.3] transmitting, to the second OVER file storage client device of the user, the second OVER file in response to the second OVER file generation request.

3. The computer-implemented method of claim 1, further comprising generating, by the processor of the OVER engine, the credential, wherein the credential is generated after the processor determines that no credential of the user is stored.

4. The computer-implemented method of claim 1, further comprising generating, by the OVER engine, a device identifier for the credential, wherein the device identifier limits the credential to the OVER file storage client device.

5. The computer-implemented method of claim 1, further comprising generating, by the OVER engine, a reference to a remotely stored credential, wherein the information associated with the credential of the user comprises the reference to the remotely stored credential.

6. The computer-implemented method of claim 1, further comprising checking, by the OVER engine, a status indicator of a stored credential, wherein the OVER file generation request comprises a credential identifier for specifying which credential among a plurality of credentials of the user is officially represented by the OVER file.

7. The computer-implemented method of claim 6, wherein the OVER file comprises a portion of the stored credential.

8. [preamble] An apparatus comprising:

[8.1] a processor;

[8.2] a memory unit operatively coupled to the processor, the memory unit configured to store information associated with a credential of a user and a plurality of instructions, wherein the instructions are configured to program the processor to:

[8.3] receive, from an officially verifiable electronic representation (OVER) file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential;

[8.4] generate an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation the credential, based on the information associated with the credential of the user;

[8.5] transmit, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;

[8.6] receive, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the OVER file storage client device of the user authenticates the user based on a Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user;

[8.7] verify that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user, in response to the verifying request;

[8.8] transmit, to the OVER file third-party client verifying device, an authentication message comprising a status indicator indicating whether the OVER file corresponds to the credential of the user;

[8.9] request the credential from the issuing agency, wherein the issuing agency stores credentials issued by the issuing agency;

[8.10] receive the status indicator and credential information associated with the credential transmitted by the issuing agency; and

[8.11] store the credential and a status indicator.

9. The apparatus of claim 8, wherein the OVER file is a first OVER file, the OVER file storage client device of the user is a first OVER file storage client device of the user, the virtual representation is a first virtual representation, the official representation is a first official representation, and the instructions are further configured to program the processor to

[9.1] receive, from a second OVER file storage client device of the user, a second OVER file generation request to provide authentication of the user based on the information associated with the credential;

[9.2] generate a second OVER file comprising a second virtual representation of the credential that has been verified by the issuing agency to be a second official representation of the credential that is invalid for use in the first OVER file storage client device for authenticating the user; and

[9.3] transmit, to the second OVER file storage client device of the user, the second OVER file in response to the second OVER file generation request.

10. The computer-implemented method of claim 8, wherein the instructions further program the processor to generate the credential, wherein the credential is generated after the processor determines that no matching credential is stored.

11. The computer-implemented method of claim 8, wherein the instructions are further configured to program the processor to generate a device identifier for the credential, wherein the device identifier limits the credential to the client device.

12. The computer-implemented method of claim 8, wherein the instructions are further configured to program the processor to generate a reference to a remotely

stored credential, wherein the information associated with the credential of the user comprises the reference to the remotely stored credential.

13. The computer-implemented method of claim 8, wherein the instructions are further configured to program the processor to check a stored status indicator of a stored credential, wherein the status indicator comprises the stored status indicator.

14. The computer-implemented method of claim 8, wherein the instructions are further configured to program the processor to check a status indicator of a stored credential, wherein the OVER file generation request comprises a credential identifier for specifying which credential among a plurality of credentials of the user is officially represented by the OVER file.

15. The apparatus of claim 14, wherein when the credential identifier matches the stored credential, and the authentication message comprises the status indicator of the stored credential.

16. [preamble] A computer-implemented method comprising:

> [16.1] storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user's identity or qualifications;
>
> [16.2] receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential;
>
> [16.3] generating, by a processor of an OVER engine, an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user;
>
> [16.4] transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;
>
> [16.5] 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 Bluetooth protocol-based communication associated with the OVER file on the OVER file storage client device of the user;

[16.6] verifying that the Bluetooth protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request;

[16.7] transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the Bluetooth protocol-based communication associated with the OVER file on the OVER file storage client device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine;

[16.8] requesting, by the processor of the OVER engine to the issuing agency, an agency authentication to validate the credential, wherein the issuing agency issued the credential of the user;

[16.9] receiving, by the OVER engine, a status indicator and credential information associated with the credential; and

[16.10] storing, by the OVER engine, the status indicator.

17. The computer-implemented method of claim 16, wherein the OVER file is a first OVER file, the OVER file storage client device of the user is a first OVER file storage client device of the user, the virtual representation is a first virtual representation, the official representation is a first official representation, and the method further comprises:

[17.1] receiving, from a second OVER file storage client device of the user, a second OVER file generation request to provide authentication of the user based on the information associated with the credential;

[17.2] generating, by the processor, a second OVER file comprising a second virtual representation of the credential that has been verified by the issuing agency to be a second official representation of the credential that is invalid for use in the first OVER file storage client device for authenticating the user; and

[17.3] transmitting, to the second OVER file storage client device of the user, the second OVER file in response to the second OVER file generation request.