

Filed on behalf of: Visa Inc.

By: Matthew A. Argenti (margenti@wsgr.com)
Michael T. Rosato (mrosato@wsgr.com)
Patrick M. Medley (pmedley@wsgr.com)
Joseph M. Baillargeon (jbailargeon@wsgr.com)
WILSON SONSINI GOODRICH & ROSATI

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

Case No. IPR2024-00488
Patent No. 9,954,854

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 9,954,854**

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
A. The '854 Patent	2
B. Prosecution History	4
C. Background and State of the Art.....	5
D. Level of Skill in the Art.....	9
II. Statement of the Precise Relief Requested for Each Claim Challenged	10
III. Claim Construction.....	11
A. “OVER file”	12
B. “scan”	13
C. “...verified by an issuing agency...”	14
IV. Ground 1: Claims 1-17 were Obvious over Osborne.....	15
A. Overview of Ground.....	15
B. Claim 1	16
C. Claim 8	35
D. Claim 15	38
E. Claims 2, 9, and 16.....	39
F. Claims 3-4, 10-11, and 17	41
G. Claims 5 and 12.....	42
H. Claims 6 and 13	44
I. Claims 7 and 14.....	45
V. Ground 2: Claims 1-17 were Obvious over Osborne and Neafsey.....	47
VI. Ground 3: Claims 1-17 are Obvious over Stafford, Purves, and Neafsey	48
A. Overview and Rationale to Combine	48
B. Claim 1	52
C. Claim 8	69
D. Claim 15	71

E.	Claims 2, 9, and 16.....	72
F.	Claims 3-4, 10-11, and 17	73
G.	Claims 5 and 12.....	74
H.	Claims 6 and 13.....	74
I.	Claims 7 and 14.....	75
VII.	Discretionary Denial is Not Warranted	76
VIII.	Grounds for Standing.....	77
IX.	Conclusion	77
X.	Mandatory Notices under 37 C.F.R. §42.8.....	79
XI.	Payment of Fees under 37 C.F.R. §§42.15(a) and 42.103	81
XII.	Certificate of Compliance.....	82
XIII.	Appendix – List of Exhibits.....	83

LISTING OF CHALLENGED CLAIMS

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

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

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

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

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

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

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

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

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

[1.5] accessing, by the OVER file verifying device, a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation

of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential;

[1.6] transmitting, by the OVER file verifying device, to the OVER engine, a second verifying request to verify that the second OVER file scanned at the second client device authenticates the user;

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

[1.8] outputting a second status indicator expressing whether the second OVER file authenticates the user.

2. The computer-implemented method of claim 1, wherein the first OVER file further comprises a device identifier for the original credential configured to limit the first OVER file, for use in authenticating the user using the information of the original credential, to the first OVER file client device

3. The computer-implemented method of claim 1, wherein the first OVER file further comprises user-specific information.

4. The computer-implemented method of claim 3, wherein the user specific-information comprises at least one of:

biometric information, location information, a password, or a device identifier.

5. The computer-implemented method of claim 1, wherein the first OVER file comprises a portion of the original credential stored by the OVER engine.

6. The computer-implemented method of claim 1, wherein the first authentication message comprises an indication that the first OVER file is expired.

7. The computer-implemented method of claim 1, further comprising accessing, by the verifying device, from the first OVER file client device,

additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been satisfied.

8.[Preamble] An officially verifiable electronic representation (OVER) file verifying device comprising:

[8.1] a hardware processor;

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

[8.3] accessing a first OVER file stored on a first OVER file client device, the first OVER file comprising:

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

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

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

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

[8.4] transmitting to the OVER engine a first verifying request to verify that the first OVER file accessed from the first OVER file client device authenticates the user;

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

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

[8.7] accessing a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential;

[8.8] transmitting to the OVER engine a second verifying request to verify that the second OVER file scanned at the second client device authenticates the user;

[8.9] receiving a second authentication message comprising a second indication of whether the second scan associated with the second OVER file on the device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine; and

[8.10] outputting a second status indicator expressing whether the second OVER file authenticates the user.

9. The device of claim 8, wherein the first OVER file further comprises a device identifier for the original credential configured to limit the first OVER file, for use in authenticating the user using the information of the original credential, to the first OVER file client device.

10. The device of claim 8, wherein the first OVER file further comprises user-specific information.

11. The device of claim 10, wherein the user specific-information comprises at least one of:

biometric information, location information, a password, or a device identifier.

12. The device of claim 8, wherein the first OVER file comprises a portion of the original credential stored by the OVER engine.

13. The device of claim 8, wherein the first authentication message comprises an indication that the first OVER file is expired.

14. The device of claim 8, wherein the operations further comprise accessing, from the first OVER file client device, additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been satisfied.

15.[Preamble] A non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to perform operations comprising:

[15.1] accessing a first OVER file stored on a first OVER file client device, the first OVER file comprising:

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

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

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

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

[15.2] transmitting to the OVER engine a first verifying request to verify that the first OVER file accessed from the first OVER file client device authenticates the user;

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

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

[15.5] accessing a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing

agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential;

[15.6] transmitting to the OVER engine a second verifying request to verify that the second OVER file scanned at the second client device authenticates the user;

[15.7] receiving a second authentication message comprising a second indication of whether the second scan associated with the second OVER file on the device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine; and

[15.8] outputting a second status indicator expressing whether the second OVER file authenticates the user.

16. The computer readable medium of claim 15, wherein the OVER file further comprises a device identifier for the original credential configured to limit the first OVER file, for use in authenticating the user using the information of the original credential, to the OVER file client device.

17. The computer readable medium of claim 15, wherein the first OVER file further comprises user-specific information comprising at least one of:

biometric information, location information, a password, or a device identifier.

Visa Inc., (“Petitioner” or “Visa”) requests review of U.S. Patent No. 9,954,854 (“the ’854 patent,” EX1002), currently assigned to Cortex MCP, Inc. (“Patent Owner”). This petition demonstrates by a preponderance of the evidence that claims 1-17 (“Challenged Claims”) of the ’854 patent are unpatentable as obvious.

I. INTRODUCTION

The ’854 patent purports to have invented a method for storing and verifying credentials. However, the claims of the ’854 patent merely recite known methods for online credential management without adding anything new or non-obvious.

The Challenged Claims recite generating files called “officially verifiable electronic representation” (OVER) files, which include representations of credentials such as a driver’s license and which can provide virtual credentials to be scanned and verified by third parties. In its complaint (EX1018), Patent Owner has interpreted the claim terms broadly, mapping digital tokens to the claimed “OVER files.” However, as explained herein, tokenization and systems for management and verification of electronic credentials, including device-specific virtual credentials, were well-known before the alleged invention of the challenged patent.

Claims 1-17 of the ’854 patent should be found unpatentable and cancelled.

A. The '854 Patent

The '854 patent is entitled “File Format and Platform for Storage and Verification of Credentials.” EX1002, Title. The '854 patent describes methods to generate and verify a credential using an “Officially Verifiable Electronic Representation (OVER) File,” which “may provide a secure file format and platform for the storage and verification of key user or consumer credentials.” EX1002, Abstract, 3:57-60. The '854 patent describes that OVER files may be generated, sent to user devices, and presented to third parties in place of a traditional credential, such as a driver’s license, insurance credentials, electronic coupons, loyalty cards, discount cards, and credit cards. EX1002, 6:50-8:16, 9:64-10:2, 10:39-58, Figs. 2-3.

The independent claims recite computer-implemented methods, devices, and non-transitory computer-readable media involving the use of OVER files that are associated with user credentials, as well as reciting steps involving engines and client devices that deal with such files. The use of OVER files can involve interactions between three parties, as shown in Fig. 1 (below).

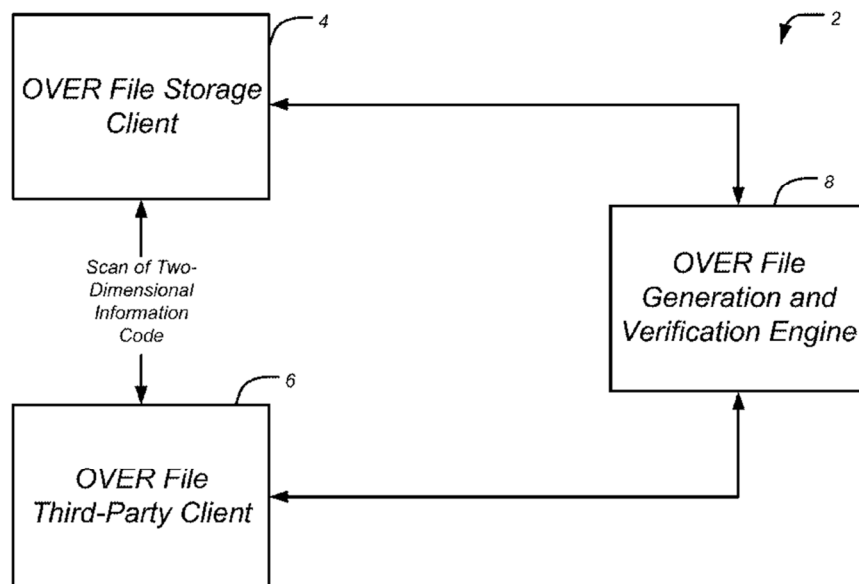


Fig. 1

EX1002, Fig. 1. The OVER file engine stores credential information for a user and generates an OVER file, providing it to the OVER file storage client of the user's device. EX1002, 4:15-32. The user presents the OVER file to a third party (e.g., a merchant) as though it were a credential, and based on a scan associated with the OVER file, the third party sends a message to the OVER file engine seeking verification of the OVER file. *Id.* The engine can respond by confirming whether the OVER file is valid. EX1002, 8:17-54.

Each independent claim recites similar limitations describing steps performed by an OVER file verifying device (e.g., corresponding to the OVER file

third party client shown in Fig. 1). Claim 1, for example, recites a computer-implemented method with steps of accessing an OVER file stored in a user's client device, transmitting a verifying request to an OVER engine, receiving an authentication message, and outputting a status indicator expressing whether the OVER file authenticates the user. These steps are performed twice, for a first OVER file on a first client device and a second OVER file on a second client device, with the second OVER file being invalid for use in the first client device.

Independent claims 8 and 15 recite similar limitations with claim 8 directed to an OVER file verifying device and claim 15 directed to a computer-readable medium.

As to the remaining Challenged Claims, none adds anything beyond steps conventionally known in the art. EX1005, ¶¶42-73.

B. Prosecution History

The '854 patent was filed as U.S. Application No. 14/982,981 ("the '981 application") on December 29, 2015, claiming priority to U.S. Application No. 13/794,878 ("the '878 application"), filed March 12, 2013, and Provisional Application No. 61/740,731, filed December 21, 2012. EX1002, Face. For purposes of this petition only, Visa assumes a priority date of December 21, 2012.

During prosecution, the Examiner issued a single office action, rejecting the pending claims over two prior art references. EX1008, 130-50 (citing U.S. Patent

Publication No. 2009/0307756 to Kang and U.S. Patent Publication No. 2012/0240204 to Bhatnagar). None of the prior art at issue in this proceeding was raised during prosecution.

To secure allowance, Applicant agreed to an Examiner's amendment that incorporated a dependent claim into each independent claim. EX1008, 38-44. Applicant had argued that this dependent claim required "verif[ying] two separate OVER files for authenticating the same user, using two separate OVER file client devices, because the second OVER file is invalid for use in the first OVER file client device." EX1008, 104-05. In the Notice of Allowance, the Examiner indicated that the asserted prior art failed to teach this limitation as well as limitations directed to the OVER file being "verified by an issuing agency to be an official representation of the credential" and "receiving an authentication message." EX1008, 44-45.

C. Background and State of the Art

This petition is supported by the Declaration of Dr. Michael I. Shamos, a Professor in the Carnegie Mellon Department of Computer Science. EX1005, ¶¶1-22; EX1006. As Dr. Shamos explains and as addressed in further detail below, the involved claims would not have been considered new or non-obvious to a person of ordinary skill in the art ("POSA") at the relevant time.

The brief background described below provides a concise overview of some important elements of credential storage and verification that Dr. Shamos explains are relevant to a POSA's understanding as of the '854 patent's priority date.

EX1005, ¶¶101-211.

1. Credential verification systems

Credential verification systems were well known, including those involving a user, a credential manager, and a third party seeking verification of a credential. For example, U.S. Patent Publication No. 2009/0271321 ("Stafford," EX1012) taught such a system "for storing, validating and disseminating credential information about an entity." EX1012, Abstract. Stafford's system receives and stores credential information, including scans of credentials, and distributes sensitive credential information to third parties using key signatures to unlock their release. EX1012, ¶¶10, 62, 73-75, 93-97, 107-25, Figs. 2-3. The techniques employed by Stafford were not unique to it, but rather represented well-understood and broadly-applied techniques to those skilled in the art. EX1005, ¶¶102-08 (citing EX1019).

One well-established method to facilitate transactions was to use electronic tokens, in a process called "tokenization." In tokenization, a digital "token" is used as a substitute for a credential such as a credit card. The token could be limited to a single device or transaction, so that if an eavesdropper or malicious third party

obtained the token, it could not be used. A credit card number, by contrast, could be used by an unauthorized party. Systems employing electronic tokens would store users' credential information remotely, associating them with tokens distributed to the users. By providing such a token in a transaction with a third party, a user would be able to conduct a transaction with the stored credential. EX1005, ¶¶109-43, 153-75 (citing EX1011-EX1017, EX1020-EX1040).

An example system employing tokenization technology is provided by U.S. Patent Publication No. 2012/0316992 ("Osborne," EX1011). Osborne is a Visa patent publication teaching a "payment privacy tokenization" (PPT) apparatus that facilitates methods in which users sign up for tokenized transactions, user credentials are associated with a token issued to the user, and the token's authenticity is verified when used for transactions with third parties. EX1011, ¶¶22, 35, 40-54, Figs. 4-7F. The tokenization techniques employed by Osborne were well-understood by the POSA and similar technologies had been employed in various related applications. EX1005, ¶161-67. *See generally id.*, §VIII.B.

2. Formats used for virtual credentials

When using remote credential verification systems to facilitate transactions, it was recognized to be useful for users to employ virtual representations of credentials to replace mechanisms traditionally provided by physical credentials. EX1005, ¶¶102-08. For example, when using a mobile device to employ credential

management systems like virtual wallets, it was convenient to provide visual indications of available credentials. EX1005, ¶¶168-171. For example, U.S. Patent Publication No. 2013/0054454 (“Purves,” EX1013) is a Visa patent publication disclosing methods for enrollment of payment accounts in users’ electronic wallets. EX1013, Abstract. Purves teaches that a user’s accounts may be illustrated using images of credentials such as credit cards. EX1013, ¶85. This type of representation would help users by providing a simple method to choose a credential for a transaction. EX1005, ¶¶168-71.

3. Mechanisms to convey virtual credential information

Various mechanisms were known to initiate a transaction with a third party. In one example, Osborne teaches that various types of interaction could trigger tokenized transactions, such as a Near Field Communication (NFC) interaction. EX1011, ¶49. Similarly, Purves teaches that a QR code may be used to trigger a wallet connection, such as connecting to a merchant. EX1013, ¶64; EX1005, ¶¶171, 176-84 (citing EX1041-1043).

There were also well-known ways of conveying information associated with credential files from a user to a third party. For example, U.S. Patent Publication No. 2013/0212248 (“Neafsey,” EX1015) discloses methods of credential management, including systems for disseminating virtual credentials in multiple

different formats, including scannable codes like optical codes. EX1015, ¶¶61; EX1016, 12.

Further, Neafsey teaches that credentials may be generated for different user devices based on device identifiers unique to each device. EX1015, ¶¶48-49; EX1016, 10; EX1005, ¶¶153-54. Such use of device identifiers to tie electronic representations to particular devices was well-known. EX1005, ¶¶198-3. For example, Osborne teaches including device identifiers such as MAC addresses in its token data when distributing tokens to user devices and using techniques of device fingerprinting to tie its tokens to such devices. EX1011, ¶¶26, 47, 148; EX1005, ¶¶199. A known benefit of tying a token to a particular device is that an eavesdropper who somehow obtains the token cannot use it on any other device. EX1005, ¶¶102-8.

D. Level of Skill in the Art

As Dr. Shamos explains, a person of ordinary skill in the art (POSA) by December 21, 2012, would typically have a bachelor's degree in computer science, computer engineering, or a related field, with at least two years of work involving electronic payment systems, network authentication systems, or related areas. A POSA could have less education but significant professional experience in one or more of these fields. *See* EX1005, ¶¶74-79.

II. STATEMENT OF THE PRECISE RELIEF REQUESTED FOR EACH CLAIM CHALLENGED

Visa requests review of claims 1-17 of the '854 patent under 35 U.S.C. §311 and AIA §6. The grounds for relief are as follows:

Ground	Claims	Description
1	1-17	35 U.S.C. §103: obvious over Osborne ¹
2	1-17	35 U.S.C. §103: obvious over Osborne and Neafsey ²
3	1-17	35 U.S.C. §103: obvious over Stafford, ³ Purves, ⁴ and Neafsey

¹ Osborne was filed on June 7, 2012, and published on December 13, 2012.

Osborne is prior art under pre-AIA 35 U.S.C. §§102(a) and (e).

² Neafsey was filed on February 13, 2013, and published on August 15, 2013.

Neafsey claims priority to U.S. Provisional Patent Application No. 61/598,219 (the “Neafsey Provisional,” EX1016), filed February 13, 2012. As discussed below, Neafsey is available as prior art as its provisional filing date.

³ Stafford was filed on May 31, 2007, and published on October 29, 2009.

Stafford is prior art under pre-AIA 35 U.S.C. §§102(a), (b), and (e).

⁴ Purves was filed on September 21, 2012, and published on February 28, 2013.

Purves is prior art under pre-AIA 35 U.S.C. §102(e).

This petition provides parallel citations to both Neafsey and corresponding disclosure in Neafsey Provisional, demonstrating that all matter relied on is found in both documents. Under *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375 (Fed. Cir. 2015), Neafsey is available as prior art under pre-AIA 35 U.S.C. §102(e) as of February 13, 2012, as illustrated by the chart below illustrating exemplary support in Neafsey Provisional for claim 1 of Neafsey. *See* EX1005, ¶¶142-50.

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

III. CLAIM CONSTRUCTION

Claim terms should be given their ordinary and customary meaning as would be understood by a POSA in light of the specification. 37 C.F.R. §42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc). Unless otherwise stated, this petition applies the ordinary and customary meaning of the claim terms. The following terms warrant discussion.

A. “OVER file”

Each independent claim recites an “officially verifiable electronic representation (OVER)” file. The claims also use “OVER” or “OVER file” to characterize other claim elements relating to the OVER file (e.g., “OVER engine,” “OVER file verifying device”). Like the claims, the specification uses the term “OVER” to refer to an “Officially Verifiable Electronic Representation.” EX1002, 2:33-35. The specification describes that an OVER file may contain “credential information.” EX1002, 6:33-35, 6:67-7:3. An OVER file may also contain or act as a credential, which may in turn be representative of another credential, such as a driver’s license. EX1002, 12:23-26. This “OVER file credential” may include an image from an issuing agency, such as a logo or a card image, and the OVER file may also include a scannable code, like a QR (quick response) code. EX1002, 9:26-30, 14:19-29, Fig. 11; EX1005, ¶¶83-85.

The ’854 patent does not describe that tokens may be either an OVER file or a part of one (such as a representation of a credential). However, Patent Owner’s complaint expressly identifies tokens as OVER files. *See, e.g.*, EX1018, 4 (“Each OVER File is a token....”), 9 (for an “OVER file comprising a virtual representation,” “[t]he token is the ‘virtual representation’”), 16-17 (“The token (i.e., ‘first OVER file’) acts a first virtual representation of the user’s credentials....” (for related patent)); EX1005, ¶86. For the purposes of this

petition, Visa applies a construction that includes Patent Owner’s interpretation of this term.

Accordingly, this petition applies an interpretation of “OVER file” as encompassing a file comprising an image of (or associated with) the credential (as described in the specification and addressed in ground 3), but also encompassing a file comprising a virtual representation in the form of a token (as asserted in Patent Owner’s infringement complaint and addressed in grounds 1-2). EX1005, ¶¶83-88.

B. “scan”

Each independent claim recites a “scan associated with the [first/second] OVER file.” The specification describes that an OVER file can include an “information code,” and a third-party device can “scan 220 the information code displayed on the user device.” EX1002, 7:65-8:16. The “scannable code” can be “for example, a barcode or a QR code.” EX1002, 14:19-29; *see also id.*, 5:16-35. The specification also refers to using information codes involving radio and electronic transmissions or interactions like Near Field Communication (NFC), Bluetooth, or sensor readings; however, it does not specify that such interactions involve scans and describes these embodiments as alternatives to other embodiments that use scans. EX1002, 5:16-35, 12:17-50. Thus, the specification uses “scan” to refer to an optical scan, but it does not use “scan” to refer to other types of interactions like electronic interactions. EX1005, ¶¶89-94.

Nonetheless, Patent Owner has asserted in its complaint that a proximity-payment request (e.g., an NFC interaction) constitutes a scan. EX1018, 10 (“proximity-payment request (i.e., scan associated with the OVER file)” (for related patent)), 36 (“scan the OVER file...such as through an NFC or a card reader”). Accordingly, this petition applies an interpretation of “scan” that encompasses an optical scan (as addressed in Grounds 3-6), while also encompassing an NFC interaction (as addressed in Grounds 1-2 and asserted in the complaint). EX1005, ¶¶89-96.

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

Each independent claim recites 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.” During prosecution of the parent application, Applicants argued that this phrase requires that the issuing agency verify that the *virtual representation* is an official representation of the credential. *See* EX1007, 44-45; *see also id.*, 40 (pointing to disclosure found at EX1001, 3:50-4:6, 4:25-41, 5:7-25, 6:12-36). Accordingly, this petition construes this phrase to require that an issuing agency have verified a *virtual representation* in an OVER file as being an official representation of a credential. EX1005, ¶¶97-100.

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

A. Overview of Ground

As discussed below, Osborne discloses or suggests each and every element of independent claims 1, 8, and 15, as well as the elements of dependent claims 2-7, 9-14, and 16-17. In particular, Osborne teaches the use of tokens representative of credentials such as credit cards to perform transactions with third parties, in a manner that meets or renders obvious each element of these claims. This ground applies interpretations of *OVER file* and *scan* consistent with Patent Owner's district court complaint (i.e., encompassing use of a token and an NFC interaction, respectively). *See supra* §§III.A-B; EX1005, ¶212.

As addressed below for element 1.3's requirement that the OVER file's *virtual representation* (mapped here to a token) must be verified as an official representation of a credential by an issuer, Osborne teaches or at least suggests that its token server may be the issuer of a user's credentials. In such a system, it would at minimum have been obvious that the OVER file comprising a virtual representation of the credential has been verified by the issuer as an official representation, since the issuer is the entity issuing the token as well as the credential. EX1005, ¶213; *see infra* §IV.B.4 (discussing this for element 1.3).

The discussion of claims 1-17 below provides further detail regarding POSAs' rationale to apply Osborne's teachings to arrive at the claimed invention with a reasonable expectation of success.

B. Claim 1

Osborne teaches or suggests each element of claim 1, as discussed below. EX1005, ¶¶214-40.

1. Preamble

1. A computer-implemented method comprising:

Osborne teaches a computer-implemented method. *See, e.g.*, EX1011, ¶¶35-38 (computing devices in communication with merchant server, database, and token server), 114-22 (describing computerized system used to perform Osborne's methods); EX1005, ¶215.

2. Element 1.1

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

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

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

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

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

Element 1.1 is lengthy, and it is most easily understood by addressing its sub-elements out of order. In brief, an *OVER engine* is configured to generate a *first OVER file* with characteristics as recited above and transmit it to a *first OVER file client device*, from which it is accessed by an *OVER file verifying device*.

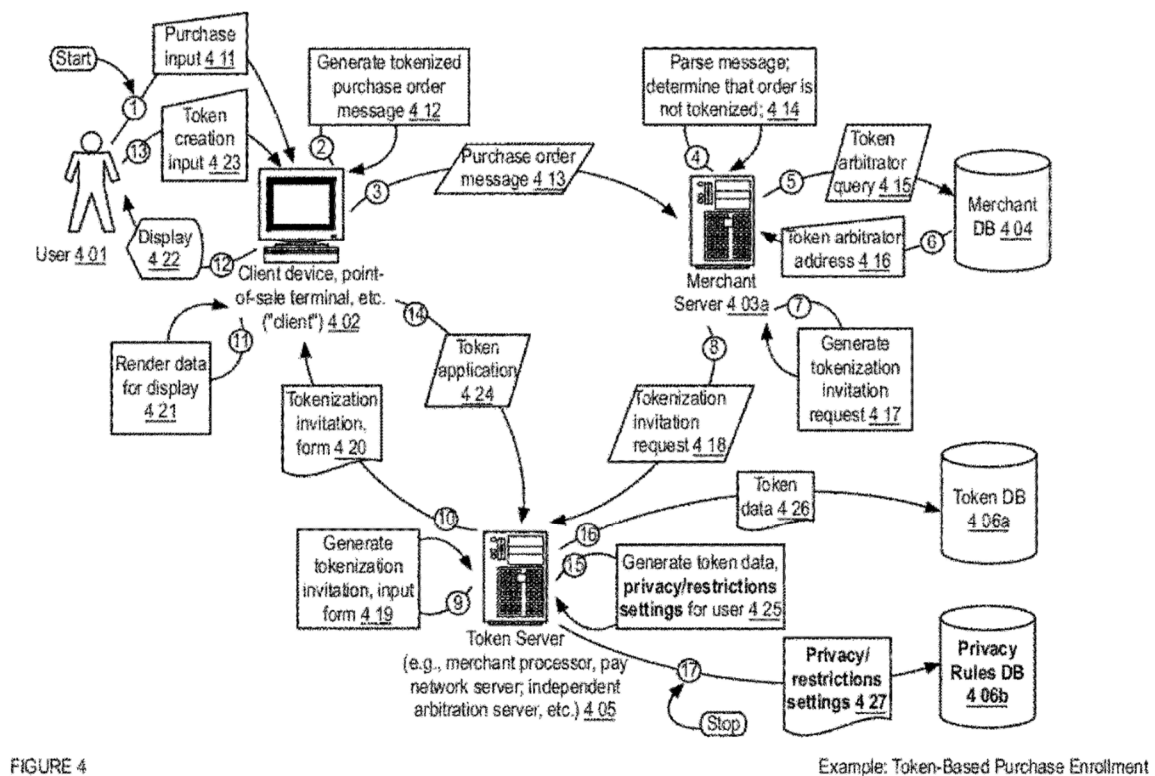
Osborne teaches such an arrangement for token-based transactions, as described below. EX1005, ¶¶216-17.

OVER engine, verifying device, and client device

First, Osborne teaches an *OVER engine*, in the form of a “payment privacy tokenization apparatus” or “PPT” apparatus to “transform payment token-based purchase orders, via PPT components, into multi-issuer purchase payment funds transfers.” EX1011, ¶¶22, 166. This system includes a “token server,” also referred to as a “token arbitrator,” that may be any entity involved in the PPT, such as “a pay network server.” EX1011, ¶53. Osborne also notes that the “the source of the token” may be the “issuer” (e.g., a funding source for the user’s account). EX1011, ¶47; *see also id.*, ¶48 (noting in XML comments that the token administrator may

be the funding source, or that “alternatively token administrator may be different from funding source”), ¶29 (user may obtain token from funding source); EX1005, ¶218.

The PPT system also includes a “merchant server” in communication with a user via clients, which may include devices such as “a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, and/or the like.” EX1011, ¶35. Osborne depicts the general arrangement of customers, parties, and the pay network server (which can include the PPT apparatus) in Fig. 4, reproduced below:



EX1011, Fig. 4. This system includes the *OVER file verifying device* (e.g., merchant point-of-sale device in communication with merchant server), as well as the *first OVER file client device* (user device, such as a card or mobile device communicating with the verifying device). EX1005, ¶219-20.

OVER file

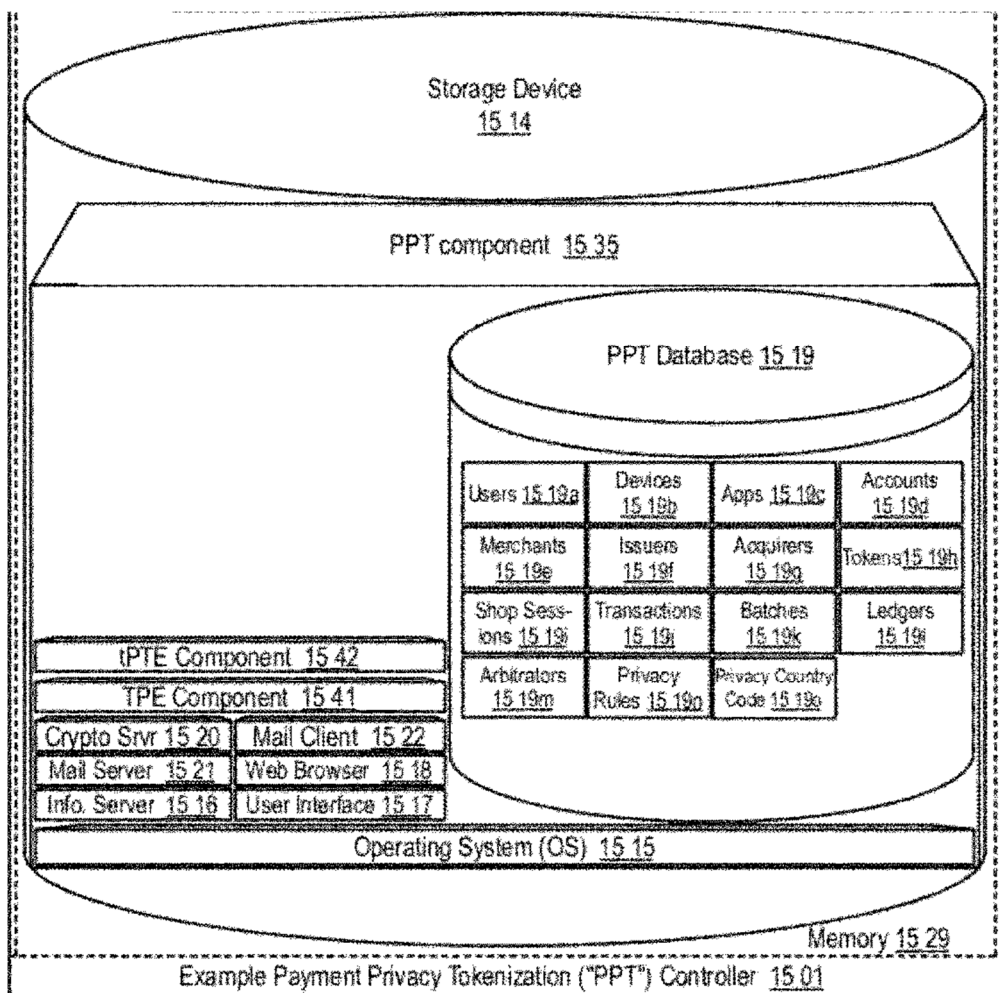
The PPT apparatus generates and verifies tokens used for transactions, corresponding to the recited *OVER file*, as discussed below. EX1011, ¶25; EX1005, ¶¶220-21.

The PPT apparatus generates tokens in response to receipt from a user of a token application received by a token server of the PPT apparatus. EX1011, ¶¶35, 40-47, 54. Osborne provides an example encoding of a tokenization application form, shown below:

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

EX1011, ¶40. This form provides *information associated with the original credential of the user* that the PPT stores, such as account number, type, billing address, etc., for the user’s credit cards. Osborne’s PPT apparatus includes a storage

device storing account information in a database, as shown in Fig. 15, excerpted below.



EX1011, Fig. 15; *see id.*, ¶¶114, 146-51. The database’s “Accounts table 1519d,” includes fields for storing the *information associated with the credential* (e.g., information about the user’s credit cards), such as “account_number,” “issuer_name,” “account_address,” “routing_number,” etc. EX1011, ¶147; EX1005, ¶222.

The token server uses these stored values to generate a data record and data structure for a token (*OVER file*), as well as a “token identifier” representing the token, which is provided to the user. EX1011, ¶¶41, 47-48, Fig. 5 (showing process); EX1005, ¶223. As depicted in Fig. 1B (below), the token is a virtual representation of a credential, such as a credit card.

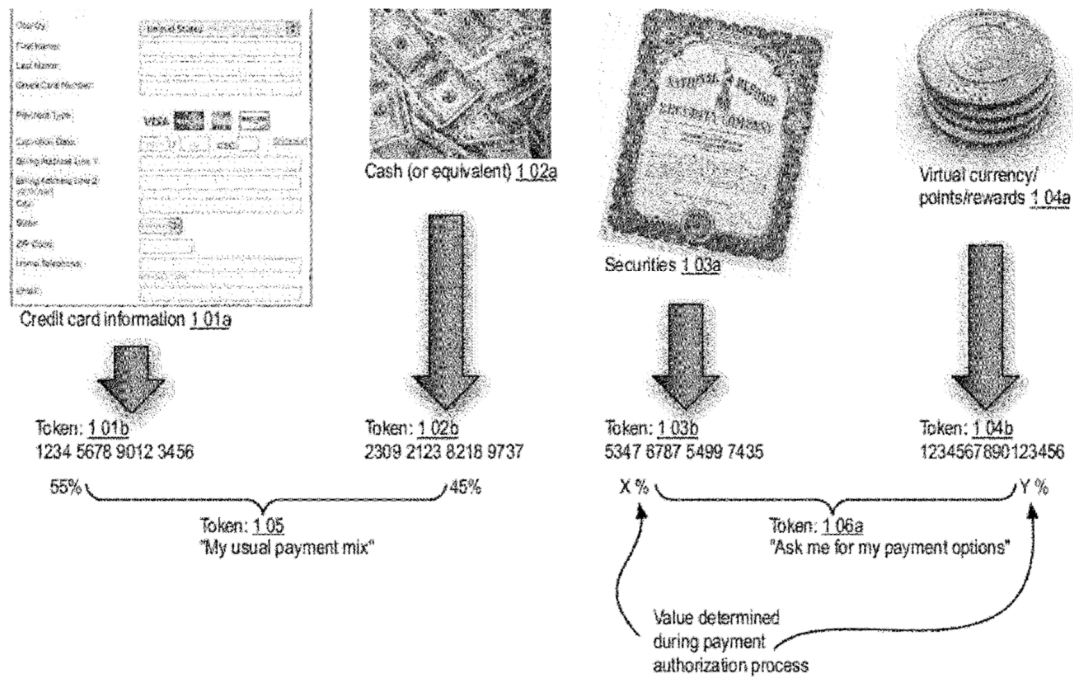


FIGURE 1B

Example: Payment Tokenization

EX1011, Fig. 1B; *see also id.*, ¶25 (confirming that token is “linked to credit card information” and used “in lieu of...card information”). Thus, the token is a *virtual representation of an original credential of a user* that is generated based on the information associated with the credential. EX1005, ¶223. Osborne teaches that a user “desir[ing] to utilize a card” may use “tokens in lieu of payment information,”

using the token to prove identity to a merchant as a stand-in for credit card or account information. EX1011, ¶25. Thus, the token is a *first new credential* used *for proving the user's identity or qualifications*, by standing in for an *original credential*. EX1005, ¶223.

...verified by the issuing agency...

Oborne teaches or at least suggests that the token would be verified by the issuing agency as an official representation. *Supra* §IV.A. As discussed above when addressing the OVER engine, Oborne teaches that any entity can operate as the token server, and it specifically identifies that the token may be provided by the credential's "funding source"—that is, by the agency that issued the credential. EX1011, ¶¶29, 47-48, 53; *see also id.*, ¶58 ("Issuer server(s)...of the issuer(s) may maintain details of the user's account linked to the payment token."). By generating the token and providing it to the user to represent the credential it has issued, the issuer would be verifying it to be an official representation of the credential. EX1005, ¶224.

Moreover, as Dr. Shamos explains, a POSA would have found it obvious for an issuer, upon generating the token, to verify that it was an official representation of the credential, using stored credential information identified by the token application form when generating the token, since verifying the token would be a

routine step based on the credential data received and doing so would increase confidence that the token legitimately represented the credential. EX1005, ¶225.

To the extent Patent Owner argues that the claim requires that the credential, rather than the token, be verified by the issuer, a POSA would have found it obvious that a credential is verified by virtue of being issued by an official issuer. Indeed, since the purpose of a credential is to be an official representation from the issuer, an issuer would make such a verification as a matter of course when issuing the credential. EX1005, ¶226.

transmit[ted] to the client device

Osborne teaches that a “token may be provided as a data structure via HTTP(S) POST, as a file, as an attachment (e.g. via email), and/or provided to the client device for later use.” EX1011, ¶48. This transmission to the client device is performed after receiving the token application as shown in Fig. 5, with step 517 occurring as a step after receiving a token generation request from the user (shown in steps 508 and 515). See EX1011, ¶¶40-41, 46-47, Fig. 5 (below). Osborne’s token server thus sends a token (*OVER file*) to the user’s device (*OVER file client device of the user*). EX1005, ¶227.

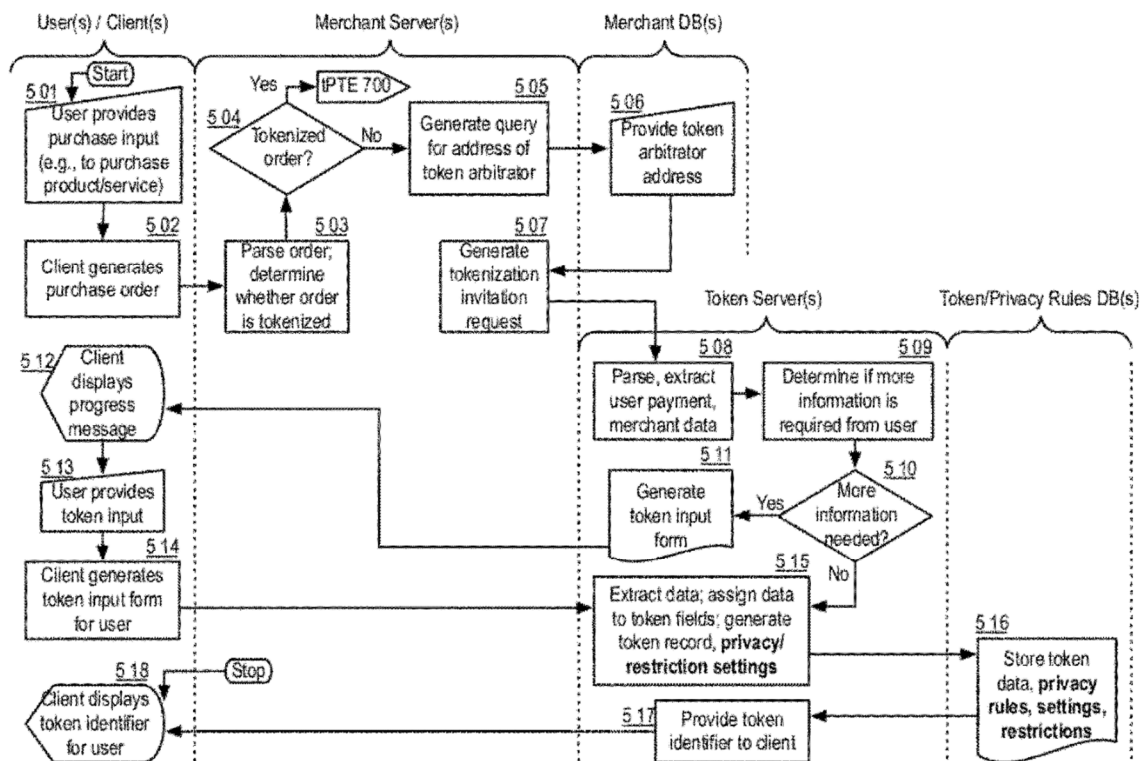


FIGURE 5

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

accessing the OVER file

Oborne teaches that the *OVER file verifying device accesses the first OVER file*. Oborne teaches a user may communicate with a merchant server via a client (e.g., "mobile device" or "point-of-sale-terminal") by "activating a RFID/NFC enabled hardware device" EX1011, ¶49. This triggers a tokenized purchase with the merchant, via a *third-party client verifying device* (the merchant server, alone or in conjunction with the merchant's point-of-sale device interacting with the user's device via NFC). EX1011, ¶50 (client provides "tokenized purchase order message to the merchant server"). For example, Oborne teaches that a "user may

be able to pass a token...to a merchant,” and “upon receiving a payment token from the user, the merchant may pass the token to a transaction arbitrator.”

EX1011, ¶25. By receiving and passing the token, the merchant device *accesses...a first OVER file* on the user device, as recited. EX1005, ¶¶228-29.

Osborne thus teaches or suggests each limitation of element 1.1. EX1005, ¶¶216-29.

3. Element 1.2

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

Osborne teaches this element as part of a merchant’s token arbitration request (*first verifying request*) triggered by a purchase order request from a user. To process the purchase order request, the merchant server sends a “token arbitration request...to a token server.” EX1011, ¶¶51-52. This is the verifying request of element 1.2. An example of an encoding of such a request, which includes a token_id field representing a token, is reproduced below.

```

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

```

Id., ¶50; EX1005, ¶230. Osborne teaches that the “token server may parse the token arbitration request message” and “determine whether the user token is authenticated.” EX1011, ¶¶53-55; *see also id.*, ¶25 (“[U]pon receiving a payment token from the user, the merchant may pass the token to a transaction arbitrator.”). Osborne thus teaches that the OVER file verifying device transmits a first verifying request to verify that the OVER file verifies the user to the OVER engine. EX1005, ¶230.

Accordingly, Osborne teaches element 1.2.

4. Element 1.3

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

Osborne teaches this element. Beginning with the scan aspect, a user communicates with a merchant server via a client (e.g., “mobile device” or “point-of-sale-terminal”) by “activating a RFID/NFC enabled hardware device” EX1011, ¶49. This NFC interaction triggers a tokenized purchase with the merchant, via the *OVER file verifying device* (the merchant server, alone or in conjunction with the merchant’s point-of-sale device interacting with the user’s device via NFC). EX1011, ¶50 (client provides “tokenized purchase order message to the merchant server”). As discussed above in §III.B, Patent Owner has argued in district court that transmitting NFC-based payment requests constitutes a scan under the ’854 patent. Applying this interpretation to Osborne, since Osborne’s RFID/NFC activation triggers the purchase to be performed with the token, the RFID/NFC activation would be a *scan associated with the first OVER file on the first OVER file client device of the user*. EX1005, ¶231.

As discussed above, a token arbitration request is sent from the merchant server based on the user's purchase order. EX1011, ¶¶51-52. In response, the token server processes the token arbitration request triggered by the scan by looking up the account number in a token database. In particular, the token server "extract[s] the payment token from the message," then issues a query to a database "using the payment token as a search term in the query." EX1011, ¶53. In response, the database produces "instructions for the token server on how to proceed with payment processing." *Id.* This includes credential information such as user account numbers, as shown in the highlighted XML example reproduced below:

```

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

```

Id.; EX1005, ¶232. Osborne further teaches that the “token server may determine whether the user token is authenticated,” for example, where “no XML data is available associated with the payment token,” this indicates that the “user has not signed up for payment tokenization services.” EX1011, ¶54; *see also id.*, ¶69 (determining “whether the user token is authenticated”). In other words, the query determines whether the *scan* (RFID/NFC interaction) *associated with the first OVER file* (token) *corresponds to the information associated with the original*

credential (whether the database query for the token returns the user's account details or not). EX1005, ¶232.

Osborne further teaches that an authenticating message is sent to the merchant server comprising a first indication of the determination discussed above. For example, if “the token server determines that the user is not authenticated, e.g., 711, option ‘No,’ the token server may generate an ‘authentication fail message.’” EX1011, ¶69. As shown in Fig. 7A, steps 712a-b, this message is sent to the merchant server (*verifying device*).

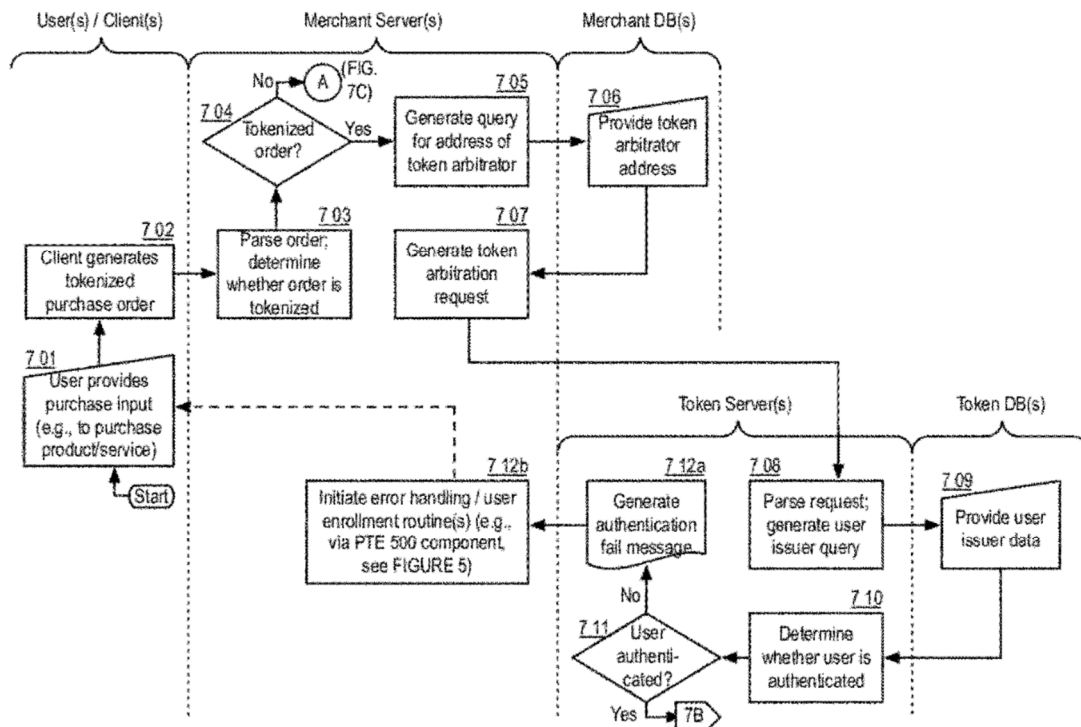


FIGURE 7A

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

EX1011, ¶69, Fig. 7A. This is an indication that the scan is not associated with the stored original credential information. EX1005, ¶233.

On the other hand, if the user token is authenticated, then the “token server may continue processing.” EX1011, ¶69. The stored user account information is then used to procure payment authorization, and a message is sent to the merchant server indicating the result. EX1011, ¶¶63 (“token server...may in turn forward the authorization success message, e.g., 647, to the merchant server”), 61 (“authorization fail’ message”), 70 (“authorization in progress” message), Figs. 7B-C. Any of these messages is an indicator that the token was authenticated, and thus that the scan corresponded to the stored original credential information. EX1005, ¶234.

Osborne thus teaches element 1.3.

5. Element 1.4

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

Osborne teaches this element. For example, an authentication failure message triggers “an error handling routine and/or a user enrollment routine,” which Fig. 7A illustrates may be performed by the merchant server. EX1011, ¶69, Fig. 7A. The initiation of these routines would be a status indicator expressing non-authentication (e.g., offering to enroll a user for tokens would indicate the user

lacked an authenticated token). EX1005, ¶235. On the other hand, after successful authentication and an authorization success, “merchant server may add a record of the transaction for the user” and also “provide the purchase receipt to the client,” which renders it for the user. EX1011, ¶73. This, too is a status indicator expressing successful authentication. EX1005, ¶235; *see id.*, ¶¶203-05 (citing EX1044). Osborne thus teaches element 1.4.

6. Elements 1.5-1.8

Elements 1.5-1.8 repeat elements 1.1-1.4, with several modifications. First, the “first” OVER file and OVER file client device are replaced, respectively, with a “second” OVER file and OVER file client device. Second, element 1.6 recites that the second OVER file is “scanned at the second OVER file device” instead of “accessed from the first OVER file device.” Third, it is not specified whether the OVER engine generates the second OVER file. And fourth, element 1.5 requires that the second OVER file be a “second new credential” that is “invalid for use in the first OVER file client device for authenticating the user.” As discussed below, Osborne teaches or suggests each of the elements 1.5-1.8. EX1005, ¶236.

The existence and use of a second OVER file is satisfied by a user having two devices and receiving respective OVER files to be used on each device. This would have been obvious in view of Osborne. A POSA would have expected users to use multiple devices; indeed, Osborne teaches that the token server may keep a

device table with various identifiers for a user's devices, such as "device_ID," "device_name," "device_MAC," (referring to a MAC address) etc. EX1011, ¶148; EX1005, ¶237; *see also In re Harza*, 274 F.2d 669, 671 (C.C.P.A. 1960) ("[M]ere duplication of parts has no patentable significance unless a new and unexpected result is produced....").

The second and third differences for elements 1.5-1.8 are also taught by Osborne. As discussed for element 1.3, Osborne teaches using an NFC interaction to provide a token to a verifying device, which meets Patent Owner's own interpretation of "scan." *Supra* §§III.B, IV.B.4. It would have been obvious to use such "scans" for tokens provided to each of two different devices of a user. EX1005, ¶238. And the claim's failure to specify whether the OVER engine generates the second OVER file provides no basis at all to distinguish over Osborne.

As to the last difference—that the second OVER file be a new, device-specific credential that is invalid on the first OVER file client device, this would also have been obvious to the POSA based on Osborne's disclosure. For example, Osborne teaches that "device fingerprinting may be utilized" to provide "additional security" for use of Osborne's tokens. EX1011, ¶26. Similarly, Osborne provides an example token data structure including a "client_fingerprint" field with device-identifying information like the client's MAC address. EX1011, ¶47. To obtain the

additional security taught by Osborne, a POSA would have been motivated to employ Osborne's device fingerprinting to tie a given token to a given device, such that the token for a second device would be a new credential, different from the first token (with both being different credentials from the original credential), with the second device's token being invalid in the first device (since the first device's fingerprint would not match). EX1005, ¶239.

Thus, Osborne teaches or suggests each of elements 1.5-1.8. EX1005, ¶240.

Accordingly, claim 1 was obvious over Osborne. EX1005, ¶¶101-240.

C. Claim 8

Claim 8 is directed to an OVER file verifying device rather than a computer-implemented method, but it includes limitations virtually identical to claim 1, as discussed below. EX1005, ¶241.

1. Preamble

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

Osborne teaches an OVER file verifying device, as discussed for claim 1. *See* EX1011, ¶35, Fig. 4; *supra* §IV.B.2; EX1005, ¶242.

2. Elements 8.1-8.2

a hardware processor;

a memory unit operatively coupled to the hardware processor, the memory unit configured to store information associated with an

original credential of a user and a plurality of instructions, wherein the instructions are configured to cause the hardware processor to perform operations comprising:

As discussed for claim 1, Osborne teaches a PPT apparatus that communicates with an OVER file verifying device, in the form of a merchant server and associated point-of-sale terminal. EX1011, ¶35, Fig. 4; *supra* §IV.B.2; EX1005, ¶243. These components are depicted as computers by Osborne. *See* EX1011, Fig. 4 (showing “client device, point-of-sale terminal” 402 as computer and “Merchant Server” 403a as second computing device); *see also id.*, ¶117 (“It should be noted that the term ‘server’ as used throughout this application refers generally to a computer, other device, program, or combination thereof.”).

A POSA would understand from Osborne that the verifying device would comprise a hardware processor and memory unit. Osborne explains the general understanding of POSAs that “computers employ processors to process information; such processors 1503 may be referred to as central processing units (CPU).” EX1011, ¶115. Osborne further explains that “stored instruction codes, e.g., programs, may engage the CPU circuit components and other motherboard and/or system components to perform desired operations,” with instructions stored in in various processor accessible and operable areas of memory.” *Id.* A POSA would have understood that these basic elements of computer systems would apply

to each computerized component described by Osborne, including the merchant server and point-of-sale terminal (*OVER file verifying device*); thus, these components would include a processor coupled to a memory unit storing instructions. EX1005, ¶244. The instructions stored in Osborne’s merchant devices would be configured to perform the operations described by Osborne for those devices, which correspond to the steps recited in claim 1 (and repeated in the remaining elements of claim 8). *Id.*

The verifying device would further be configured *to store information associated with an original credential of a user* in its memory unit. As discussed above for element 1.1, Osborne teaches that such information is received by the PPT apparatus via a token application form and stored by the apparatus. *Supra* §IV.B.2. Osborne further teaches that the merchant server and point-of-sale terminal (*verifying device*) may provide the completed application including the original credential information to the token server. *See* EX1011, ¶40 (“The client may generate a completed application form, and provide, e.g., 424, the token application to the token server (either directly or via the merchant server).”). As Dr. Shamos explains, a POSA would have understood that Osborne’s client (e.g., point-of-sale device) and the merchant server (collectively, the *verifying device*) would store the application containing the original credential information at least temporarily to allow the data to be transmitted to the token server. EX1005, ¶245.

Thus, the verifying device's memory unit is configured to store information associated with the user's original credential, as recited in element 8.2. *Id.*

Accordingly, Osborne teaches elements 8.1-8.2. EX1005, ¶¶243-45.

3. Elements 8.3-8.10

Elements 8.3-8.10 are almost verbatim copies of elements 1.1-1.8, respectively. The only changes are that elements 8.3-8.10 omit "by the OVER file verifying device" from claim elements (since the preamble and elements 8.1-8.2 specify that the steps are performed by such a device), and element 8.3 recites "the original credential" instead of "an original credential of a user," since the "original credential" was introduced in element 8.2. Neither of these constitute substantive differences relative to the mapping discussed above for claim 1. Accordingly, Osborne teaches elements 8.3-8.10 for similar reasons as those discussed for 1.1-1.8 above. EX1005, ¶246.

Thus, claim 8 was obvious over Osborne. EX1005, ¶¶241-47.

D. Claim 15

Claim 15 recites a "non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to perform operations comprising" a series of steps recited in elements 15.1-15.8. As discussed above for claim 8, Osborne teaches a verifying device (merchant server and point-of-sale terminal) storing instructions in a memory unit to be executed by

a processor to perform the steps of claim 8. *Supra* §IV.C.2. These steps (elements 8.3-8.10) are identical to the steps recited in elements 15.1-15.8, respectively, with the only differences being that element 15.1 recites “an original credential” and “a user,” and it does not expressly recite that the OVER file is a new credential. Thus, claim 15 was obvious over Osborne for similar reasons to claim 8. *See supra* §IV.C; *see also supra* §IV.B (substantively identical elements for claim 1); EX1005, ¶248.

E. Claims 2, 9, and 16

Claims 2, 9, and 16 depend from claim 1, 8, and 15, respectively. Each contains substantively identical limitations. Claims 2 and 9 recite that the “**first** OVER file further comprises a device identifier for the original credential configured to limit the first OVER file, for use in authenticating the user using the information of the original credential, to the **first** OVER file client device.” Claim 15 recites the same limitation, except that it omits two instances of “first” highlighted in bold above. Since claim 15 does not recite an “OVER file” or “OVER file client device” without the terms “first” or “second,” this petition assumes claim 16 was intended to encompass at least an embodiment including the two bolded words “first,” paralleling claims 2 and 9. Osborne teaches these elements. EX1005, ¶249.

For example, Osborne teaches that the token server may keep a device table with various identifiers for a user’s device, such as “device_ID,” “device_name,”

“device_MAC,” (referring to a MAC address) etc. EX1011, ¶148; EX1005, ¶250. Osborne further teaches that “device fingerprinting may be utilized” to provide “additional security” for use of Osborne’s tokens and provides an example token data structure that includes a “client_fingerprint” field with device-identifying information like the client’s MAC address. EX1011, ¶47. Osborne further teaches that the “token may be provided as a data structure...to the client device for later use.” EX1011, ¶48; *see also id.*, ¶26 (fingerprinting may operate using a “client device of a user”). Since the token represents the credential, the device identifier would limit the credential to the client device via its association with the token (for example, the token would not be authenticated if used with a device having a device identifier not associated with the token). *See* EX1011, ¶47 (including credential account numbers and related information along with device fingerprint in token); EX1005, ¶250.

Therefore, to obtain the additional security taught by Osborne, a POSA would have been motivated to include a device identifier in an OVER file (token) sent to a device of the user to employ Osborne’s device fingerprinting to tie a given token to a given device, thus using the device identifier when authenticating the user using the information of the original credential (i.e., when confirming that the authenticity of the token matched to the original credential’s information). This would have added an extra layer of security by ensuring the user’s token was only

being used by someone who also had possession of the user's device (since the device's fingerprint would not match otherwise). EX1005, ¶251.

Accordingly, claims 2, 9, and 16 were obvious over Osborne. EX1005, ¶¶249-52.

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

Claims 3 and 10 depend from claims 1 and 8, respectively, reciting that “the first OVER file further comprises user-specific information.” Claims 4 and 11 depend from claims 3 and 10, respectively, reciting that “wherein the user specific-information comprises at least one of: biometric information, location information, a password, or a device identifier.” Claim 17 depends from claim 15, and recites substantively the same limitations as claims 3-4 and 10-11, namely that “the first OVER file further comprises user-specific information comprising at least one of: biometric information, location information, a password, or a device identifier.” Osborne teaches these elements. EX1005, ¶253.

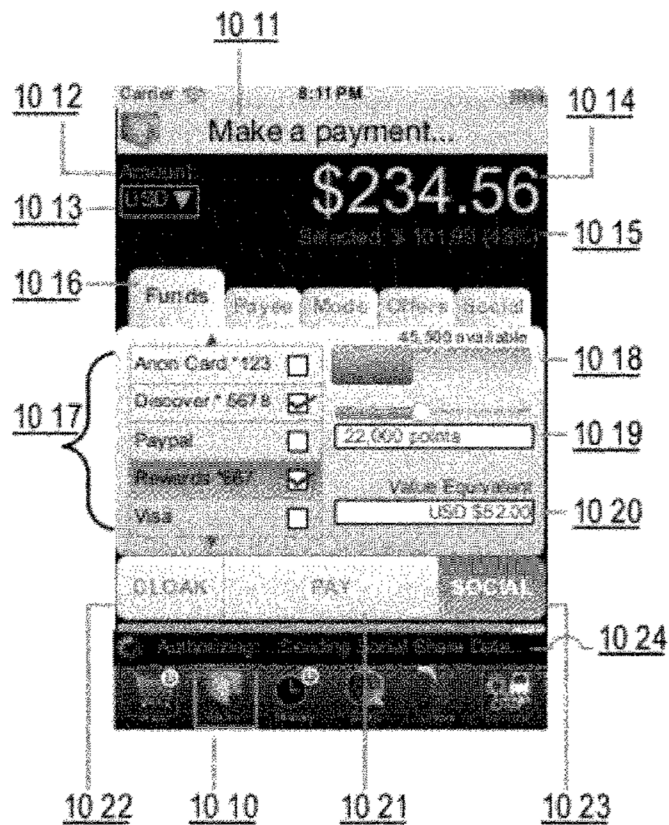
Osborne teaches that its PPT system stores user-specific information in a “Users table,” including, for example, the user's “state, address firstline, address secondline, zipcode,” etc. EX1011, ¶148; *see id.*, Fig. 15, ¶47 (token server stores user's address). These entries include at least location information (e.g., address, zip code, ...) about the user. EX1011, ¶¶148 (also storing “device_ID,” “device_GPS,” “password”), 30 (biometric and/or like recognition); *see also id.*,

¶¶47-48, Fig. 3C (client device displaying user-specific information such as user address disclosed as being stored in token data structure, demonstrating inclusion in OVER file). As discussed above for claims 2, 9, and 16, Osborne teaches or suggests including a device identifier in an OVER file sent to a user's device to facilitate device fingerprinting for additional security. *Supra* §IV.E; *see also* EX1012, ¶¶26, 47-48 (token data structure including device identifier and other user-specific information such as address). Osborne thus renders claims 3-4, 10-11, and 17 obvious. EX1005, ¶¶254-55.

G. Claims 5 and 12

Claims 5 and 12 depend from claims 1 and 8, respectively, reciting that “the first OVER file comprises a portion of the original credential stored by the OVER engine.” Osborne renders these claims obvious. EX1005, ¶256.

Osborne teaches that credential details including account numbers are stored in a token data structure. *See* EX1011, ¶54. Osborne further teaches that the user device may include interface diagrams displaying a portion of a credential, such as a part of an account number. EX1011, ¶85; *see id.*, Fig. 10A (excerpted below).



In view of this disclosure, a POSA would have found it obvious to include a portion of the stored credential (e.g., part of an account number) in the OVER file in order to achieve the disclosed display of portions of credentials. EX1005, ¶¶25758.

Accordingly, claims 5 and 12 were obvious over Osborne. EX1005, ¶¶256-59.

H. Claims 6 and 13

Claims 6 and 13 depend from claims 1 and 8, respectively, reciting that “the first authentication message comprises an indication that the first OVER file is expired.” Osborne teaches these elements. EX1005, ¶260.

For example, Osborne teaches that a user can specify “token attributes” including specifying “activation 227 and expiry 228 dates for the tokens.” EX1011, ¶29. Osborne confirms that a token includes an expiry date, as reflected in the example XML encoding of Osborne’s token data structure. *See* EX1011, ¶47 (“<expiry>2011-02-28 23:59:59</expiry>”). Osborne also teaches that an “authentication fail message” can be sent where the token server determines the user is not authenticated, which may also trigger “an error-handling routine.” EX1011, ¶69. Where the user’s token had expired, the resulting authentication fail message would be an indication that it was expired. EX1005, ¶261. Indeed, it would have been obvious to specifically include a reason for rejection of the token (i.e., due to expiry) as part of the authentication fail message to inform the merchant and user and facilitate the error-handling routine taught by Osborne. EX1005, ¶261; *see id.*, ¶¶206-11 (expiration messages standard for card transactions).

Accordingly, claims 6 and 13 were obvious over Osborne. EX1005, ¶¶260-62.

I. Claims 7 and 14

Claims 7 and 14 depend from claims 1 and 8, respectively. Claim 7 recites that the method further comprises “accessing, by the verifying device, from the first OVER file client device, additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been satisfied.” Claim 14 recites substantively the same limitation, except that it omits claim 7’s reference to “the verifying device.” Osborne teaches these elements. EX1005, ¶263.

Osborne teaches that “additional security may be layered by using authentication methods” in combination with tokens. EX1011, ¶26. This can include use of a “user name and password,” “a digital certificate,” and “device fingerprinting.” *Id.* When implementing the additional types of security measures disclosed by Osborne, it would have been readily apparent to a POSA to do so by *accessing additional credential information from the first OVER file client device by the verifying device indicating whether a secondary condition for authorizing the user has been satisfied.* EX1005, ¶264. In such an implementation, the information (username/password, certificate, or fingerprint) would be accessed from the user’s device by the verifying device, and the secondary condition would be that the provided information matched the corresponding values associated with the token. *Id.*

For example, Osborne teaches that an “authentication chip may be configured to recognize the user's payment token physical card” using digital fingerprinting, with the user “required to present the payment token physical card to the authentication chip disposed in communication with the client before the user can make a purchase order using the token.” EX1011, ¶26. In particular, Osborne explains that “the chip may be embedded into the client, come pre-installed in the client, attached as a periphery to the client, and/or the like.” *Id.* As explained above (*supra* §IV.B.2), Osborne discloses that the client can take the form of various hardware components such as a point-of-sale terminal or kiosk. EX1011, ¶35. Osborne recognizes this use of an authentication chip as a condition for authorization, stating it “provides an authenticity shield preventing others who may know of the user’s payment token from utilizing the user’s payment token in a fraudulent transaction.” EX1011, ¶26. In light of Osborne’s disclosure, it would have been obvious for a *verifying device* to employ additional security measures such as the authentication chip described by Osborne to confirm a device fingerprint of the user’s device providing the token (*OVER file client device*). EX1005, ¶¶265-66.

Accordingly, claims 7 and 14 were obvious over Osborne. EX1005, ¶¶263-67.

V. GROUND 2: CLAIMS 1-17 WERE OBVIOUS OVER OBORNE AND NEAFSEY

As discussed above for Ground 1, Osborne teaches or suggests each element of claims 1-17. For elements 1.3, 1.6-1.7, 8.5, 8.8-8.9, 15.3, and 15.7-15.8, Ground 1 applied a construction of “scan” encompassing NFC interactions. However, an optical scan would also have been obvious, as exemplified by Neafsey. EX1005, ¶268.

In particular, Neafsey teaches various formats of virtual credentials that may be used for conducting transactions. Among these formats are optically scannable codes, such as QR and bar codes, for example. EX1015, ¶61; EX1016, 12; EX1011, ¶32 (QR and barcodes may be scanned with camera). A POSA would have been motivated to incorporate an optically scannable code into an OVER file to be used to trigger the use of tokens to purchase goods, in a manner similar to Osborne’s disclosure of using NFC or mag stripe interactions, as Neafsey teaches that such optically scannable codes would serve similar roles. The combination would thus be a simple substitution of known elements to achieve predictable results. EX1005, ¶269; *see KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416-17 (2007). Doing so would provide greater flexibility to users, increasing convenience and allowing a greater range of mobile devices to be employed. EX1005, ¶269.

A POSA would also have had a reasonable expectation of success in this combination. Indeed, Osborne expressly teaches the use of optical codes such as QR

and bar codes in conjunction with similar transactions. *See* EX1011, ¶¶80 (QR code for money transfer), 93 (payment via “user-obtained QR code” alternative to use of NFC), 104 (“payment via pay code such as barcodes or QR codes”). Thus, a POSA would have expected success in using optically scannable codes to stand in for credentials (e.g., as a scannable part of an OVER file) to trigger a tokenized transaction as taught by Osborne. EX1005, ¶270; *see supra* §I.C.3.

In this combination, scanning an optically-scannable code would replace the use of NFC or mag stripe interactions in Osborne, invoking token use in a similar way. EX1005, ¶271. The remaining claim elements for claims 1-17 would be obvious for the same reasons discussed above for Ground 1. EX1005, ¶271.

Accordingly, claims 1-17 were obvious over Osborne and Neafsey. EX1005, ¶¶268-272.

VI. GROUND 3: CLAIMS 1-17 ARE OBVIOUS OVER STAFFORD, PURVES, AND NEAFSEY

A. Overview and Rationale to Combine

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

In particular, Stafford teaches a system for “validating and disseminating credential information” that meets almost all elements of the independent claims as well as many dependent claim limitations. EX1012, Abstract. Instead of tokens, Stafford’s system uses key signatures (e.g., hash values for encrypted files) to

verify users' identity and provide credential information to a third party. *See* EX1012, Fig. 3, ¶¶107-21; EX1005, ¶¶273-74.

Stafford discloses methods for providing credentials to third parties that parallel the methods in the '854 patent. Stafford's system stores credential information for a user ("entity") in a credential database, provides users key signatures representing those credentials, and allows a third party ("IdBus1") with which the user has shared the key signatures to receive credential verification. *See* EX1012, ¶¶10, 97-102, 108, 115, 118-26, Figs. 2-3; EX1005, ¶275.

Stafford teaches that the key signatures and other information may be provided to a third party "online or in person," and that the "delivery process may vary" based on the information provided and the recipient. EX1012, ¶¶106-13. Stafford thus expressly suggests including other information with its key signatures and employing various known delivery processes. EX1005, ¶276. Such known processes and information would include using an optical scan for delivery, including an image as a virtual representation of a credential in an OVER file, and using device identifiers to make such files unique to a given user device. EX1005, ¶276.

These aspects are taught by Purves and Neafsey. In particular, Purves teaches providing issuer-verified representations of credentials (such as credit card images). *See* EX1013, ¶¶39, 85, 102, 104, 108-12. A POSA would have been

motivated to incorporate such representations with Stafford's key signatures to provide user devices convenient images of the credentials that may be selected by the user. EX1005, ¶277.

Neafsey also teaches that optical codes (which would include the optically-scannable QR and bar codes taught by Purves) may be used to convey virtual credential information. EX1015, ¶¶61, 22 (credential encode strings of bits in different formats); EX1016, 4, 12 (optical code); *see also* EX1013, ¶¶64 (QR code may be used to trigger wallet connection), 95 ("QR code 1508, bar code, or other visual element suitable for scanning by a mobile device"). Neafsey further teaches that clients may have different devices, and that credentials may be provided in different formats appropriate to a particular device. EX1015, ¶61; EX1016, 12. For example, these different credentials may be generated based on a "unique device ID" of the recipient device. EX1015, ¶¶48-49; EX1016, 9-10; EX1005, ¶278.

As Dr. Shamos explains, a POSA would have been motivated in light of these teachings to provide OVER files (such as files comprising the hash codes and credential representation of Stafford and Purves) to client devices in formats appropriate to each client device, e.g., by tying the OVER files to a given device's unique device ID. EX1005, ¶279. In particular, a POSA would have understood different client devices would sometimes require using different formats appropriate to each device, as certain formats could not be used on certain devices.

For example, a first device may be able to display some types of code but not other types of codes, while a second may permit the opposite. EX1005, ¶279; *see* EX1015, ¶61 (multiple different devices and formats possible); EX1016, 12. In such a case, each OVER file would be valid in one user device but invalid for use in the other. EX1005, ¶279.

As discussed in detail below for the independent claims, it would have been obvious to use these features as part of Stafford's credential-distribution system (1) to provide user devices convenient images of the credentials they are showing to third parties and (2) to use the scannable code formats such as QR and bar codes to transfer Stafford's key signatures to the third party by providing device-specific, encoded key signatures to the user. EX1005, ¶280.

A POSA would have been motivated to combine Stafford, Purves, and Neafsey with a reasonable expectation of success to arrive at the claimed invention. All three references are directed to similar applications (electronic use of credentials replacing physical credentials typically carried in physical wallets, such as driver's licenses, credit cards, etc.). EX1005, ¶281. Further, incorporating features such as credential images and device-specific, optically-scannable codes into a credential management system like Stafford's would have been straightforward, as the use of these features would have been familiar to the POSA and their application would have been predictable. *Id.*; *supra* §I.C.3.

A POSA would have recognized various benefits from incorporating Purves's credential images into Stafford's system. For example, the images would improve ease-of-use and reduce user error by providing users images matching the credentials the user seeks to provide to third parties. EX1005, ¶282.

Similarly, a POSA would have viewed the device-specific, optically-scannable codes taught by Neafsey as a convenient way to convey key signatures to third parties in a more efficient and reliable manner than reading or typing a code manually, both of which are slow and error-prone. By adapting Stafford's credential management system to provide optically encoded key signatures, a POSA would reasonably have expected to achieve these benefits for users. EX1005, ¶283; *supra* §I.C.3.

The discussion of claims 1-17 below provides further detail regarding POSAs' rationale to combine Stafford, Purves, and Neafsey to arrive at the claimed invention with a reasonable expectation of success. EX1005, ¶284.

B. Claim 1

Stafford, Purves, and Neafsey teach each element of claim 1, as discussed below. EX1005, ¶¶285-309.

1. Preamble

Stafford, Purves, and Neafsey teach a computer-implemented method. *See, e.g.,* EX1012, ¶54, Fig. 1; EX1013, ¶¶130-46; EX1015, ¶¶17-34, Figs. 1-2; EX1016, 4-8, Figs. 1-2; EX1005, ¶286.

2. Element 1.1

As discussed above in ground 1, element 1.1 involves an *OVER engine* that is configured to generate a *first OVER file* with certain specific characteristics and transmit it to a *first OVER file client device*, from which it is accessed by an *OVER file verifying device*. Stafford, Purves, and Neafsey teach such an arrangement, as described below. EX1005, ¶287.

OVER engine, verifying, and client devices

Stafford teaches a system (*OVER engine*) that stores credential information for proving users' identity or qualifications. EX1012, ¶54 (“FIG. 1 illustrates a system 100 for storing, validating and disseminating credential information about an entity.”), Fig. 1; *see also id.*, claim 1 (“method of compiling a credential database including” receiving and verifying credential information, generating data representations of credential information and document, and storing them in encrypted form).

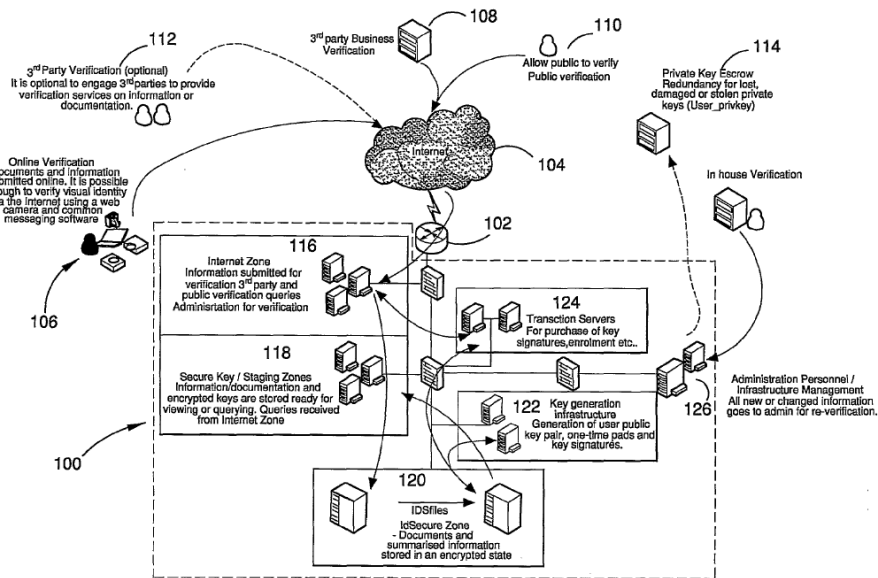


FIGURE 1

Stafford uses the terms “entity” or “IDMember” to refer to the user whose credentials are stored. EX1005, ¶¶288-89. Stafford’s system stores “credential information,” such as “name, address, date of birth, as well other information.” EX1012, ¶¶53-54. This includes memory (a “data store”) hosting a “database of encrypted credential information.” EX1012, ¶57; EX1005, ¶289. Credential information is encrypted and securely stored. EX1012, ¶¶58, 71, 88. Stafford’s example credentials include driver’s licenses, professional memberships, a degree (such as Ph.D.), etc. EX1012, ¶¶4, 65, 131, 139.

Stafford also teaches an entity client terminal (*first OVER file client device*) operated by an entity/IdMember that communicates with Stafford’s system to store credentials, with the entity/IdMember setting the sensitivity of credential information. EX1012, ¶¶54, 81. Sensitive credential information requires use of

“highly secure symmetric or similar encryption process e.g. a one time pad” when being released. EX1012, ¶88; *see id.*, ¶¶73-74, Fig. 2 (showing credential release process); EX1005, ¶290.

Users can request release of sensitive credentials. *See* EX1012, ¶74 (“To release data, in a first example the entity (IdMember) logs on to the website and elects to ‘release’ information using the appropriate interface.”). The request/release process is shown in Fig. 2, reproduced below.

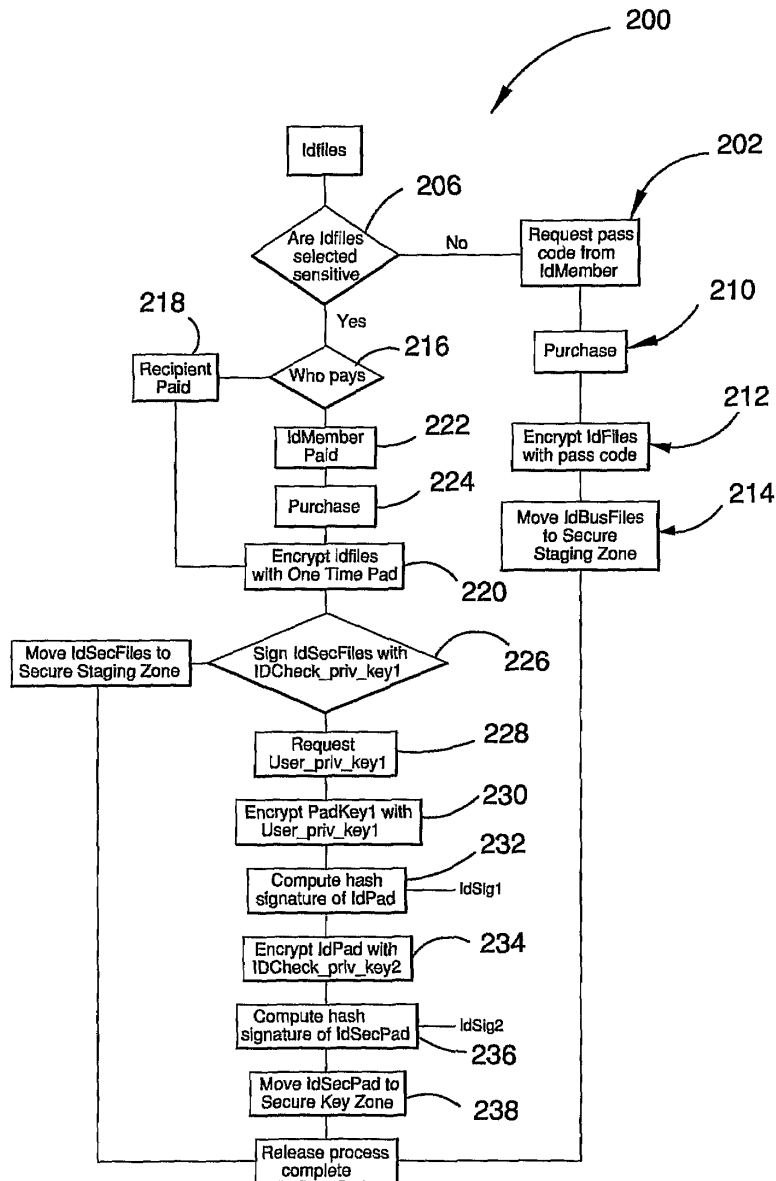


FIGURE 2

EX1012, Fig. 2. As shown, when sensitive files are selected for release, the recipient or IdMember purchases a “key signature” that includes “a hash value or similarly secured...encrypted passwords or one-time pads” that identify and authorize release of encrypted credentials (IdFiles). EX1012, ¶¶75-79; *see id.*,

¶¶38, 88, 93-95; EX1005, ¶291. As discussed below, these key signatures would be provided in an *OVER file*. EX1005, ¶291.

Stafford also teaches an *OVER file verifying device*. As illustrated in Fig. 3, Stafford teaches that a third-party OVER file verifying device (referred to as IdBus1, *see* EX1012, ¶108) sends a request for release of information to the credential-database system. EX1012, ¶115; Fig. 3 (marked-up below).

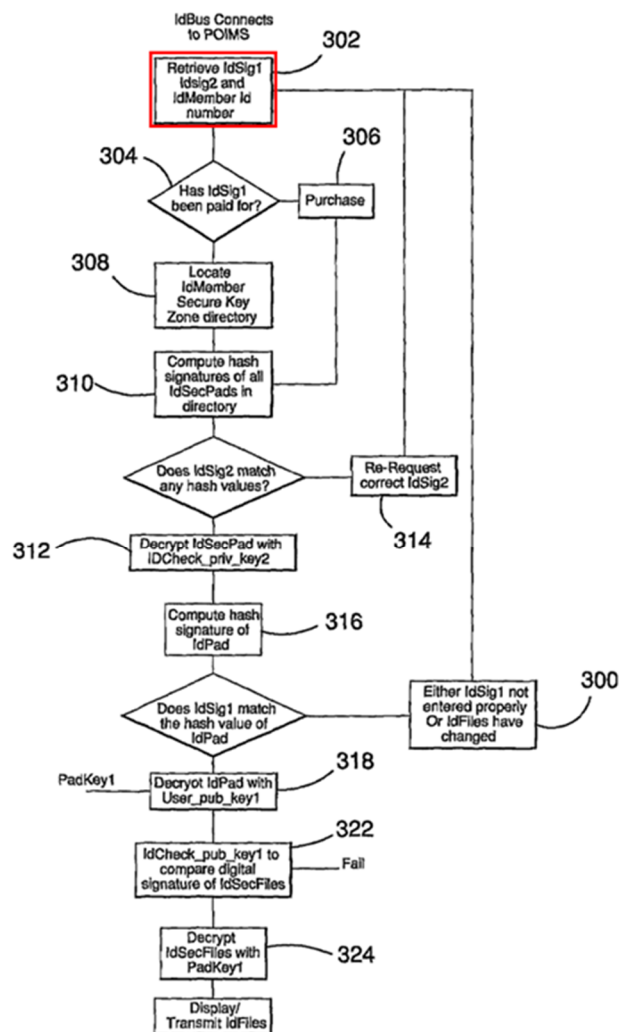


FIGURE 3

The request includes the key signatures that are used to verify that an *OVER file* (encoding the signatures, as discussed below) authenticates the user, as only if the key signatures match the hash values of the encrypted credential file are the credential files transmitted. *See* EX1012, ¶¶119-22; EX1005, ¶292.

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

Stafford's system generates key signatures to release sensitive files. *Supra* §VI.B.2. These signatures can comprise hash values (IdSig1 and IdSig2), which can either be displayed to the user or transmitted electronically to the user's device. EX1012, ¶¶97-99. The credential to be released is stored in an encrypted format using one-time pads (IdSecPad and IdPad), and IdSig1 and IdSig2 are hash values of the credential's one-time pads, thereby identifying the encrypted credential. EX1012, ¶¶116-22. The release of the credential is authorized by comparing the hash values to the IdSecPad and IdPad corresponding to the credential, with a match indicating that release is authorized. *Id.*; EX1005, ¶293. A hash value thus acts as a virtual credential representation of the stored credential, 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, ¶293.

Stafford teaches that its encrypted credentials may be verified by the issuer and may include storing an image of the credential (e.g., a scanned copy). EX1012, ¶¶62, 65, 67. However, to the extent that Stafford does not expressly teach that the key signature files sent to the user include a virtual representation *verified by the issuing agency*, this aspect of the claim is met by Purves. EX1005, ¶294.

Purves teaches that a user device (e.g., a device implementing a digital wallet) may be sent an image of a credential such as a credit card to conveniently represent a real credential. EX1013, ¶¶102, 108-09. The card image may be “from an issuer.” EX1013, ¶85. The server may also generate an image of the credential, optionally with “confidential information...obscured.” EX1013, ¶122; *see also id.*, ¶¶111-12 (“multiple versions of the card” may be used in various formats). A representative image provided “from an issuer” would be *verified by the issuing agency to be an official representation*, as would an image produced from an actual credential, since an actual credential naturally represents itself. EX1005, ¶295.

In light of Purves’s teaching to provide user devices with images representing a credential, it would have been obvious to use similar images in the context of Stafford. For example, the system would provide an image of the user’s credential (e.g., a generally-representative, issuer-provided image or a real image of the credential with optionally-obscured confidential information) along with the

encoded key signature to remind users which credential the key signature represents and enable quick selection from among a plurality of options available on the user's device. *See* EX1013, ¶¶85, 122; EX1005, ¶296. Such an image would be a virtual representation verified by the issuer as being an official representation of the credential. EX1005, ¶296.

accessing the OVER file

Stafford teaches that the key signatures and other information may be provided to a *verifying device* (IdBus1) “online or in person,” and that the “delivery process may vary” based on the information provided and the recipient. EX1012, ¶¶106-13. Stafford thus expressly suggests including other information with its key signatures and employing various known delivery processes. EX1005, ¶297. Such known processes and information would include using an optical scan in the delivery process, as taught by Neafsey, in addition to the virtual representation of a credential taught by Purves, as discussed above. In particular, Neafsey teaches that credentials may be provided in varying formats specific to user devices, including by keying formats to unique device IDs. EX1015, ¶¶48-49, 61; EX1016, 9-10, 12. Such formats include optically-scannable formats, such as QR and bar codes. EX1015, ¶61; EX1016, 12; EX1012, ¶95. As discussed above in §VI.A, it would have been obvious to use such optically-scannable codes to encode Stafford's key signatures, allowing them to be transferred to the recipient

(IdBus1) in a simple, reliable manner. EX1005, ¶297. Such a scan of the OVER file would provide the *accessing* of the *OVER file* by the *OVER file verifying device* recited in element 1.1. *Id.*

Stafford, Purves, and Neafsey thus teach or suggest each limitation of element 1.1. EX1005, ¶¶287-98.

3. Element 1.2

Stafford, Purves, and Neafsey teach element 1.2. As illustrated in Fig. 3, Stafford teaches that a third-party client verifying device (referred to as IdBus1, *see* EX1012, ¶108) sends a request for release of information to the credential-database system. EX1012, ¶115; Fig. 3 (marked-up below).

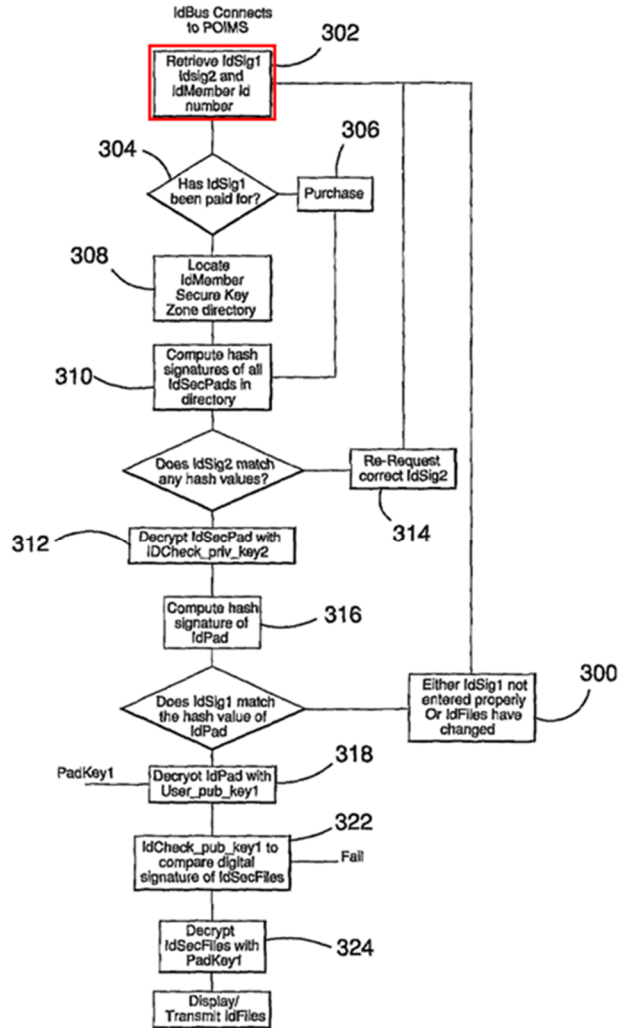


FIGURE 3

The request includes the key signatures IdSig1 and IdSig2, which are used to verify that the OVER file (encoding the signatures) authenticates the user, as only if the key signatures match the hash values of the encrypted credential file are the credential files transmitted. *See* EX1012, ¶119-22; EX1005, ¶299.

As discussed above in §VI.A, it would have been obvious to provide the key signatures encoded as an optically scannable code in light of the teachings of Neafsey and Purves. *See* EX1015, ¶65; EX1016, 12; EX1013, ¶64; EX1005, ¶301.

Doing so would allow the user to more easily transmit the key signature to a third party using an optical scan. EX1005, ¶301; *see supra* §VI.A. The optical encoding would be scanned by the third-party device to provide the key signatures used in step 302 of Stafford's Fig. 3. The scanning of this code by the OVER file verifying device corresponds to the recited accessing of the OVER file. Stafford, Purves, and Neafsey thus teach element 1.2. EX1005, ¶301.

4. Element 1.3

Stafford in view of Purves and Neafsey teaches this element. Stafford's system responds to the request discussed for element 1.2 (and thus the associated scan of the code taught by Neafsey) by comparing the encoded hash values IdSig1 and IdSig2 of the key signature. EX1012, ¶115-21, Fig. 3 (marked up below).

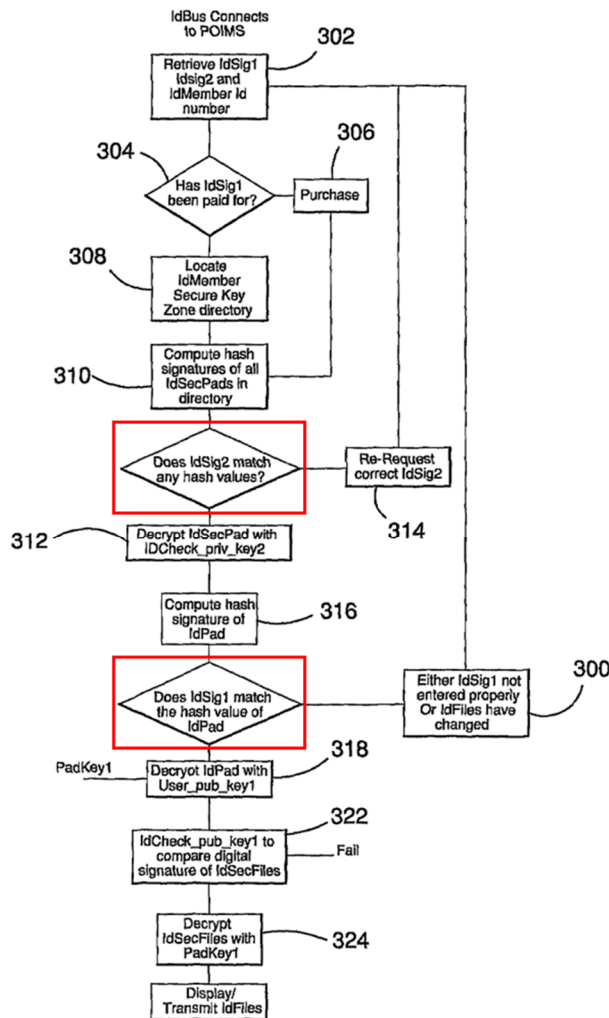


FIGURE 3

This comparison verifies that the scan (which provides the key signatures) corresponds with the information associated with the credential (since it matches the encrypted credential's hash values). See EX1012, ¶¶93 (IdFiles (credentials) encrypted with one-time pad) 115-22 (hash values match credential's one-time pad); EX1005, ¶¶302-03.

Stafford teaches that an authenticating message is received by the third-party device with a first indication of whether the scan corresponds to the first OVER

file. For example, where either key signature fails to match, an appropriate message is sent to re-request the non-matching hash value. EX1012, ¶¶120-22. Fig. 3 (marked-up below). On the other hand, where the key signatures match, a decrypted copy of the IdFiles is transmitted to the third-party device. EX1012, ¶¶120-26. These alternatives, indicated in Fig. 3 (marked-up below) both correspond to the recited authentication message, since a re-request message indicates a lack of correspondence and the sending of the IdFiles indicates a successful correspondence between the credential information and the recited scan. EX1005, ¶304; EX1012, Fig. 3.

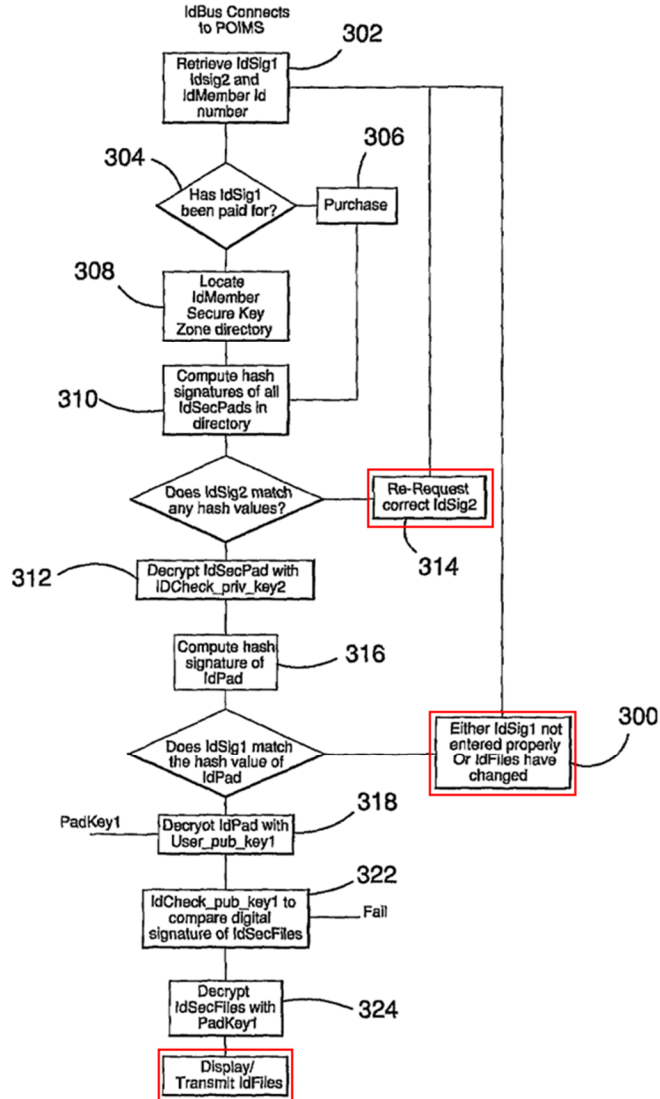


FIGURE 3

Stafford, Purves, and Neafsey thus teach element 1.3. EX1005, ¶¶302-04.

5. Element 1.4

Stafford in view of Purves and Neafsey teaches *outputting a first status indicator expressing whether the first OVER file authenticates the user*, as recited in element 1.4. For example, when “IdSig does not match the hash value... request

for re-entry of IdSig1 is made and the process retried.” EX1012, ¶122. This request for re-entry is an indicator expressing that the first OVER file did *not* authenticate the user. EX1005, ¶305. On the other hand, where the key signatures match, “decrypted and released IdFiles can then be transmitted or displayed to IdBus1 for use in the necessary data comparison and credential verification,” which is an indicator that the OVER file authenticates the user. EX1012, ¶126; EX1005, ¶¶203-05, 305.

Stafford, Purves, and Neafsey thus teach element 1.4.

6. Elements 1.5-1.8

As discussed above for ground 1, elements 1.5-1.8 repeat elements 1.1-1.4 as applicable to a second OVER file that is a second credential on a second client device scanned by the OVER file verifying device, with the second OVER file being invalid for use on the first client device. *Supra* §IV.B.6. These elements would have been obvious over Stafford, Purves, and Neafsey. EX1005, ¶306.

As discussed in §VI.A, it would have been obvious to provide a second OVER file comprising a second encoded key signature to a second device of the user, as Neafsey teaches that different devices may receive different virtual credentials in different formats corresponding to the particular device. *See* EX1015, ¶61; EX1016, 12; EX1005, ¶307; *Harza*, 274 F.2d at 671. As Neafsey teaches, each such virtual credential would be generated using the “unique device

ID” of the recipient device, meaning that each credential would be limited to being used on a particular device matching the device ID. EX1015, ¶¶48-49; EX1016, 10-11; EX1005, ¶307. As Dr. Shamos explains, a POSA would have understood different client devices would sometimes require using different formats appropriate to each device—for example, a first device and second device may each support credential formats that the other does not support. EX1005, ¶¶297, 307. In such a case, by limiting each type of format to a particular device according to the device ID, the encoded key signatures of a first device would be invalid for use on a second device, and the encoded key signatures of the second device would be invalid for use on the first device. EX1005, ¶307.

In such a combination, the *second OVER file* (second encoded key signature) would be present on and accessed and *scanned at the second OVER file client device* by the recipient’s verifying device, and it would constitute a *second new credential* that is *invalid for use in the first OVER file client device for authenticating the user*. EX1005, ¶¶308-09. The remaining aspects of elements 1.5-1.8 would have been obvious for the same reasons as elements 1.1-1.4. *Id.* Thus, Stafford, Purves, and Neafsey teach elements 1.5-1.8.

Accordingly, claim 1 was obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶274-309.

C. Claim 8

Claim 8 is directed to an OVER file verifying device rather than a computer-implemented method, but it includes limitations virtually identical to claim 1, and would have been obvious over the prior art for similar reasons, as discussed below. EX1005, ¶310.

1. Preamble

As discussed for claim 1, Stafford, Purves, and Neafsey teach an OVER file verifying device (Stafford's IdBus1 configured as taught by Stafford, Purves, and Neafsey). *See supra* §VI.B.2; EX1005, ¶311.

2. Elements 8.1-8.2

Stafford, Purves, and Neafsey teach the processor and memory recited in elements 8.1-8.2. EX1005, ¶312.

Stafford discloses a computer-implemented “system 100 for storing, validating and disseminating credential information about an entity,” which may be connected “to a computer network such as the Internet.” EX1012, ¶54; *see id.*, Fig. 1 (depicting system 100 as a system comprising computers). Thus, Stafford discloses a computer apparatus that stores credential information. EX1005, ¶313. A POSA would have understood that such a system would include a processor coupled to a memory unit storing instructions and the user's credential information. *Id.*

Stafford further describes that the recipient (IdBus1) is a computer-based device that would include the recited processor and memory. For example, Stafford repeatedly refers to the systems of IdBus1 interfacing with the credential system and other computer components, including allowing “IdBus1 systems to interface with the system 100 i.e. a common interface” and placing data “into a format parseable by IdBus1’s systems (e.g. XML).” EX1012, ¶¶110-12; *see also id.*, ¶128 (IdBus1 computes and compares hash values). A POSA would have understood that such a device would be a computing device comprising a processor and memory storing instructions and other data. EX1005, ¶314. Among this stored data would be *information associated with an original credential of a user*—for example, IdBus1 not only receives the key signatures (which are directly associated with the original credential) but also receives “decrypted and released IdFiles” (i.e., copies of the original credential images stored by Stafford’s system). *Id.*; EX1012, ¶¶115, 126.

Purves confirms that such a computer system would include a processor and memory. For example, Purves teaches that “computers employ processors to process information,” which “may be referred to as central processing units (CPU),” and which operate on “instructions and data in various processor accessible and operable areas of memory.” EX1013, ¶127; *see also id.*, ¶132 (CPU “execute[s] stored instructions (i.e., program code) according to conventional data

processing techniques”). Purves details components present in typical computer systems, including CPUs and memory to store information and instructions.

EX1013, ¶¶131-49; *see also* EX1015, ¶¶30-34 (similar components for virtual credential-receiving device); EX1016, 6-8; EX1005, ¶315.

Thus, Stafford, Purves, and Neafsey teach elements 8.1-8.2.

3. Elements 8.3-8.10

Elements 8.3-8.10 are almost verbatim copies of elements 1.1-1.8, respectively, with no substantive differences relative to the mapping discussed above for claim 1. *See supra* §§IV.C.3, VI.B.2-6. Accordingly, Stafford, Purves, and Neafsey teach elements 8.3-8.10 for similar reasons as those discussed for 1.1-1.8 above. EX1005, ¶316.

Thus, claim 8 was obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶310-17.

D. Claim 15

Claim 15 recites a “non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to perform operations comprising” a series of steps recited in elements 15.1-15.8. As discussed above for claim 8, Stafford, Purves, and Neafsey teach a verifying device (merchant server and point-of-sale terminal) storing instructions in a memory unit to be executed by a processor to perform the steps of claim 8. *Supra* §VI.C. These

steps (elements 8.3-8.10) are identical to the steps recited in elements 15.1-15.8, respectively, with the only differences being that element 15.1 recites “an original credential” and “a user,” and it does not expressly recite that the OVER file is a new credential. Thus, claim 15 was obvious over Stafford, Purves, and Neafsey for similar reasons to claim 8. *See supra* §VI.C; *see also supra* §VI.B (substantively identical elements for claim 1); EX1005, ¶318.

Accordingly, claim 15 was obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶318-19.

E. Claims 2, 9, and 16

As discussed in ground 1, claims 2, 9, and 16 are materially identical, requiring only the use of device identifiers for use in authenticating the user. Stafford, Purves, and Neafsey render these claims obvious. EX1005, ¶320.

As discussed above for claim 1, Neafsey teaches generating different credentials for different devices based on a “unique device ID” of the recipient device. EX1015, ¶¶49, 61; EX1016, 9, 12. A POSA would have used such device IDs to tie encodings of Stafford’s key signatures to a given device by including such device IDs in a first OVER file containing Stafford’s encoded key signatures, to ensure that each device received an appropriately encoded key signature. EX1005, ¶321. Doing so would limit a given encoded key signature to a given device, and in particular would limit the first OVER file to the first device. *Id.*

Moreover, this step would be performed *for use in authenticating the user using the information of the original credential*, since the purpose of Stafford's key signatures is to authenticate the user by matching the information of the original credential (via the hashes of the one-time pads used to encrypt it), which would be furthered by the use of device IDs to ensure the encoded key signatures were used by the devices configured to display them appropriately. *Id.*

Accordingly, claims 2, 9 and 16 were obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶320-22.

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

Stafford teaches storing user-specific information, including the specific categories listed in claim 3-4, 10-11, and 17. For example, associated with its stored credentials, Stafford stores location information (addresses) as well as encrypting a private key that is stored “using a biometric such as a fingerprint or password.” EX1012, ¶53, 71. Further, as discussed above for claims 2, 9, and 16, it would have been obvious to include a device identifier in Stafford's OVER file to limit encoded key signatures to appropriate devices. *See supra* §VI.E; EX1005, ¶323.

Accordingly, claims 3-4, 10-11, and 17 were obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶323-24.

G. Claims 5 and 12

Stafford teaches storing scans of a credential. EX1012, ¶¶62, 67; *supra* §VI.B.2. And as discussed for claim 1, it would have been obvious in view of Purves to include an image of a portion of a stored credential in an OVER file. *Supra* §IV.A; EX1013, ¶122 (credential image with confidential information obscured).

Accordingly, claims 5 and 12 were obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶325-26.

H. Claims 6 and 13

Stafford teaches that certain information “has a validity date associated” and “remains current only for a pre-determined set of time before it requires revalidation.” EX1012, ¶135. It would have been obvious to a POSA to send an *authentication message comprising an indication that the OVER file was expired*, either because the credential itself had expired or because elements of the OVER file (e.g., the key signatures) had expired. EX1005, ¶327.

For example, Stafford contemplates a credential including a driver’s license, which POSAs would have known would generally include an expiration date; for such a credential, an issuer would respond that the credential was not valid if it had expired. EX1012, ¶4; *see id.*, ¶135 (“Certain IdMember information remains current only for a pre-determined set of time...”); EX1005, ¶328. In such a case, it

would have been obvious to receive a corresponding status indication (such as “not verified,” “expired,” etc.) from the issuer and send it to the recipient of the credential. EX1005, ¶328.

Stafford further teaches that the key signatures themselves may expire. For example, Stafford teaches that an IdSig may not match the hash value of an IdPad if the “IdPad has changed since the hash key signature was created.” EX1012, ¶122. This would be an example of Stafford’s key signature expiring due to passage of time. EX1005, ¶329. As a further example, Stafford teaches that the key signatures may be limited by a “set amount of attempts” before becoming invalid. *Id.* Where the keys do not match despite a re-attempt, the transmission of data is aborted. *Id.* It would have been obvious to a POSA, considering this discussion of Stafford, that it would have been advantageous to send an authentication message to the third-party verification device that the key signatures of the *OVER file* had expired. EX1005, ¶329.

Accordingly, claims 6 and 13 were obvious over Stafford, Purves, and Neafsey. EX1005, ¶327-30.

I. Claims 7 and 14

Stafford teaches *accessing, by the verifying device, from the first OVER file client device, additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been*

satisfied. For example, Stafford teaches that the *first OVER file client device* (IdMember's device) may provide the *verifying device* (IdBus1) with a "member identification number" (MIN) in addition to the key signatures. EX1012, ¶¶52, 108-13. This MIN is sent with the key signatures by IdBus1 to the system, which uses the MIN (1) to confirm that payment for data release was received, and (2) to locate the user's credential information for release. EX1012, ¶¶115-16, 118. Each of these is a secondary condition for authorizing the user. EX1005, ¶331. Thus, the MIN is *additional credential information associated with the first OVER file indicating whether a secondary condition for authorizing the user has been satisfied*. *Id.*

Accordingly, claims 7 and 14 were obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶331-32.

VII. DISCRETIONARY DENIAL IS NOT WARRANTED

This petition does not implicate the Board's discretion according to *Fintiv*. *Apple Inc., v. Fintiv, Inc.*, IPR2020-00019, Paper 11. *See generally* Memorandum on Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (*Fintiv* Memo). Patent Owner filed its district court complaint in the Western District of Texas on January 26, 2023, asserting four patents including the '854 patent. The court granted a motion to transfer the case to the Northern District of California on November 3,

2023, and the case was transferred on November 7, 2023. As of the filing of this petition, a trial date has not been set but is reasonably expected to be after issuance of a final written decision here. *See* EX1045; EX1046, 66 (37 month average time to trial in N.D.Cal.).

This petition also does not implicate §325(d). The petition presents new art and argument, as none of the asserted references was disclosed or considered during examination, nor are the references relied on in the petition cumulative to the references applied during examination. *Supra* §I.B. *See generally* EX1008. Indeed, the discussion in the grounds above explains in detail why the claims of the '854 patent were obvious over the prior art, confirming that their allowance constituted material error.

VIII. GROUNDS FOR STANDING

Visa certifies that, under 37 C.F.R. §42.104(a), the '854 patent is available for *inter partes* review, and Visa is not barred or estopped from requesting *inter partes* review of the '854 patent on the grounds identified.

IX. CONCLUSION

For the reasons set forth above, claims 1-17 of the '854 patent are unpatentable. Visa therefore requests that an *inter partes* review of these claims be instituted.

Respectfully submitted,

Dated: January 26, 2024

/Matthew A. Argenti/
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836

X. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

Real Party-in-Interest (37 C.F.R. §42.8(b)(1)): Visa Inc. is the real party-in-interest.

Related Matters (37 C.F.R. §42.8(b)(2)): Patent Owner has asserted the '854 patent against Petitioner in a case originally filed in the United States District Court in the Western District of Texas (6-23-cv-00048), which was transferred and is currently pending in the United States District Court in the Northern District of California (5-23-cv-05720). Concurrently, Petitioner is filing petitions against three related patents: U.S. Patent No. 9,251,531 (IPR2024-00486 and IPR2024-00487); U.S. Patent No. 10,749,859 (IPR2024-00489); and U.S. Patent No. 11,329,973 (IPR2024-00490).

Lead and Back-Up Counsel (37 C.F.R. §42.8(b)(3)):

Lead Counsel: Matthew A. Argenti (Reg. No. 61,836)

Back-Up Counsel: Michael T. Rosato (Reg. No. 52,182); Patrick M. Medley (Reg. No. 74,735); Joseph M. Baillargeon (Reg. No. 79,685)

Service Information – 37 C.F.R. §42.8(b)(4). Petitioner hereby consents to electronic service.

Email: margenti@wsgr.com; mrosato@wsgr.com; pmedley@wsgr.com; jbaillargeon@wsgr.com.

Post: Wilson Sonsini Goodrich & Rosati, 650 Page Mill Rd., Palo Alto, CA
94304

Tel.: 650-354-4154

Fax: 650-493-6811

XI. PAYMENT OF FEES UNDER 37 C.F.R. §§42.15(A) AND 42.103

The required fees are submitted herewith. If any additional fees are due at any time during this proceeding, the Office is authorized to charge such fees to Deposit Account No. 23-2415.

XII. CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. §42.24(d), the undersigned certifies that this Petition complies with the type-volume limitation of 37 C.F.R. §42.24(a). The word count application of the word processing program used to prepare this Petition indicates that the Petition contains 13,365 words, excluding the parts of the brief exempted by 37 C.F.R. §42.24(a).

Respectfully submitted,

Dated: January 26, 2024

/Matthew A. Argenti/
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836

XIII. APPENDIX – LIST OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 9,251,531 to Shaunt M. Sarkissian
1002	U.S. Patent No. 9,954,854 to Shaunt M. Sarkissian
1003	U.S. Patent No. 10,749,859 to Shaunt M. Sarkissian
1004	U.S. Patent No. 11,329,973 to Shaunt M. Sarkissian
1005	Declaration of Michael I. Shamos, Ph.D., J.D.
1006	Curriculum vitae of Michael I. Shamos
1007	U.S. Patent Application No. 13/794,878 File History
1008	U.S. Patent Application No. 14/982,981 File History
1009	U.S. Patent Application No. 16/422,715 File History
1010	U.S. Patent Application No. 16/893,023 File History
1011	U.S. Patent Pub. No. 2012/0316992 to Timothy W. Osborne (“Osborne”)
1012	U.S. Patent Pub. No. 2009/0271321 to Grant Stafford (“Stafford”)
1013	U.S. Patent Pub. No. 2013/0054454 to Thomas Purves et al. (“Purves”)
1014	U.S. Patent Pub. No. 2012/0310838 to Theodore Harris et al. (“Harris”)
1015	U.S. Patent Pub. No. 2013/0212248 to Jeffrey Scott Neafsey et al. (“Neafsey”)
1016	U.S. Provisional Patent Application No. 61/598,219 (“Neafsey Provisional”)
1017	U.S. Patent Publication No. 2008/0270166 to Duane Morin et al. (“Morin”)

1018	First Amended Complaint (Dkt. No. 25) <i>Cortex MCP, Inc. v. Visa, Inc.</i> , No. 5-23-cv-05720 (N.D. Cal.), <i>as filed in</i> No. 6-23-cv-00048 (W.D. Tex) (Apr. 10, 2023) (“Complaint”)
1019	Steiner et al., “Kerberos: An Authentication Service for Open Network Systems.” <i>Usenix Winter</i> (1988) (“Steiner”)
1020	Cross River, “Tokenization in Card Networks” (May 2023) (“Cross River”)
1021	U.S. Patent No. 7,014,107 to Irek Singer et al. (“Singer”)
1022	Heather Mark. “Shift4: Secure Payment Processing” (2006) (“Shift4”)
1023	Tom Arnold. “Credit Card Information Surrogate: A Method and System for using surrogates to integrate PCI-level security for legacy information systems.” (2007) (“Arnold”)
1024	Brown et al. “Microsoft Code Name ‘Geneva’ Framework Whitepaper for Developers” (2008) (“Brown”)
1025	Thakar et al. <i>PCI Compliance for Dummies</i> (2009) (“Thakar”)
1026	Ben Jackson. “Token Gestures.” <i>Digital Transactions</i> (2009) (“Jackson”)
1027	First Data. “Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance.” (2009) (“First Data 2009”)
1028	U.S. Patent Pub. No. 2009/0249082 to Ulf Mattson (“Mattson”)
1029	U.S. Patent Pub. No. 2010/0070754 to Nathan P. Leach (“Leach”)
1030	Propay Press Release. “ProPay Adds Automated Clearing House (ACH) Data Encryption And Tokenization To Its Suite Of ProtectPay Services.” (May 10, 2010) (“Propay”)
1031	Richard J. Sullivan. “The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy.” (2010) (“Sullivan”)

1032	CyberSource. “CyberSource Electronic Check Services Implementation Guide” (2010) (“CyberSource”)
1033	Visa. “Visa Best Practices for Tokenization Version 1.0.” (2010) (“Visa Best Practices”)
1034	U.S. Patent No. 8,458,487 to Gary Palgon et al. (“Palgon”)
1035	PCI Security Standards Council. “PCI DSS Tokenization Guidelines.” (2011) (“Tokenization Guidelines”)
1036	U.S. Patent Pub. No. 2011/0258122 to Daniel Jeffrey Shader et al. (“Shader”)
1037	U.S. Patent Pub. No. 2011/0320316 to Joseph R. Randazza et al. (“Randazza”)
1038	Tim Horton et al. “A Primer on Payment Security Technologies: Encryption and Tokenization.” (2011) (“First Data 2011”)
1039	U.S. Patent Pub. No. 2012/0016731 to Randy Smith et al. (“Smith”)
1040	U.S. Patent Pub. No. 2012/0150669 to Garrett S. Langley et al. (“Langley”)
1041	Guenther Starnberger et al. “QR-TAN: Secure Mobile Transaction Authentication.” <i>2009 International Conference on Availability, Reliability and Security</i> . IEEE. (2009) (“Starnberger”)
1042	U.S. Patent Pub. No. US 2011/0251892 to Kevin Laracey (“Laracey”)
1043	U.S. Patent Pub. No. 2012/0209749 to Ayman Hammad et al. (“Hammad”)
1044	U.S. Patent Pub. No. 2009/0113543 to Neil P. Adams et al. (“Adams”)
1045	Patent Scheduling Order (Dkt. No. 73) <i>Cortex MCP, Inc. v. Visa, Inc.</i> , No. 5-23-cv-05720 (N.D. Cal.) (Jan. 3, 2024) (“Scheduling Order”)
1046	United States District Courts — National Judicial Caseload Profile, https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf (March 2023)

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6(e) and 42.105(a), this is to certify that I caused to be served a true and correct copy of the foregoing Petition for Inter Partes Review of U.S. Patent No. 9,954,854 (and accompanying Exhibits 1001-1046) by overnight courier (Federal Express or UPS), on this 26th day of January, 2024, on the Patent Owner at the correspondence address of the Patent Owner as follows:

K&L Gates LLP-Pittsburgh
210 Sixth Avenue
Pittsburgh, PA 15222-2613

Dated: January 26, 2024

/Matthew A. Argenti/
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836