

Petitioner's Demonstratives

Visa, Inc. v. Cortex MCP, Inc.

IPR2024-00486, IPR2024-00488,
IPR2024-00489, & IPR2024-00490

U.S. Patent Nos. 9,251,531; 9,954,854; 10,749,859;
& 11,329,973

Instituted Grounds

'531 Patent:

Claims	35 U.S.C. §	Prior Art
1-2, 4-14, 21, 27	103	Oborne
3, 22-26, 28-33	103	Oborne & Purves
1-2, 4-18, 20, 21-27	103	Oborne & Neafsey
3, 19, 22-26, 28-33	103	Oborne, Purves & Neafsey
1, 3-5, 7-16, 18-20, 21-26, 28-33	103	Stafford & Purves
2, 6, 17, 27	103	Stafford, Purves & Neafsey

Instituted Grounds
'854 Patent:

Claims	35 U.S.C. §	Prior Art
1-17	103	Oborne
1-17	103	Oborne & Neafsey
1-17	103	Stafford, Purves & Neafsey

Instituted Grounds
'859 Patent:

Claims	35 U.S.C. §	Prior Art
1-2, 4-10, 13-14, 16-21	103	Oborne
3, 11-12, 15	103	Oborne & Purves
1, 3-4, 6-9, 11-12, 14-17	103	Stafford & Purves
2, 5, 10, 13, 18-21	103	Stafford, Purves & Neafsey

Instituted Grounds
'973 Patent:

Claims	35 U.S.C. §	Prior Art
1-2, 4-7, 16-17	103	Oborne
3, 8-15	103	Oborne & Purves
1, 3, 5-8, 10, 12-15	103	Stafford & Purves
2, 4, 9, 11, 16-17	103	Stafford, Purves & Neafsey

The Common Specification

(54) FILE FORMAT AND PLATFORM FOR STORAGE AND VERIFICATION OF CREDENTIALS

(57) ABSTRACT

In various embodiments, a computer-implemented method for generating and verifying **officially verifiable electronic representations** may be disclosed. The method may comprise receiving, by a credential database, a request for a credential action. The credential database may be configured to store one or more credentials comprising a status indicator. The method may further comprise determining, by the credential database, a response to the credential action based on the one or more user credentials stored in the credential database and transmitting, by the credential database, the response to a client device.

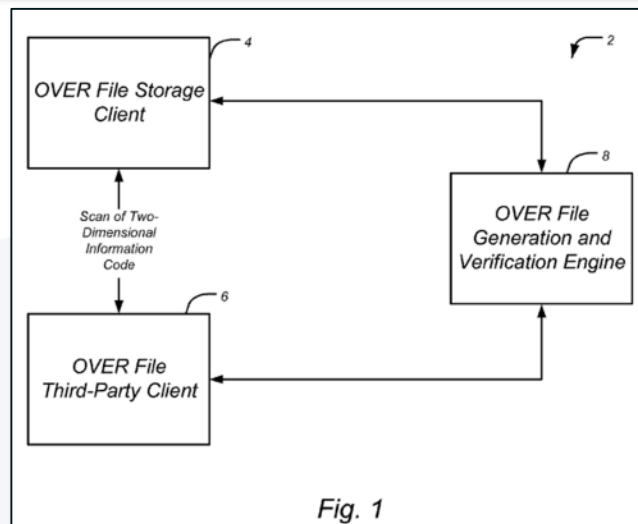


Fig. 1

In some embodiments, an **Officially Verifiable Electronic Representation (OVER) File** may provide a secure file format and platform for the storage and verification of key user or consumer credentials. As shown in FIG. 1, in one embodiment, an OVER File management platform 2 may comprise three main components, an OVER File storage client 4, an OVER File third party client 6, and an OVER File generation and authorization engine 8. The OVER File storage client 4 may be executed by a user device to store generated OVER Files representative of the user's credentials. The OVER File storage client 4 may be included as part of a virtual wallet platform or may comprise a stand-alone user application. The OVER File storage client 4 may initiate generation of new OVER Files and may comprise a display function for displaying stored user credentials for third-party verification. The **OVER File credentials** may comprise any **officially verifiable electronic credential**, such as, for example, a government issued identification such as a driver's license, non-driver's

EX1001, Abstract, Fig. 1, 3:50-67

'531 Patent Claim 1

1. A computer-implemented method comprising:

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

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

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

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

[1.5] receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file store client device of the user;

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

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

EX1001, claim 1

Claim Construction

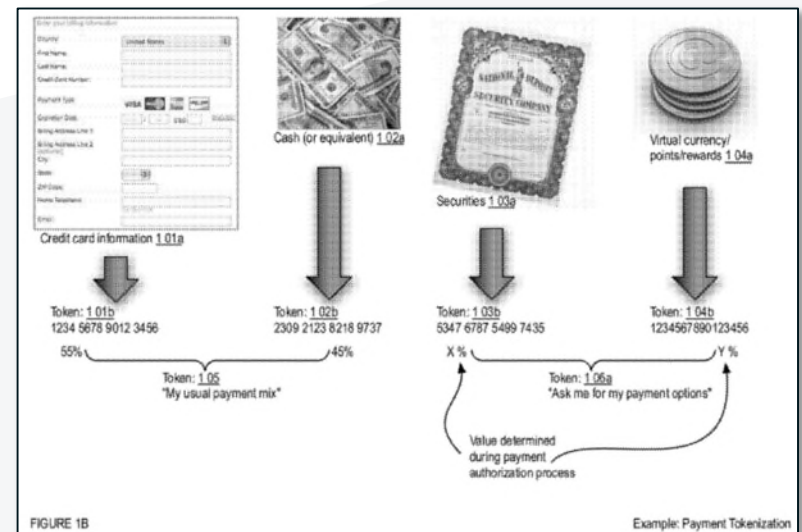
Term	Petition	PO response
OVER File [all patents]	“encompassing a file comprising an image of (or associated with) the credential ... [or] a file comprising a token”	No dispute
Scan [’531 and ’854 patents]	“encompasses an optical scan... [or] an NFC interaction”	No dispute
“...verified by an issuing agency...” [all patents]	“an issuing agency ha[s] verified a virtual representation in an OVER file as being an official representation of a credential”	No dispute

(54) **PAYMENT PRIVACY TOKENIZATION APPARATUSES, METHODS AND SYSTEMS**

ABSTRACT

[0048] The token server may also determine a set of privacy rules, restrictions, transaction processing rules (e.g., in which country should the servers involved in transaction processing reside), etc. applicable to the token created for the user. The token server may store the token data structure to a token database, and the privacy rules/restrictions/settings to a privacy rules database, e.g., **516**. The token server may also provide a token identifier, e.g., **517** to the client. The token may be provided as a data structure via HTTP(S) POST, as a file (via file transport protocols), as an attachment (e.g., via email), and/or otherwise provided to the client device for later use. The client may store the token identifier and/or display the token identifier for the user, e.g., **518**.

In some implementations, each token may be pre-funded. For example, the source of the token (e.g., issuer, acquirer, independent token arbitrator) may first obtain assurance that funds have been uniquely and exclusively allocated for the token from the source to which the token points. Thus, in some implementations, the token may be pre-funded and pre-authorized for up to (or in the alternative, for exactly) a predefined amount of a purchase transaction. For example, the token server may generate a token data structure similar to the example XML-encoded data structure below:



9

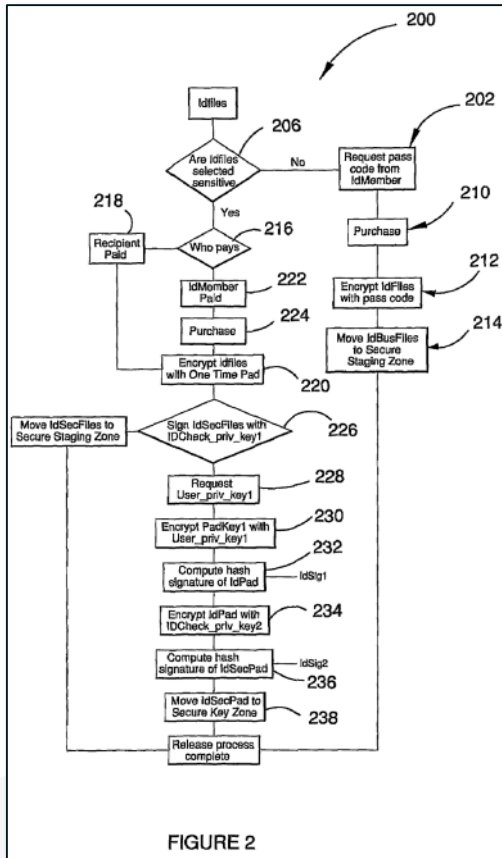
Prior Art: Stafford

(54) METHOD AND SYSTEM FOR VERIFICATION OF PERSONAL INFORMATION

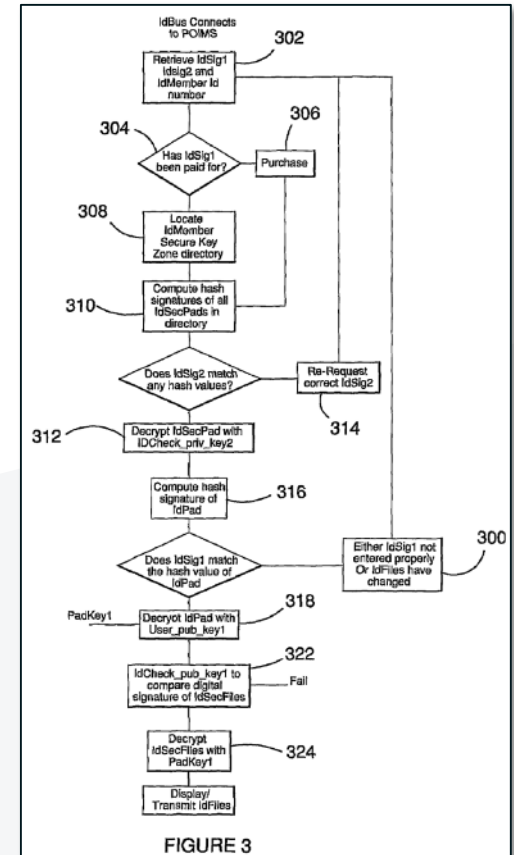
(57) ABSTRACT

In one form, there is disclosed a system (100) for storing, validating and disseminating credential information about an entity. The system (100) generates data representing at least part of the credential information and a data representation of at least part of a document supporting that information and stores the credential information and data representation in a database (120) in an encrypted form.

[0065] Verification of the information conveyed by the documentation can either be performed in a number of ways and may include; use of an Internet link with webcam for physical identification (e.g. that a person appears visually similar to a photograph), manual verification of individual documents, automated verification with third parties, or verification of document or data authenticity with a document's issuing body etc. The system may also have the facility to also allow the assignment of a 'confidence' rating against an entity that issues credentials. This rating can be used by recipients in their assessment of the weight to be given to an IdMembers' credential information. For example, the issuing body "Belford University" may verify that IdMember has a PhD, but if the system has a poor confidence rating for rate Belford University recipients may not trust the otherwise verified credentials? Or alternatively an IdMember user may choose not to release information to a recipient unless their confidence level is over a certain threshold set by either the system or the IdMember.



[0031] FIG. 2 is a flow chart illustrating a process for preparing information for release to a third party in an embodiment of the present invention; and



[0032] FIG. 3 is a flow chart illustrating a method of transmitting released data to the third party in an embodiment of the present invention.

Prior Art: Purves

(54) WALLET SERVICE ENROLLMENT PLATFORM APPARATUSES, METHODS AND SYSTEMS

Service providers	Payment methods
Hautelook	Card1 Image XXXX-XXXX-XXXX-XXXX 1227
BestBuy	☐ My personal card
Nordstrom 	Newly Enrolled Card #1 1228
Gap	☐ My Visa cash back card
Ann Taylor	Newly Enrolled Card #2 12 29
Portland General Electric	
Amazon	
Verizon	
Home Depot	
Fresh Direct	

(57) ABSTRACT

The WALLET SERVICE ENROLLMENT PLATFORM APPARATUSES, METHODS AND SYSTEMS ("WSEP") facilitates the enrollment of payment accounts in a consumer's virtual wallet. The consumer may be logged into their payment account issuer's web site and designate one or more payment accounts for enrollment in a virtual wallet. The issuer may then share account, billing and/or other relevant information with the virtual wallet provider to facilitate the enrollment of the designated payment accounts in the virtual wallet. The WSEP may also be configured to facilitate the creation and funding of pre-paid accounts in a consumer's virtual wallet.

1205c. The payment methods panel 1210 may list one or more payment methods 1210a-d that are present in the wallet. The panel 1210 may display an image of the card (e.g., from the issuer), a nickname for the card, card identifier, card brand, and/or the like. The payment methods may also include bank or other financial accounts, debit cards, credit cards, prepaid cards, gift cards, and/or the like. In some implementations, the customer may also add new card to the wallet directly from the control panel interface. The customer may select one or more of these payment methods for sharing with the merchant 1205c. When the wallet provides the shared payment method to the selected service provider, only select information such as the nickname, brand, and last four digits of the card number, etc., may be shared. In some implementations, the actual card or account number may not be shared with the service provider.

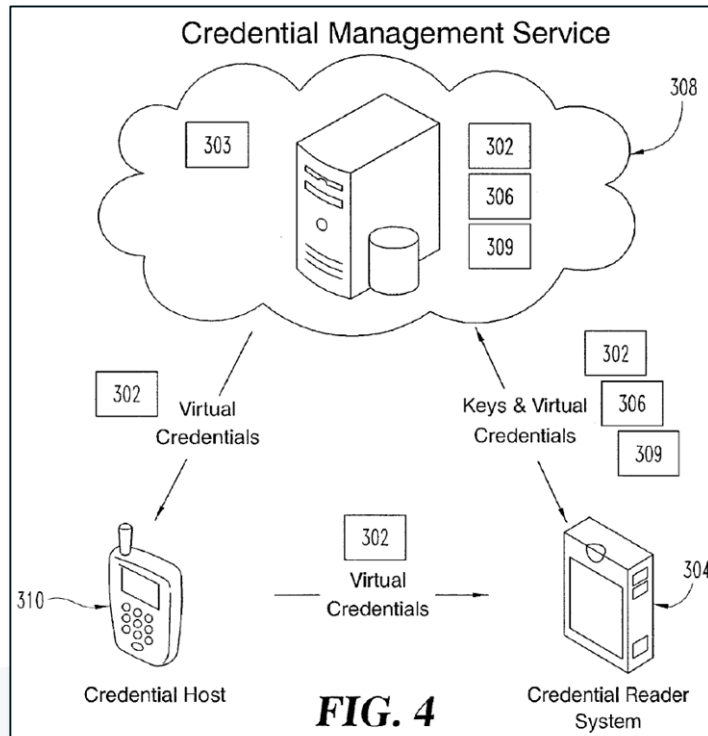
[0083] FIG. 11 shows a block diagram illustrating an example prepaid card personalization in some embodiments of the WSEP. In one implementation, a consumer having a wallet account may obtain a new gift card (open loop or closed loop) or a reloadable prepaid card 1130. The consumer may personalize the card for online or offline usage and be able to view and service the account with the issuer. In one

virtual wallet account. The user may then activate the wallet account 2102a. The user may then indicate that they desire to add a new payment account to their virtual wallet 2103. The WSEP may then request that the user consent to the retrieval of their payment account information from the payment account issuer 2104. The user may be asked to provide the account number of the payment account that the user wishes to link to their virtual wallet account 2105. The WSEP may then use the user's account number or other credential such as a username/password combination or the like to initiate a request for retrieval of pre-provisioned data associated with the payment account 2106. In some embodiments, the request for retrieval of pre-provisioned data 2106 (e.g., "prefill data") may be in the form of an HTTP(S) message including XML-formatted data containing fields substantially similar to the following:

EX1013, Abstract, ¶¶83, 85, 107, Fig. 12a

Prior Art: Neafsey

(54) CREDENTIAL MANAGEMENT SYSTEM



[0049] Process 320 proceeds from operation 326 to operation 328. At operation 328, the credential management service 308 generates a virtual credential 302 and sends the virtual credential 302 to the credential host 310. The credential management service 308 may generate the virtual credential 302 based on the unique device ID by hashing the unique ID with the master key 303.

[0061] As seen in FIG. 9, by virtualizing these credentials 502 (i.e., generating them in a central cloud credential management service 504 rather than on type specific programmers) several features may be realized. For example, worldwide encoding schemes can be consolidated into one central cloud credential management service 504. Rather than creating and selling hardware devices that create credentials, the virtual credentials 502 themselves may be sold, which are hosted by and delivered to a mobile device 104 such as a smartphone. Virtual credentials 502 may be written to any credential host (e.g., a mobile device 104 such as a smartcard, smartphone, or the like). Virtual credentials 502 can be generated by the cloud credential management service 504 in multiple formats (e.g., prox, MIFARE Classic, MIFARE DESFire EV1, optical, XceedID, eISA, bar code, QR code) depending on the requesting host. Virtual credentials 502 can be generated and encoded for multiple regions and localities (e.g., Americas, Europe, Asia etc.). Customers of the cloud credential management service 504 may purchase these virtual credentials 502 and have them generated on demand by the cloud credential management service 504.

EX1015, Abstract, ¶¶49, 61, Fig. 4; EX1016, 10, 12, Fig. 4

Oborne Combination Grounds

Oborne+Neafsey

318. Neafsey teaches that various formats of virtual credentials may be used for conducting transactions. Among these formats are optically-scannable codes, such as QR (quick response) and bar codes. EX1015, [0061]; re optical, see EX1016, 12; EX1011, ¶32 (describing QR and barcodes that may be scanned with a camera). A POSITA would have been motivated to incorporate an optically scannable code into an OVER file to be used to trigger the use of tokens to purchase goods, in a manner similar to Osborne's disclosure of using NFC or mag stripe interactions, as Neafsey teaches that such optically scannable codes would serve similar roles. The combination would thus be a simple substitution of known elements to achieve predictable results. Doing so would provide greater flexibility to users, increasing convenience and allowing a greater range of mobile devices to be employed (e.g., devices with screens capable of displaying a QR code could be used even if NFC communication was unavailable).

Oborne+Purves

295. A POSITA would have been motivated to combine Osborne and Purves with a reasonable expectation of success to arrive at claim 3. Both references are directed to similar applications, including the use of virtual wallets and credentials, and the teachings of Purves would be recognized as useful to add new credentials to Osborne's digital wallet (for example, where a user had not yet added any credentials, or where adding further credentials were desired). It would have been common sense to generate the new credential only "when the processor determines that no credential of the user is stored," since the purpose of Osborne's tokens is to represent a credential, and with a new credential the user is able to benefit from Osborne's tokenization system. This combination would be a predictable combination of known, related technologies, to produce a predictable result (a wallet system capable of engaging in tokenized transactions and of adding new credentials as needed).

Oborne+Neafsey+Purves

345. As discussed above for claim 3, a POSITA would have looked to combine Osborne and Purves, as the two references provide complementary teachings regarding virtual credentials, tokenization, and wallets. Neafsey's teachings regarding virtual credentials would similarly be complementary to Osborne and Purves. A POSITA would be motivated to combine Purves's disclosure regarding providing credential images with Osborne and Neafsey's virtual credentials to include a credential image as part of an OVER file also including a token as taught by Osborne and a scannable code as taught by Neafsey to provide an improved interface for users with a simple visual indication of the credentials to be invoked in a tokenized transaction.

486-Pet., 42-54; 487-Pet., 34-48; 486-EX1005, ¶¶295, 318, 345

Oborne: Issuing Agency Verification [Element 1.3]

- Oborne teaches or suggests verification by an issuing agency:
 - (1) Token generated by funding source is a verified token

[0029] In some implementations, a user may be able to control the attributes of each token associated with the user via a web interface, e.g., 220. For example, the user may be able to login to the web interface, e.g., 221, and visualize payment tokens associated with the user, e.g., 223. The user may also be provided with user interface elements to generate new tokens. For example, the user interface may provide elements for creating a new token, e.g., 224. For example, the user interface may allow the user to select financial details 225 such as, but not limited to: a funding source from whom to obtain a token, an account type for the token, an initial token value (e.g., for pre-funding, and/or pore-authorization),

options. For example, the user's payment token may be linked to one or more issuer financial institutions ("issuers"), such as banking institutions, which issued the account(s) for the user linked to the payment token. For example, such accounts may include, but not be limited to: credit card, debit card, prepaid card, checking, savings, money market, certificates of deposit, stored (cash) value accounts and/or the like. Issuer server(s), e.g., 609a-n, of the issuer(s) may maintain details of the user's account linked to the payment token. In some

Id., [0058]. 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.

EX1011 (Oborne), ¶¶29, 58

486-EX1005 (Shamos Decl.), ¶240

Oborne: Issuing Agency Verification [Element 1.3]

- Oborne teaches or suggests verification by an issuing agency:
 - (2) Oborne teaches verification of virtual representation by checking credential data, meeting PO's example of verification of virtual representation

PO's example of verifying
a virtual representation:
486-POR, 12
(quoting EX1001, 6:44-52)

[t]he OVER File database 128 may contact the issuing agency database 130, such as a state DMV database, and provide the driver's license identification number to the issuing agency database 130. The issuing agency database may respond by indicating the validity of the requested credential containing the driver's license identification number and may provide the legal name, address, and birth date of the person associated with the driver's license identification number.

In some implementations, each token may be pre-funded. For example, the source of the token (e.g., issuer, acquirer, independent token arbitrator) may first obtain assurance that funds have been uniquely and exclusively allocated for the token from the source to which the token points. Thus, in

tion 1252 by selecting the verify button 1253. In one implementation, the verification may include contacting the issuer of the pay card for confirmation of the decoded information 1252 and any other relevant information. In one implementation, the user may add the pay card to the wallet by selecting the 'add to wallet' button 1254. The instruction to add the pay

Oborne teaches these limitations in at least two ways. First, when adding a user's card to a wallet for Oborne's system, Oborne teaches that verification of the pay card's information 1252 (such as name, account number, etc.) may be performed, and that "verification may include contacting the issuer of the pay card for confirmation of the decoded information 1252 and any other relevant information."

EX1011 (Oborne), ¶¶47, 108

EX1005 (Shamos Decl.), ¶219

486-Pet., 23, 33; 486-EX1005, ¶¶219, 240-42; 486-Reply, 2-6

Oborne: Issuing Agency Verification [Element 1.3]

- Oborne teaches or suggests verification by an issuing agency:
 - (3) Verifying token as official representation would also have been obvious:

EX1005 (Shamos Decl.), ¶241:

application form when generating the token. The issuer of a token representing a payment credential would logically ensure that the token accurately represented the credential. The existence of unofficial, forged or altered tokens in the marketplace would create problems for both issuers and users. It would be a routine step to verify that the token was an official representation of the credential based on the credential data received and doing so would increase confidence that the token legitimately represented the credential.

- PO's expert does not dispute validly linking token to account would have been desirable:

EX1047 (Malek Tr.), 50:20-51:7:

it is a goal of Oborne to provide a token for the purchase of making subsequent payments, it would be desirable for the token that is provided to be properly associated to at least one user payment account, correct?

MR. WILSON: Objection. Form.

THE WITNESS: I haven't offered an opinion about that. I don't know. Possibly.

486-Pet., 23; 486-Reply, 4-7

Oborne: OVER Engine [Claim 1 – All Elements]

- Petition identified Osborne’s disclosure of the OVER Engine:

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

Oborne teaches an *OVER* generation and verification engine (*OVER engine*). Oborne teaches 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,”

Osborne teaches that the token server “parse[s] the form to extract data fields and values from the form” 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, ¶¶47-48, Fig. 5 (showing process); EX1005, ¶238.

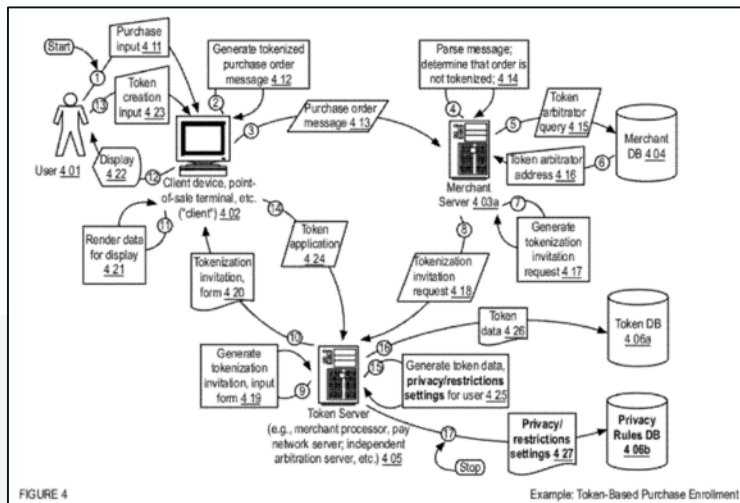
thus teaches that the OVER engine (token server) receives the recited verifying request from a third-party device based on the recited scan. EX1005, ¶245.

Oborne thus teaches element 1.5.

7. **Element 1.6**

verifying that the scan associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request;

Osborne teaches that the token server processes the token arbitration request triggered by the scan (discussed above for element 1.5) 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



Oborne: Dependent Claim 2

- “...a second OVER file...invalid for use in the first OVER file storage client device”
- Osborne teaches users have different devices, as PO’s expert admits:

So at the bottom of that Paragraph 105, I say, "As I mention above, I have not found any disclosure or suggestion of Osborne in the use of multiple devices by a single user." Actually when I was preparing for my deposition, I was reading the exhibits more carefully and I was reading Osborne in detail. I did come across a disclosure in Osborne that, in fact, talks about multiple devices for users, and I'm going to try to find that here.

So it's in Paragraph 148 of Osborne, the second sentence. It says, "A User's Table, 1519A, may include

EX1047 (Malek Tr.), 9:20-10:4

- Osborne teaches device fingerprinting for device-specific tokens:

```
<token>
<unique_ID>4NFU4RG94</unique_ID>
<!-- user_ID may optionally be used in some embodiments-->
<user_ID>john.a.public@gmail.com</user_ID>
<timestamp>2011-02-22 15:22:43</timestamp>
<expiry>2011-02-28 23:59:59</expiry>
<auth_flag>true</auth_flag>
<auth_protocol>verifychat</auth_protocol>
<security_protocol>digital certificate, digital_cer_link
</security_protocol>
<digital_cer>52486ghb0bn_encrypted_hash_information_89032y4gh<digital_cer>
<digital_cer_link>http://www.acmedigitalcertification.com/auth.php?var=0t1h
v43059876</digital_cer_link>
<!-- In some embodiments, client_details are optional and the token may be
tied to a specific client-->
<client_details>
  <client_IP>192.168.23.126</client_IP>
  <client_type>smartphone</client_type>
  <client_model>HTC Hero</client_model>
  <OS>Android 2.2</OS>
  <app_installed_flag>true</app_installed_flag>
  <client_fingerprint>font list, MAC address, memory size, hardware
chip, screen resolution</client_fingerprint>
```

[0026] In some implementations, additional security may be layered by using authentication methods. As an example, a user may be required to provide a user name and password to activate a payment token. As another example, a user may be required to provide a digital certificate to verify the user's identity prior to utilization of a payment token for a purchase transaction. As another example, device fingerprinting may be utilized. For example, a client device of a user may be a device that is used exclusively by the user, such as a smart-phone, tablet computer, laptop computer, and/or the like. In

EX1011 (Oborne), ¶¶26, 47-48

486-Pet., 31-32; 486-Reply, 8-11

Oborne: Dependent Claim 2

Oborne's tokens. EX1011, [0026]. There would be no purpose to device fingerprinting if a token could be used on any device. Similarly, Oborne provides an example of a token data structure that includes a "client_fingerprint" field with device-identifying information such as the client's MAC address. EX1011, [0047]. Device MAC addresses are 48 bits long and are globally unique. To obtain the additional security taught by Oborne, a POSITA would have been motivated to employ Oborne's device fingerprinting to tie a given token to a particular device, such that the token for a second device would be invalid if used in a first device (since the device's fingerprint would not match).

EX1005 (Shamos Decl.), ¶254

- “But even if one possible obvious combination falls outside of the claims, it fails to undercut the fact that the other possible obvious combination lies within their scope.” *ACCO Brands Corp. v. Fellowes, Inc.*, 813 F.3d 1361, 1367 (Fed. Cir. 2016)

486-Pet., 31-32; 486-Reply, 8-11; 486-EX1005, ¶¶213-18

Oborne: Dependent Claims 7 and 20

- “the status indicator indicates an invalid credential and the credential information indicates a reason for the invalid credential”
- Petition provided numerous examples of status indicators meeting this limitation that were obvious over Oborne

486-Pet., 36:

As discussed for claim 4, Oborne teaches status indicators indicating whether a credential is valid (e.g., a verification and/or authorization response). A negative response for either indicator would indicate an invalid credential. EX1005, ¶262. Moreover, it would be obvious for the credential information to indicate a reason for invalidity; for example, if the information provided for the credential did not match the issuer's information, it would be routine to indicate this mismatch in a rejection response. Further, where a credential was not valid for a given transaction, Oborne expressly teaches indicating the reason for invalidation. For example, an issuer response can indicate lack of funds, or indicate that a “number of failed authorization attempts exceeds a threshold” by sending a “transaction terminated” message. EX1011, ¶72. Each of these messages indicates a reason that the credential is invalid. EX1005, ¶¶264-65.

- Dr. Shamos confirmed conventionality of such status indicators, e.g.:

H. Reason for Invalid Credential

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

See generally EX1005, ¶¶264, 219-27 (citing, *inter alia*, EX1032, 88; EX1040, 125; EX1044, ¶46)

486-Pet., 36, 52; 486-Reply, 11-12

Oborne: Dependent Claims 8 and 29

- “reference to a remotely stored credential”

[0133] The memory 1529 may contain a collection of program and/or database components and/or data such as, but not limited to: operating system component(s) 1515 (operating system); information server component(s) 1516 (information server); user interface component(s) 1517 (user interface); Web browser component(s) 1518 (Web browser); database(s) 1519; mail server component(s) 1521; mail client component(s) 1522; cryptographic server component(s) 1520 (cryptographic server); the PPT component(s) 1535; and/or the like (i.e., collectively a component collection). These components may be stored and accessed from the storage devices and/or from storage devices accessible through an interface bus. Although non-conventional program components such as those in the component collection, typically, are stored in a local storage device 1514, they may also be loaded and/or stored in memory such as: peripheral devices, RAM, remote storage facilities through a communications network, ROM, various forms of memory, and/or the like.

the above tables). Employing standard data processing techniques, one may further distribute the databases over several computer systemizations and/or storage devices. Similarly, configurations of the decentralized database controllers may be varied by consolidating and/or distributing the various database components 1519a-n. The PPT may be configured to keep track of various settings, inputs, and parameters via database controllers.

EX1011 (Oborne), ¶¶133, 150

engine itself. This was conventional, as credentials themselves, for security purposes, would be stored in a location separate from the place where the representation would be generated. This was the method of operation of the Kerberos system from the 1980s, described below beginning at ¶121.

266. This limitation was obvious, at least because it was common for tokens to be generated on a different server from the one on which the original credential were stored, at least for reasons of security.

468-EX1005 (Shamos Decl.), ¶¶61, 266

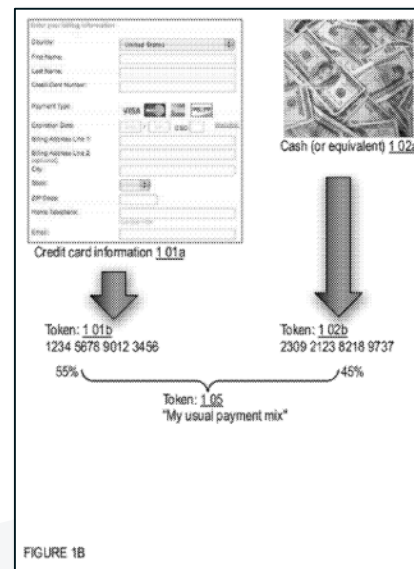
486-Pet., 37; 486-Reply, 13

Oborne: Dependent Claims 12-13

- Petition's "credential identifier" in claims 12-13 consistent with claim 11
- Claim 11—credential identifier may be account number or token indicator (where one token refers to others):

stored when creating a token, with the token data structure indicating which account number(s) correspond to a given token. See EX1011, ¶¶40, 47 (identifying by account numbers of user's credentials associated with token); see also *id.*, ¶25, Fig. 1B (token may indicate mix of one or more specified credentials via token indicators). EX1005, ¶¶208-12, 273-74.

Accordingly, claim 11 was obvious over Oborne.



EX1011 (Oborne), Fig. 1B (excerpt) (showing token 105 identifying other tokens 101b and 102b by their token ids)

- Claims 12 and 13—*same* token identifier is credential identifier that is compared with stored credential:

routing numbers, etc.). By using the token identifier to query a database and retrieve stored credentials (e.g., cards' account numbers), Oborne is comparing the credential identifier with the stored credentials. EX1005, ¶¶275-76.

Accordingly, claim 12 was obvious over Oborne.

the status indicator. EX1005, ¶277. Further, this is sent "when the credential identifier matches a stored credential" because, as discussed for claim 12, the accounts are identified by using the credential identifier (token ID) as a database query to retrieve stored account information (matching identifier to stored credentials). See EX1011, ¶69.

Oborne thus renders claim 13 obvious. EX1005, ¶¶277-78.

Oborne, Neafsey, and Purves: Dependent Claim 19

- “the OVER file comprises a credential image”
- PO’s expert admits Purves’ user device stores credential images:

Q. So then I want to make sure I have it right. The card information, such as the card image, are transmitted from the Purves server to the user's mobile device where they're stored in RAM in order to display the wallet information on the user's device screen; is that right?

A. Yeah, so a user's -- so in a web-based application, the web browser would request data from the server, would receive that data. If that data involves images, those would be also loaded up in the memory parse, you know, processed by the web browser and then displayed on the screen to the user.

EX1047 (Malek Tr.), 69:16-71:18

- PO fails to identify any legitimate security concerns, as addressed for Stafford grounds

486-Pet., 53-54; 486-Reply, 14-15

Oborne and Purves: Dependent Claims 23-26, 28-33

- Purves teaches generating new credential and adding credential to wallet account, including obtaining requested credential information from issuer

[0083] FIG. 11 shows a block diagram illustrating an example prepaid card personalization in some embodiments of the WSEP. In one implementation, a consumer having a wallet account may obtain a new gift card (open loop or closed loop) or a reloadable prepaid card 1130. The consumer may personalize the card for online or offline usage and be able to view and service the account with the issuer. In one implementation, through the issuer's online or mobile service channel 1105, the consumer may click a WSEP button 1110. In a further implementation, the WSEP button may spawn a modal widget 1115 powered by the wallet. The consumer may authenticate to the wallet and may confirm their wish to personalize the new card and share the personalization information with the issuer. In one implementation, the personal-

account 2102a. The user may then indicate that they desire to add a new payment account to their virtual wallet 2103. The WSEP may then request that the user consent to the retrieval of their payment account information from the payment account issuer 2104. The user may be asked to provide the

[0108] In some embodiments, the issuer may then use the data in the request to perform a lookup of account and/or prefill information that may be shared with the requesting service. In some embodiments, the issuer will have a permissions rule set that governs what data may be shared with requesting services. Example rules include, "Never share my business account number," "Default to my personal account,"

EX1013 (Purves), ¶¶83, 107-08

- Petition explained usefulness of applying Purves's approach to adding new credentials when addressing request recited in claim 23

Stafford + Purves

355. A POSITA would have been 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.

356. Similarly, a POSITA would have viewed Purves's QR codes 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 QR-encoded key signatures, a POSITA would reasonably have expected to achieve these benefits for users.

[0085]. The server may also generate an on-the-fly image of the credential to be used to represent the credential on the user's device, optionally with "confidential information ... obscured." EX1013, [0122]; *see also id.*, [0111]-[0112] ("multiple versions of the card" may be used in various formats). A representative image provided "from an issuer" would be "verified by the issuing agency" as an official representation, as would an image produced from an actual credential, since an actual credential naturally represents itself.

367. In view of Purves's teaching to provide user devices with images representing a credential (such as a credit card), it would have been obvious to use similar credential images in the context of Stafford. For example, the system would provide an image of the user's credential (e.g., a generally-representative, issuer-provided image provided by the issuer or a real image of the credential with optionally-obscured confidential information) along with the encoded key signature to remind users which credential the key signature represents and enable quick selection from among a plurality of options available on the user's device. See EX1013, [0085], [0122]. Such an image would be a virtual representation verified by the issuer as being an official representation of the credential.

368. Should Patent Owner argue that the claim requires that the credential itself be verified by the issuer (as opposed to verifying the virtual representation), this would also have been obvious, as Stafford expressly teaches contacting an issuer to verify a credential. See EX1012, [0065].

486-EX1005 (Shamos Decl.), ¶¶355-56, 366-68

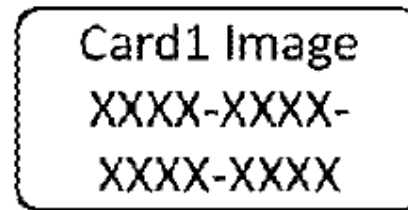
Stafford + Purves [Element 1.3]

370. Stafford in view of Purves teaches limitation 1.4. Stafford teaches that the key signatures generated by its online credential-database system can be sent to the user electronically (e.g., by email or by sending to a user's display to be copied). EX1012, [0097]-[0099]. As discussed for limitation 1.3, it would have been obvious to send an OVER file comprising a virtual representation (e.g., an issuer-verified credential image) and the key signatures encoded as a scannable QR code. Thus, Stafford in view of Purves teaches the recited transmitting step of

486-EX1005 (Shamos Decl.), ¶370



key signature, generated
based on pad associated
with credential, encoded
as QR code



generic or redacted
credential image
provided by issuer
as official virtual
representation

EX1013 (Purves), ¶¶64, 85, 111; EX1054 (Hairamani), Fig. 2

486-Pet., 59-64; 486-Reply, 16-28

Stafford + Purves: Key Signatures [Element 1.3]

- Stafford's key signatures are based on information (e.g., IdPads) associated with a credential, which was verified by issuing agency
- They are electronic, virtual representations of credential documents

Dr. Malek:

process.”). Because the documents for release have already been selected and confirmed before any hash values are created, there is no reason in Stafford to remind a user what documents are represented by IdSig1 and IdSig2. Additionally, the

EX2009 (Malek Decl.), ¶164

A. It's a representation that is virtual, that, you know, for example, could be -- you know, it would be something that is, for example, digital.

Q. I was going to ask you if you thought "virtual" meant electronic, but it sounds like that's similar --

A. Yeah, electronic, sure. I mean, that would be at least one aspect of it.

Q. And then the representation part of that term, are there any particular requirements on what something needs to be a representation of something else?

A. I -- you know, I haven't offered an opinion about that. I've applied the plain and ordinary meaning of it.

EX1047 (Malek Tr.), 31:25-34:5

Dr. Shamos:

10. I agree with Dr. Malek that the term “virtual representation” has its plain and ordinary meaning in these claims. EX1047 (Dr. Malek's Deposition Transcript), 31:25-34:5. I also agree with Dr. Malek that “virtual” here simply means that the representation is digital/electronic. *Id.* Turning then to the word “representation,” a POSITA would have understood that a “representation” of the credential does not have to look like the credential or include its contents. While a “representation” of something *may* be a depiction of it in one sense of the word, it may also simply be a symbol or stand-in for the thing it represents. Consider the example of a coat-check ticket. A coat-check ticket does not look like or describe the coat, but it still “represents” the coat.

11. In my opinion, a POSITA would have understood Stafford's key signatures to be a “virtual representation of the credential” under the plain meaning of that phrase. The user holds a set of key signatures that represent a given credential that has been set up for release, and when the user is ready for a third-party recipient to receive the credential information, the key signatures are passed to the recipient, who essentially trades the key signatures for the credential

EX1048 (Shamos Reply Decl.), ¶10

486-Reply, 16-19

Stafford + Purves: Card Images [Element 1.3]

- No dispute that Purves's card images are virtual representations verified by issuer as official representations
 - Arguments against Stafford key signatures fail to address combination as a whole
- PO's arguments against Purves fail
 - Purves's card images are stored
 - PO distorts claim language to manufacture requirement of verification using virtual representation

Stafford + Purves Teach Storing Card Images

- Stafford teaches storage of virtual representations, e.g.:

[0097] Next, in step 232 a hash value of IdPad is created, called IdSig1. IdSig1 represents a first key signature component that is required by a recipient to collect/obtain the released information. IdMember can choose to either copy IdSig1 from the display or have it sent to him/herself in an email. If the email option is used, the system will encrypt IdSig1 with User_pub_key1 prior to sending.

EX1012 (Stafford), ¶197

- Both experts agree Purves's images were stored on user device:

Q. So then I want to make sure I have it right. The card information, such as the card image, are transmitted from the Purves server to the user's mobile device where they're stored in RAM in order to display the wallet information on the user's device screen; is that right?

A. Yeah, so a user's -- so in a web-based application, the web browser would request data from the server, would receive that data. If that data involves images, those would be also loaded up in the memory parse, you know, processed by the web browser and then displayed on the screen to the user.

EX1047 (Malek Tr.), 69:16-71:18

25. Even though Purves does not expressly state that the transmitted credential image is "stored" on the user's device, this would have been perfectly clear to a POSITA since the image is displayed on the user's device. EX1013, ¶¶85, 104. A POSITA would have recognized that data displayed on a device's screen is stored in memory on the device, at the very least in a screen buffer. Dr. Malek appears to acknowledge this. EX2009, ¶162 (acknowledging that Purves teaches "transient storage on a client or user device"). A POSITA also would have understood that the image is transmitted to the device since the device must receive the image in order to display it. Patent Owner is therefore incorrect in asserting that Purves does not teach transmitting the credential image to the user's device or storing the credential image on the user's device.

EX1047 (Shamos Reply Decl.), ¶25

Stafford + Purves: Verification Limitations

- POR:

b. Purves Does Not Teach Using Card Images For Verification

- No requirement that the virtual representation be *used for verification*
- Element 1.3 requires virtual representation that *has been verified*, not *used for verification*

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

- Element 1.5's verification step does not require use of virtual representation, only a "scan associated with the OVER file"

receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file store client device of the user;

Stafford + Purves: Rationale to Use Card Images

- PO:

information. The message can be used to direct the IdMember eg using a web link embedded in an email, to a payment screen and then on to the rest of the release process.”). Because the documents for release have already been selected and confirmed before any hash values are created, there is no reason in Stafford to remind a user what documents are represented by IdSig1 and IdSig2. Additionally, the

EX2009 (Malek Decl.), ¶164

- Stafford’s key signature generation (Fig. 2) occurs first; its use to release credential to 3P (Fig. 3) can occur later

after the key signatures are generated, as Patent Owner argues. If the user decides to pay for the service themselves, the selection of particular key signatures at the time of the transaction with the third-party recipient is still a separate step. This is

particular third-party recipient at the time of the transaction. For example, if a user pre-pays for the release of tickets on two different flights, the user would still select the key signatures associated with the first ticket when boarding the first flight.

33. Using images to keep track of items is thus sensible and useful. A user can set up multiple items for release. EX1012, ¶¶74 (“The IdMember can be

of information authorized for release.”). The user receives key signatures for each item that has been set up for release. *Id.*, ¶¶102-05. But the key signatures are not “spent” until the user gives them to a third-party recipient, who then submits the key signatures to the system to obtain the associated credential information. *Id.*, ¶¶113-26, 133. The user may thus hold multiple sets of key signatures, much like a person can hold multiple single-use tickets or credit cards in a physical wallet that can be selected and used later. Using images (rather than abstruse key signature character strings) to identify/select particular items that were previously set up for release thus makes perfect sense.

EX1048 (Shamos Reply Decl.), ¶¶32-33

486-Reply, 21-23

Stafford + Purves: Rationale to Use Card Images

- Purves's wallet has single-use items like tickets and other accounts (EX1013, ¶¶54, 102):

wallet login, and/or the like. A transit authority connected to a wallet may load or associate transit passes with the wallet, allow returning customer to login to their transit account or purse through the wallet login widget, allow redemption of transit passes or tickets from the wallet, and/or the like.

2008. In doing so, the consumer may be assisted in the creation of a virtual wallet account by avoiding the entry of repetitive data that the issuer already has on file. This pre-fill of data may also be advantageously used in the establishment of other account types, including pre-paid accounts, reward accounts, savings accounts, and/or the like. In other embodi-

- Stafford's system supports varied credential types for different transactions (EX1012, ¶¶81, 109):

[0109] As will be appreciated, the type of information required to be submitted and the level of information verification required by IdBus1 in order to provide the desired service or goods to the IdMember will depend on the nature of the service or goods.

may be able to be set by IdMember. However, in most cases the system will have predetermined sensitivities for some types of data, eg for example, the IdMembers date of birth, salary details, credit rating, tax file number, bank account numbers, credit card numbers etc., would all be considered highly sensitive information and as such classified to an appropriate sensitivity rating. Sensitive data is not able to be

- Stafford's users can have many credentials prepared for release (EX1012, ¶118):

[0118] Once a payment has been verified the system 100, uses the IdMember's MIN to interrogate the data storage in the Secure Key Zone 120 at 308. The IdMember's directory in the Secure Key Zone 120 may include multiple IdSecPad's corresponding to different parcels of information authorized for release.

Stafford + Purves: Rationale to Use Card Images

- PO does not address representative images in POR and claims obscured images pose security risk
- Purves expressly teaches use of representative images and obscured images:

1205c. The payment methods panel 1210 may list one or more payment methods 1210a-d that are present in the wallet. The panel 1210 may display an image of the card (e.g., from the issuer), a nickname for the card, card identifier, card brand, and/or the like. The payment methods may also

EX1013 (Purves), ¶¶85, 122

be used 2323. In some embodiments, the card image server may create an “on the fly” image to represent the card and overlay that image with appropriate consumer specific data such as name, photo, and/or the like 2323a. In some embodiments, confidential data such as PAN number, account number and/or the like may be obscured from the overlaid data using a tool such as ImageMagik. In doing so, the card image server may protect confidential consumer information. The

- Representative images, obscured images, and partial numbers routinely used:

35. I disagree with Dr. Malek's argument against using a representative credential image. Dr. Malek argues that representative images still convey valuable information such as the existence of an account with a particular bank. EX2009, ¶168. But such images were routinely used in virtual wallets. For example, a user who wishes to charge a transaction but possesses multiple credit cards must select one for a given transaction, and it was common in virtual wallets to provide representative images of the cards to facilitate the selection. E.g., EX1053

405), ¶110 (discussing same).¹ It was also common for virtual wallets to list available payment options with sensitive information obscured. For example, available payment options were often listed with part of the account numbers masked (e.g., masking all but the last four digits of a credit card number). E.g., *id.*,

EX1048 (Shamos Reply Decl.), ¶35

Stafford + Purves: Rationale to Use Card Images

- No dispute unrecoverable redactions were known

Q. So you mentioned that a redacted image, the way to ensure that a redacted image can't be recovered is to not send the image in the first place. Is it your opinion that it is impossible to redact an image such that the redaction can't be undone?

A. You see that's not the opinion that I've offered in this case. The opinion that I've offered is in the context of what Dr. Shamos is saying. Dr. Shamos is not saying to send -- to send no image or to send an image that is completely redacted. He's saying you would send an image that would help the user to know, to remember what the card or what kind of a bank account we're dealing with.

EX1047 (Malek Tr.), 79:16-82:1

For example, obscuring encompasses redacting/removing data from the image altogether. Generating an image with information irrecoverably obscured was commonplace and readily achieved by a POSITA. E.g., EX1055 (Redactis) (tool "allows you to redact an image, blocking out confidential information," including permanent redactions). Indeed, Purves teaches using an obscured image even for sensitive credentials like payment cards using available tools. EX1013, ¶122 ("In

EX1048 (Shamos Reply Decl.), ¶36

Q. Look at Paragraph 167 of your declaration, please.

In this paragraph, you present a conceptualization of what a credit card with the confidential information obscured might look like, right?

A. Yes.

Q. Did you create that image?

A. I believe the counsel created this image.

Q. Are you aware of whether whoever created that image used ImageMagick?

A. I -- I don't know what tool they used, no.

Stafford + Purves: "Security Issues" Don't Undermine Rationale

- Stafford and Purves teach secure transmission may be used

released information. IdMember can choose to either copy IdSig1 from the display or have it sent to him/herself in an email. If the email option is used, the system will encrypt IdSig1 with User_pub_key1 prior to sending.

EX1012 (Stafford), ¶97

Q. That approach of using HTTPS instead of HTTP, that wasn't something that was unique to your project at PricewaterhouseCoopers, was it?

A. No, I think HTTPS has been known for many years.

Q. So again, that sentence reads, "Employing such encryption security protocols, the WSEP may encrypt all incoming and/or outgoing communications."

Do you see that?

A. Yes.

Q. Do you have any reason to disagree with that statement in Purves?

A. I don't have an opinion about it, no.

EX1047 (Malek Tr.), 24:6-9, 76:7-14

Microsoft Internet Explorer or Netscape Navigator. Secure Web browsing may be supplied with 128 bit (or greater) encryption by way of HTTPS, SSL, and/or the like. Web

EX1013 (Purves), ¶152

52. The subsequent conveyance of the key signatures from the user to the third-party recipient also would have been just as if not more secure using QR codes. In a typical use-case for this type of transfer, the user presents a QR code image for scanning by the recipient, which facilitates an essentially automatic transfer of the QR-encoded data. Compare this to Stafford's examples for conveying the non-QR-encoded key signatures to the third-party recipient. In one example taught by Stafford, the user simply copies down the key signatures from their display. EX1012, ¶97. In other words, the key signatures themselves are displayed on the user's device and written down so that they can be manually entered by the third-party recipient. The QR-code-mediated transfer provided by the combination is not only easier and less error-prone than Stafford's example, it is more secure since it does not require the user to write down the key signature characters or read them aloud to facilitate manual entry by the third-party recipient.

EX1048 (Shamos Reply Decl.), ¶52

486-Pet., 61-64; 486-Reply, 25-27

Stafford + Purves: “Security Issues” Don’t Undermine Rationale

- Purves teaches using QR codes in transactions like Stafford’s ecommerce transactions, confirming lack of security risk

605. Invoking the WSEP button may trigger a wallet widget to either authenticate the customer or authenticate and connect the service, merchant, or application to the customer’s wallet account. In some embodiments, the WSEP button may be implemented in other channels and physical world scenarios such as point of sale interactions. For example, using a physical card swipe or chin/pin interaction may trigger a wallet account connection or login. As another example, using a quick response (QR) code scan, a near-field communication (NFC) tap or other mobile trigger in lieu of a WSEP button may also trigger a wallet connection or login. As yet another

EX1013 (Purves), ¶164

versatility of the preferred embodiment. The first example illustrates an example applicable to, e.g. ecommerce related activities and relates to the release of Sensitive Information for a business recipient.

EX1012 (Stafford), ¶106

- Proposed combination:

as part of Stafford’s credential distribution system (1) to provide user devices with convenient images of the credentials and (2) to use the well-known QR code format to transfer Stafford’s key signatures to the third party by providing QR-encoded key signatures to the user.

and error-prone. By adapting Stafford’s credential management system to provide QR-encoded key signatures, a POSITA would reasonably have expected to achieve these benefits for users.

486-EX1005 (Shamos Decl.), ¶¶353, 356

- Dr. Malek’s misunderstanding:

And my understanding is that what Dr. Shamos essentially is opining is that a user would take the information that comes from Stafford, the sig ID 1 and sig ID 2, and would create those QR codes manually, and so I would opine that that would be nonsensical to me.

Q. What do you mean by “create those QR codes manually?”

A. Well, I mean that the user would have to create them. So the user would have to go figure out how to create a QR code.

EX1047 (Malek Tr.), 28:9-16

486-Pet., 55, 63; 486-Reply, 25-27

Arguments for '531 Patent Apply to '854 Patent

- Arguments for '531 claims apply similarly to each disputed claim in the '854 Patent:

'854 Claims	'531 Claims
Independent Claims 1, 8 & 15	Claim 1, with claim 2 addressing “second OVER file” limitations
Dependent claims	No dispute by PO

Arguments for '531 Patent Apply to '859 Patent

- Arguments for '531 claims apply similarly to each disputed claim in the '859 Patent:

'859 Claims	'531 Claims
Independent Claims 1, 9, 18 & 20	Claim 1, with NFC/Bluetooth taught by Osborne and Purves
Claims 2, 10, 19 & 21	Claim 2
Claims 6 & 14	Claims 8 & 29
Claim 12	Claims 23-26 and 28-33

Arguments for '531 Patent Apply to '973 Patent

- Arguments for '531 claims apply similarly to each disputed claim in the '973 Patent:

'973 Claims	'531 Claims
Independent Claims 1, 8 & 16	Claim 1, with NFC/Bluetooth taught by Osborne and Purves
Claim 8 “requesting” limitation	Claims 23-26 and 28-33
Claims 2, 9 & 17	Claim 2
Claims 5 & 12	Claims 8 & 29

'859 Patent – Claims 19 and 21

- Petition explained that claims 2, 19, and 21 recite same limitations:

As to claims 2, 10, 19, and 21, each claim repeats elements 1.2-1.4 as applied to a second OVER file, with the second OVER file being invalid for use in the first user device. Applying the same teachings of Neafsey, an OVER file would

- Detailed analysis provided for claim 2:

Claim 2 depends from claim 1 adds the word “first” before each of claim 1’s OVER file, OVER file storage client device, virtual representation, and official representation. Claim 2 then recites three elements identical to elements 1.2-1.4, except that (1) the word “second” is applied instead of the word “first”; (2) the generation copied from element 1.3 need not be “based on the information associated with the credential of the user”; and (3) the second OVER file is “is invalid for use in the first OVER file storage client device for authenticating the user.” Osborne teaches these elements.

- Dr. Shamos confirms same obviousness reasoning applies to claims 19 and 21:

271. Claim 19 is identical to claim 2 except that it depends from claim 18 instead of claim 1. Therefore, claim 19 was obvious over Osborne for the same reasons as for claim 2. See *supra*, ¶¶230-232, and the cross-references cited therein.

276. Claim 21 is identical to claim 2, except that it depends from claim 20 rather than claim 1. Hence claim 21 was obvious over Osborne for the same reasons as claim 2, *q.v.*

- Headings, statement of precise relief, and conclusion also asserted Osborne rendered claims 19 and 21 obvious, just as for claim 2

489-Pet., 10, 14, 30-31, 41, 43, 78-80; 489-Reply, 12-14, 489-EX1005, ¶¶271, 276