IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

IPR2024-00486
IPR2024-00488
IPR2024-00489
IPR2024-00490

PATENT NO. 9,251,531
PATENT NO. 9,954,854
PATENT NO. 10,749,859
PATENT NO. 11,329,973

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

Table of Contents

I. Background 1
II. Materials Considered 2
III. Legal Principles.....4
IV. Level of Ordinary Skill in the Art.....4
V. Stafford's Key Signatures Are a "virtual representation of the credential" 4
VI. Stafford's Key Signatures Are "based on the information associated with the credential" 6
VII. Stafford's Key Signatures Have Been "verified by an issuing agency".....10
VIII. Purves Teaches Credential Images that Have Been "verified by an issuing agency".....12
IX. A POSITA Had Reason to Combine Stafford and Purves.....16
A. Purves' Teachings Are Applicable to Stafford 16
B. The Combination Is Not "Nonsensical".....17
C. Patent Owner's Arguments Against Credential Images Are Incorrect.....21
D. Patent Owner's Arguments Against QR Codes Are Incorrect.....26
E. The Combination's Substantial Benefits Outweigh Any Actual Security Concerns 36
X. Concluding Statement 38
XI. Jurat 38

I, Michael I. Shamos, declare as follows.

I. **Background**

1. As noted in my previous declarations, I have been retained by Wilson Sonsini Goodrich & Rosati Professional Corporation on behalf of Petitioner Visa Inc. ("Visa") to provide my opinions concerning the validity of claims at issue in several *inter partes* reviews ("IPRs"). The filed proceedings include IPR2024-00486, IPR2024-00487, IPR2024-00488, IPR2024-00489, and IPR2024-00490. IPR2024-00486 and IPR2024-00487 challenge claims 1-33 of U.S. Patent Nos. 9,251,531 ("'531 Patent" or EX1001). IPR2024-00488 challenges claims 1-17 of U.S. Patent No. 9,954,854 ("'854 Patent" or EX1002). IPR2024-00489 challenges claims 1-21 of U.S. Patent No. 10,749,859 ("'859 Patent" or EX1003). IPR2024-00490 challenges claims 1-17 of U.S. Patent No. 11,329,973 ("'973 Patent" or EX1004). I understand that all of these IPRs were instituted. I understand that IPR2024-00486 and IPR2024-00487 were consolidated and that all claims of the '531 Patent will be addressed in IPR2024-00486, as IPR2024-00487 is now terminated. I refer to the foregoing patents as the "Challenged Patents." I also understand that Patent Owner Cortex MCP, Inc. ("Patent Owner") submitted Patent Owner Responses that were accompanied by declarations from Dr. Sam Malek.

2. Although I am being compensated at my rate of $600.00 per hour for the time I spend on this matter, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding, any of the parties, or the Challenged Patents.

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

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

II. Materials Considered

5. In forming my opinions, I have reviewed and am familiar with the Challenged Patents, their Prosecution histories, and the other materials cited in my previous declarations and in this declaration. I have also considered the Patent Owner Responses and accompanying declarations of Dr. Malek. Since the arguments from Patent Owner and Dr. Malek that I address herein are essentially the same in each case, to avoid unnecessary clutter I cite to the Patent Owner Response in IPR2024-00486 ("486-POR") and Dr. Malek's declaration in that proceeding (EX2009) rather than providing parallel cites for all proceedings. In addition to the list of exhibits provided in my previous declarations, some of which I discuss below, I cite the following additional exhibits in this declaration.

Exhibit No.	Description
1047	Transcript of December 12, 2024, Deposition of Dr. Sam Malek with signed Errata Sheet
1049	U.S. Patent Pub. No. 2010/0217682 to Eric Chan ("Chan")
1050	Jerry Gao et al., "Understanding 2D-BarCode Technology and Applications in M-Commerce–Design and Implementation of A 2D Barcode Processing Solution," *31st Annual International Computer Software and Applications Conference* (2007) https://ieeexplore.ieee.org/document/4291101
1051	U.S. Patent Pub. No. 2014/0006277 to Raj Rao ("Rao")
1052	U.S. Patent No. 9.275,387 to Howard Spector et al. ("Spector")
1053	U.S. Patent Pub. No. 2013/0024371 to Hariramani et al. ("Hariramani")
1054	Supplementary high-resolution versions of the figures of Hariramani ("Hi-Res Hariramani")
1055	Archived copy of "Redactis," published by Integral Data Solutions and archived on May 11, 2008, by the Internet Archive's "Wayback Machine" https://web.archive.org/web/20080511201324/http://www.integralds.com/products/redactis/redactis.htm
1056	U.S. Patent No. 8,540,149 to Chun-Yu Chu ("Chu")
1057	U.S. Patent Pub. No. 2010/0017860 to Natsuki Ishida ("Ishida")

6. I have also relied on my education, skill, training, and experience in the relevant fields of technology. I have further considered the viewpoint of a person of ordinary skill in the art ("POSITA") in the subject matter of the Challenged Patents as of December 21, 2012.

III. Legal Principles

7. In forming my opinions for this declaration, I have applied the same legal principles that I described in my original declarations.

IV. Level of Ordinary Skill in the Art

8. I understand that Dr. Malek does not dispute the level of ordinary skill that I set forth in my original declaration. *See* EX2009, ¶¶37-41. I continue to apply that level of ordinary skill here.

V. Stafford's Key Signatures Are a "virtual representation of the credential"

9. I understand that the Board preliminarily disagreed that Stafford's key signatures satisfy the "virtual representation of the credential" limitation. In particular, the Board stated:

> At this juncture and on a preliminary basis, we do not agree with Petitioner that Stafford's hash values IdSig1 and IdSig2 "act[] as a virtual credential representation of the stored credential." *See* Pet. 61. Our reading of Stafford is that hash signatures are derived values from one-time pads, which may be used to encrypt the credential, but the pads do not appear to include any information related to the credential or its contents. Further, comparisons of derived hash values may lead to a location where a credential is stored in a secure location—but, our preliminary view is that any alleged "association" with the credential appears to be extremely attenuated, at best.

IPR2024-00486, Paper 8 ("486-ID") at 38-39. As I explain below, however, a POSITA would have viewed Stafford's key signatures as a virtual representation of the credential for multiple reasons.

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

information. *See* EX1012, ¶¶116-122. The key signatures act as a stand-in for the credential, much like the coat-check ticket in the analogy that I discussed above.

12. Even Dr. Malek acknowledges that the key signatures are a representation of the credential. In arguing against the rationale to combine Stafford and Purves, he states that "there is no reason in Stafford to remind a user **what documents are represented by IdSig 1 and IdSig 2**." EX2009, ¶164 (emphasis added). While I disagree with his arguments against the rationale (as I explain below), I agree with him that the underlying credential is "represented by" Stafford's key signatures.

VI. Stafford's Key Signatures Are "based on the information associated with the credential"

13. I understand that Patent Owner and Dr. Malek argue that Stafford's key signatures cannot be the recited OVER file because the key signatures supposedly are not "based on the information associated with the credential of the user." 486-POR, 52-54; EX2009, ¶¶131-48. I disagree with this argument since Stafford's key signatures are indeed "based on" the information associated with the credential in multiple ways. The language "information associated with the credential" is important. The information does not have to be from the credential, in the same sense that a coat-check ticket does not have to include part of the coat.

14. First, Stafford's key signatures are computed using information associated with the credential. While generation of the OVER file "based on"

information associated with the credential does not *require* that the OVER file be computationally derived from that information, Stafford's key signatures are nevertheless computed using information associated with the credential, including the OTP and its encrypted version (IdPad) as well as the user's private key.

15. Turning to the first example, the key signatures are computed using the OTP. *See* EX1012, ¶¶93-102 (IdPad created for release of particular credential information), 115-26 (eventual release of credential information tied to IdPad). Dr. Malek appears to disagree, asserting that "Stafford never teaches that IdSig1 and IdSig2 are in any way based on information associated with the credential" and that they are "are simply random numbers." EX2009, ¶¶135, 147. This is incorrect. IdSig1 is a hash computed from IdPad (an encrypted version of the one-time pad "OTP" used to encrypt the credential information), and IdSig2 is a hash computed from IdSecPad (an encrypted version of IdPad). EX1012, ¶¶46-48, 95, 99. The OTP, IdPad, and IdSecPad are tied to this particular credential information–e.g., the credential information is encrypted using the OTP, and the OTP/IdPad/IdSecPad are associated with the credential information in the system's datastores)—and are therefore information "associated" with the credential. *See id.*, ¶¶88, 93-95; *see also id.*, ¶¶57-59 (discussing storage of such information), 69 (credential information may include "digitized original documentation"), 118 (different IdSecPads correspond to "different parcels of information authorized for

release"). Moreover, hashes are not "simply random numbers" as Dr. Malek asserts. EX2009, ¶147. Rather, a hash is computed by applying a hashing algorithm to actual data. A POSITA therefore would have understood that IdSig1 and IdSig2 are computed by applying a hashing algorithm to IdPad and IdSecPad, respectively. The key signatures are therefore computed from information associated with the credential.

16. As another example, the OVER file is computed using the user's private key, which is another piece of information associated with the credential. As I explained above, the key signatures are computed from IdPad, which is itself computed by encrypting the OTP with the user's private key. EX1012, ¶95 ("The key or pad (PadKey1) used for the One Time Pad is encrypted with User_priv_key1, requested in Step 228, to create IdPad in step 230."), Fig. 2 (depicting blocks 228 and 230). The key signatures are therefore based on this private key. The private key is also used to decrypt the credential information during the release process and is therefore associated with the credential information. *Id.*, ¶74 ("Information is decrypted by the system using the User_priv_key1 provided by the entity to generate unencrypted IdFiles."). The private key is therefore "information associated with the credential" given its association with the credential information in this release process and in the datastores. *Id.*, ¶¶74, 95, Fig. 2; *see also id.*, ¶¶57 (staging zone includes credential

information and key data), 58 (secure zone stores "all credential information … and other associated data").

17. Dr. Malek treats the claims as requiring that the OVER file be based on the credential itself, but this misreads the claims. After discussing Stafford's key-signature-generation process, Dr. Malek argues that IdSig1 and IdSig2 are not "based on Stafford's credentials (IdFiles) at all." EX2009, ¶¶144-45. But the claims say that the generation of the OVER file is based on information "associated with" the credential, not based on the credential itself or its contents. As I explained above, the OTP/IdPad/IdSecPad and the user's private key are all pieces of information that is "associated" with the credential.

18. In any event, Dr. Malek is wrong in arguing that Stafford's key-signature generation is not "based on" the credential's contents. *See* EX2009, ¶¶144-45; *see also id.*, ¶147 (arguing key signatures are "not associated with any specific credential" but are instead "associated with a specific one-time release of information that may or may not contain any specific credential"). The credential's contents are still involved in the process for generating the credential even if they are not ultimately included in the resulting key signatures. The user submits various credential information/documents and selects one or more for release. EX1012, ¶¶57-58 (information storage), 63-70 (submission process), 72-79 (selecting items for release). The key signatures are generated based on the user's

selection of that information. *Id.*, ¶¶94-99. The key signatures are also specifically tied to the selected information and are required to obtain the credential's contents. *Id.*; *see also id.*, ¶¶75-79. For example, they are tied to and facilitate the release of "credential information" such as a bank account number or a credit card number. EX1012, ¶¶57, 81; *see also id.*, ¶¶74 (discussing release of "verified credential data"), 117 (discussing release of "credential information"), 133 (same). The released information itself (IdFiles) may even be "digitized original documentation." *Id.*, ¶69. Key-signature generation is therefore "based on" the credential's contents even though the resulting key signatures do not include the credential's contents.

VII. <u>Stafford's Key Signatures Have Been "verified by an issuing agency"</u>

19. I understand that Patent Owner and Dr. Malek argue that Stafford does not satisfy this limitation because it merely teaches verification of the credential's information, not direct verification of the key signatures. 486-POR, 54-55; EX2009, ¶¶153-57. Yet they point to an example in the specification that they say corresponds to the "verified by an issuing agency" limitation, and that example performs verification using the same type of credential-information check that Stafford discloses.

20. Patent Owner and Dr. Malek identify only one example in the specification as corresponding to the "verified by an issuing agency" limitation.

They argue that verification by an issuing agency in the specification is shown by a driver's license example starting in column 6 of each patent. 486-POR, 12-13; EX2009, ¶49. In the cited example, based on a user request that includes driver's license information such as the driver's license identification number, the system contacts an issuing agency database "to **verify the information contained in the OVER File generation request** and to obtain additional credential information." EX1001, 6:22-27 (emphasis added); *see also* EX1002, 6:35-40; EX1003, 6:42-46; EX1004, 6:48-53. For example, it may check the "driver's license identification number" that was included in the generation request. EX1001, 6:44-52; EX1002, 6:57-65; EX1003, 6:63-7:4; EX1004, 7:3-11. The database response indicates "the validity of the requested credential containing the driver's license identification number" and provides additional information such as a credential image and the person's name, address, and date of birth. *Id.* In other words, in the identified example of issuer verification, the specification does not state that the issuing agency directly examines the OVER file or the "virtual representation of the credential." Instead, according to Patent Owner and Dr. Malek, the virtual representation has been verified by the issuing agency to be an official representation of the credential because credential information was successfully checked against credential information in an issuing agency's database.

21. Stafford teaches this same type of check. The user "submits their credential information or documentation to the system." EX1012, ¶¶62-64. Verification can be performed in several ways, including "verification of document or data authenticity with a document's issuing body." *Id.*, ¶65; *see also id.*, ¶67 (information derived from document "verified as authentic"). In other words, as in the DMV example, which Patent Owner and Dr. Malek identify as corresponding to the "verified by an issuing agency" limitation, Stafford teaches communicating with the issuing agency to verify that the credential data supplied by the user is correct.

22. In any event, as I discuss in the following section, Purves also teaches issuer verification.

VIII. Purves Teaches Credential Images that Have Been "verified by an issuing agency"

23. I disagree with Patent Owner's argument that Purves does not teach issuer verification. Patent Owner argues that Purves "cannot satisfy the claim requirements for the virtual representation verified by an issuing agency" because it "does not disclose storing images or credit card information on a user device." 486-POR, 56; *see also id.*, 57 ("Absent the card image on the user device, Purves cannot possibly teach these claim requirements for a virtual representation that has been verified by an issuing agency."), 58 (repeating storage argument). Patent Owner's reasoning is that Purves does not teach other limitations involving

transmission of the OVER file to the client device and a scan of the OVER file. *Id.*, 56-57. But Patent Owner's analysis does not address the "verified by an issuing agency" limitation itself. Moreover, Patent Owner is not addressing the combination of Stafford and Purves, including Stafford's teachings of transmission to the user's device (EX1012, ¶¶93-105, Fig. 2) and Purves' teachings of performing a scan in place of other credential interactions such as NFC activations or card swipes (EX1013, ¶64, Fig. 3).

24. In any event, Patent Owner's assertion that Purves does not teach transmission or storage of the credential image on the user's device is simply wrong. Patent Owner argues that I admitted during my deposition that Purves does not teach transmitting the credential image to the user's device or local storage of the image on the user's device. 486-POR, 55-56 (citing EX2016, 114:5-11). This is incorrect. In the passage of the transcript cited by Patent Owner, I was not addressing transmission of the credential image, nor was I addressing storing generally. Instead, I was asked about Purves' express disclosure of the information being "permanently" stored on the user's device. I clarified this point in the preceding portion of the transcript that Patent Owner excludes from its citation:

> So, I think what you are asking is whether the information is permanently stored on the user device or whether the user simply can access it through the wallet server. Is that the question?
>
> Q. That is the question, yes.

EX2016, 113:17-22.

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.

26. To the extent Patent Owner is attempting to distinguish Purves by arguing that its storage may involve volatile memory such as RAM, this would be irrelevant since storage of the virtual representation in non-volatile storage is not required by the claims. In any event, this would not be a meaningful distinction since secure local storage of virtual-wallet data in non-volatile memory was well-known and conventional. *See, e.g.*, EX1049 (Chan), ¶24 ("As shown, the electronic wallet 148 may be configured to access storage means on a persistent store (e.g. flash memory 108 in FIG. 1) adapted to securely store data for one or more

payment cards (e.g. credit cards or debit cards 148A, 148B, 148C) issued to the user of wireless handheld device 100.”).

27. Patent Owner also argues that Purves’ image does not satisfy the Board’s construction of the OVER file because the image (i.e., the virtual representation) is not used to verify those credentials. 486-POR, 57-58 (“[T]he card image is used by the consumer to confirm the account being enrolled in a virtual wallet, not a third party seeking to verify a user’s credential.”). But in all of the Challenged Patents, verification in subsequent claim elements involves the OVER file, not the virtual representation specifically. While the OVER file “compris[es]” the virtual representation, I understand that the word “comprise” in a patent claim is open ended, meaning that the OVER file may encompass things other than virtual representation. This mirrors the Institution Decision’s statement that the OVER file “encompasses” a virtual representation of the credential (not that OVER file “means” a virtual representation, as Patent Owner states). 486-ID, 9; 486-POR, 57-58. A POSITA therefore would not have understood the claims to require that the virtual representation be used to verify the credential. In any event, Patent Owner does not dispute that the key signatures or the QR code are used for verification, so Patent Owner’s argument does not address the references’ combined teachings.

IX. A POSITA Had Reason to Combine Stafford and Purves

28. In the following sections, I address arguments made by Patent Owner and Dr. Malek as well as comments made by the Board regarding the rationale for combining Stafford and Purves.

A. Purves' Teachings Are Applicable to Stafford

29. Dr. Malek incorrectly argues that Purves' virtual wallet teachings are not applicable to Stafford's single-use items. Dr. Malek states that the differences between Stafford's and Purves' system precludes the combination, arguing that Stafford and Purves are "not related in any way" with Purves merely being a "payment system" whereas Stafford is merely a "document distribution system." EX2009, ¶160; *see also* 486-ID, 40 ("As Patent Owner points out, Stafford teaches the use of one-time key signatures, while Purves is directed to a virtual wallet with multiple payment accounts."). But Purves is not limited to payment transactions, nor is it limited to persistent, multi-use wallet items. For example, it teaches that its virtual wallet can include tickets, which are typically single-use items. EX1013, ¶¶54 (wallet may include tickets), 102 (discussing "other account types, including pre-paid accounts, reward accounts, savings accounts, and/or the like"); *see also* EX1012, ¶75 ("plane ticket" example in Stafford). Virtual wallets routinely included single-use items such as tickets or single-use payment tokens. E.g., EX1051 (Rao), ¶¶118, 164 (tickets, coupons, etc.); EX1052 (Spector), 48:23-49:36

(single-use payment token). Nor is Stafford limited to "document distribution," as Dr. Malek argues. For example, Stafford teaches that different types of credentials can be represented by key signatures, including those associated with payment accounts. EX1012, ¶¶53 (credential information may be "any type of information relating to an entity"), 73 (type of information depends on user's purpose), 81 (releasable items include "bank account numbers, credit card numbers etc."). Stafford also teaches that its process is applicable to "ecommerce related activities," including the communication of information to facilitate provision of goods and services. *Id.*, ¶¶106-109 (information submitted to provide "service or goods to the IdMember will depend on nature of the service or good"). While Stafford describes a specific example involving a loan application, Stafford's broader discussion of transmitting payment account information such as a credit card number (*id.*, ¶81) and the applicability of Stafford's techniques to ecommerce, including the provision of goods and services (*id.*, ¶¶106-109), indicates applicability to purchase transactions.

B. <u>The Combination Is Not "Nonsensical"</u>

30. Patent Owner and Dr. Malek's argument that the combination is nonsensical is based on their misunderstanding of Stafford. Dr. Malek states that "[b]ecause 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." EX2009, ¶164; *see also* 486-POR, 60-61 (similar argument). In other words, he assumes there is nothing for the user to keep track of because the key signatures are effectively "spent" before they are created. However, Dr. Malek is conflating the initial setup of information for release (a step during which the key signatures are generated and provided to the user) and the subsequent transfer of credential information to the third-party recipient (a step during which the user gives the third-party recipient the previously generated key signatures so the recipient can submit them to the system and obtain the credential information).

31. The user's initial selection of documents/information for release is separate from the user's selection of key signatures to be given to the third-party recipient. When the user initially selects documents/information for release, the system generates associated key signatures, sends those key signatures to the user, and moves the associated credential information to the secure staging zone. Stafford makes this clear when summarizing the initial release process:

> At this point in the release process, information that has been selected for release has been prepared for collection by the recipient/user of the information. In summary the following actions have occurred:
>
> 1 IdMember has received two key signatures IdSig1 and IdSig2. IdSig1 is a hash value of IdPad which has been encrypted by User_priv_key1. IdSig2 is a hash value of the IdSecPad

2 IdSecFiles2 have been moved to the Secure Staging zone

3 IdSecPad has been moved to the Secure Key Zone.

EX1012, ¶¶102-105. The transfer of key signatures to the third-party recipient is separate from the initial setup that results in the user receiving the generated key signatures. *Id.*, ¶31 & Fig. 2 ("process for preparing information"), ¶32 & Fig. 3 ("method of transmitting released data"). For example, Stafford describes scenarios in which the user "provides the information recipient with their MIN and key signatures IdSig1 and IdSig2 that have **previously been created in the release process**." *Id.*, ¶¶133-34.

32. Patent Owner's argument that the key signatures are supposedly generated after the user has determined who pays for the service is also incorrect. POR, 61 (quoting EX1012, ¶84). As an initial matter, the quoted passage of Stafford states that the user "can" be given the "option" of determining who pays for the service. EX1012, ¶84. But even if the system required the user to make this determination when setting up files/information for release, this still would not mean that the user never chooses key signatures to give to a third-party recipient 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 equally true if the user decides that the third-party recipient will pay for the

service. Indeed, the third-party recipient may not even be known in advance. *See, e.g.*, *id.*, ¶¶9 (same information may be released to various recipients), 129, 133 (user may have credential profiles to facilitate repeated release of the same set of credential information). Paying for Stafford's service upfront or having the third-party recipient pay later does not change the fact that the user may select which previously generated key signatures (potentially from among many) to give to a 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 presented with a listing of personal or sensitive information objects (e.g. a generic profile created earlier with a list of information objects and personal configurations or preferences of IdMember) from which he/she can select which data (or preselected set of data) to release."), 118 ("The IdMember's directory in the Secure Key Zone 120 may include multiple IdSecPad's corresponding to different parcels 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.

C. **Patent Owner's Arguments Against Credential Images Are Incorrect**

34. The combination involves using a credential image such as a representative image or an image with sensitive information obscured. Patent Owner and Dr. Malek attack both approaches, and I address their arguments below.

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 (Hariramani), Figs. 1A (element 102), ¶89 (discussing same), Fig. 4A (element

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.*, Fig. 17 (element 1717), ¶176 (discussing same), Fig. 22F (element 2284), ¶211 (discussing same), Fig. 60A (elements 6026, 6027), ¶352 (discussing same), Fig. 60B (element 6035), ¶354 (discussing same); EX1040 (Langley), Fig. 10A (virtual wallet displaying card with last four digits of PAN), ¶158 (describing same); EX1049 (Chan), ¶37 ("When displayed as selectable payment options, the card numbers could be fully revealed, partially hidden (e.g. 4500 XXXX XXXX 4742), or could simply be listed by the issuing institution's name (e.g. XYZ Bank VISA™ Credit Card)."). Moreover, Purves expressly teaches identifying items in the virtual wallet with the same type of information Dr. Malek argues a POSITA would not have included. EX1013, ¶¶85 (panel may display "image of the card (e.g., from the issuer), a nickname for the card, card identifier, card brand, and/or the like"), 122

[1] For clarity, higher-resolution versions of the figures of EX1053 (Hariramani) are included as EX1054. I understand that these higher-resolution figures were obtained from the USPTO's Patent Center website (under the "Supplemental Content" tab for the Hariramani patent application).

(using "template" image). A POSITA would have recognized that security was no less important in Purves' context than in Stafford's context since Purves' virtual wallet includes various sensitive credentials. Yet Purves still teaches associating wallet items with obscured or representative images. *See* EX1013, ¶122. Dr. Malek does not dispute this, nor does his declaration address Purves' use of encrypted transmissions to protect data. *See id.*, ¶¶131 (discussing cryptographic processors/transceivers), 143 (discussing cryptographic units), 152 (discussing secure web traffic using "HTTPS, SSL, and/or the like"), 157 (cryptographic server components allow for "encryption and/or decryption of provided data" including "both symmetric and asymmetric (e.g., Pretty Good Protection (PGP)) encryption and/or decryption"), Fig. 25. In my opinion, a POSITA would not have viewed following Purves' teachings as creating a meaningful security risk.

36. I also disagree with Patent Owner and Dr. Malek's argument that using an image with sensitive information obscured would have fatally undermined security. Dr. Malek's basis for this assertion is that that obscured data can supposedly be recovered or reconstructed from a blurred image using deconvolution techniques. EX2009, ¶167. But obscuring is not limited to blurring. 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 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."). Patent Owner and Dr. Malek thus chose a minimally blurred image rather than considering well-known obscuring techniques that would have been familiar to a POSITA. That is not how a POSITA would have approached the combination.

37. I understand that the Board also expressed concern regarding obscured images. In particular, the Board stated:

> Petitioner relies on Stafford's teachings relating to managing sensitive documents where extensive encryption is used to protect specific documents, and in this context, we question the rationale to add elements of Purves which could compromise the security of the key signature. These issues include, for instance, the addition of an image of the user's credential because, even with some obscured confidential information, this addition may add some risk to the secure handling of the key signature.

486-ID, 40. Respectfully, however, a POSITA would not have viewed the combination's use of obscured credential images as compromising the security of

the underlying documents (as I explained above), nor would it have risked exposure of the key signatures themselves since the image does not depict or otherwise convey the key signatures. And even if the combination's use of obscured images were a concern—and a POSITA would not have thought so—the combination also encompasses the use of a representative image. This type of generic image would help the user keep track of the items without including personal details and would not have undermined security in general or compromised the "secure handling of the key signature" in particular. 486-ID, 40.

38. Regarding the Board's comment that Stafford manages sensitive documents "where extensive encryption is used to protect specific documents" (486-ID, 40), security is similarly important in Purves' context since Purves manages sensitive credentials such as credit cards. EX1013, ¶85. Yet, as I explained above, Purves still teaches using credential images. This reflects the conventional understanding that sending an obscured credential image to the user's device was reasonable and sufficiently secure even for sensitive credentials. *Id.*, ¶122 (obscuring "protect[s]" confidential information).

39. Therefore, in my opinion, a POSITA would not have viewed the combination's use of credential images as introducing a meaningful security risk, certainly not a risk that would outweigh the substantial benefits. *See also infra*, §IX.E (benefits outweigh risks).

D. **Patent Owner's Arguments Against QR Codes Are Incorrect**

40. The arguments presented by Patent Owner and Dr. Malek against QR codes are flawed in numerous respects.

41. First, Dr. Malek makes a false distinction between QR codes and Stafford's one-to-one communications. Dr. Malek states that "[u]nlike email or text, QR codes are designed to disseminate information to different recipients (or the general public) using cameras," whereas "Stafford is not designed or intended to widely disseminate sensitive credentials, EX1012 (Stafford) ¶¶88-126, and using QR codes would only conflict with Stafford's extensive security protocols." EX2009, ¶175. But while disseminating information to different people (i.e., one-to-many communication) is *one* application for QR codes, QR codes are not limited to that application as Dr. Malek suggests. QR codes were also routinely used for one-to-one communication. *See, e.g.*, EX1040 (Langley), ¶¶92-93 (user device may display QR code to facilitate transaction with merchant rather than using NFC-based transmission), 171 (user displays QR code for merchant scan), Fig. 10D (depicting same); EX1050 (Gao), 3-5 (discussing use of QR codes in peer-to-peer and point-of-sale transactions for "more secure, efficient, and easy to

use payment solutions”).[2] Indeed, Purves itself teaches triggering one-to-one communication for a transaction using a QR code (rather than, e.g., a physical card swipe or NFC tap). EX1013, ¶64. Thus, just like email, text, and many other communication mechanisms, QR codes were known to useful for **both** one-to-one communications and one-to-many communications.

42. I also disagree with Patent Owner’s argument that QR-encoded key signatures would not work. Patent Owner points to an example in Stafford as the basis for arguing that using QR codes would not work regardless of whether encryption is used. 486-POR, 66 (citing EX1012, ¶¶97, 99); EX2009, ¶177. In the cited passage, Stafford describes how the user may obtain the generated key signatures (so that they can be given to the third-party recipient). Stafford gives two examples: (1) the user may copy the key signatures down from their display or (2) the user can receive them via email, in which case IdSig1 is encrypted with the

[2] This 2007 conference paper is available on IEEE Xplore at https://ieeexplore.ieee.org/abstract/document/4291101, and the IEEE Xplore website states that the paper was uploaded August 2007. This paper confirms my understanding, based on my experience in the field, that QR codes were well-known to be useful for secure one-to-one communications.

user's public key. According to Patent Owner, "neither option would work with a QR code." 486-POR, 66. I address each of these points in turn below.

43. Patent Owner argues that the first option (which Patent Owner characterizes as a "user sending an unencrypted QR code") would not work because it "would provide direct access to the key signatures, defeating Stafford's email encryption security protocol." *Id.*; EX2009, ¶176. As an initial matter, Patent Owner appears to suggest that the combination would involve the user "sending" the QR code to the third-party recipient. As I previously explained, however, the combination involves sending the QR code to the **user**. EX1005, ¶353. The user then presents the QR code image to the third-party recipient for scanning (which conveys the key signatures to the third-party recipient) according to well-known QR-code-scanning techniques. *Id*. In other words, the combination does not require the user to transmit the QR code to the third-party recipient's device, as Patent Owner implies.

44. Even if Patent Owner meant to address the server sending an encrypted QR code to the user, Patent Owner's reasoning has multiple flaws. Patent Owner states that this would "defeat[] Stafford's email encryption security protocol" (POR, 66), but the email example Patent Owner cites is just that: an example. Patent Owner itself acknowledges that this is an "option" in Stafford, not a requirement. 486-POR, 66. Indeed, Patent Owner implies that Stafford *does* teach

sending an unencrypted key signature as another option (*id.*), so it is unclear why Patent Owner views unencrypted QR-encoded key signatures as contradictory to Stafford. Regardless, Patent Owner also overlooks conventional techniques for securing data in transit via encrypted transmissions. Even if the QR code itself or the underlying key signatures were not encrypted by the server before transmission, unencrypted data objects were routinely secured during the transmission process via in-transit encryption (which was known to make intercepted transmissions computationally infeasible for an attacker to interpret). Purves itself teaches such encrypted transmissions. *E.g.*, EX1013, ¶157.

45. In arguing against the second "option," Patent Owner states that "[i]f the QR code was encrypted, the user could not present it to the recipient without also revealing the user's private decryption key, which would introduce a different security vulnerability in Stafford." 486-POR, 66. Dr. Malek makes a similar argument, though he addresses "a QR code encoding the encrypted IdSig1 and IdSig2 values" (i.e., QR-encoding of encrypted key signatures rather than encrypting QR-encoded key signatures). EX2009, ¶177. Patent Owner and Dr. Malek are both wrong. While the combination is not limited to Stafford's specific options for transmitting the key signatures—such as its email transmission of asymmetrically encrypted key signatures—encrypted QR codes (and QR codes of encrypted key signatures) would have been functional and secure in Stafford's

context. Given Patent Owner and Dr. Malek's different characterizations, I address each in turn below.

46. Contrary to Patent Owner's argument, using encrypted QR codes in the combination would have worked. As I previously explained, though a QR code is typically interpreted/displayed as an image, the QR-encoded data itself can be encrypted and decrypted just like any other data. In other words, encryption/decryption algorithms do not care how the underlying data is ultimately used: decrypting simply yields the pre-encryption data, whatever that may be. Asymmetric encryption, as in Stafford's example, is no different. Stafford describes conventional use of asymmetric encryption to securely communicate data to a particular user. *See* EX1012, ¶71 (system uses entity's public key for "secure communications between the system and the entity"). This is equally useful and feasible with QR-encoded data, as I discussed above. In other words, if an asymmetric encryption algorithm is used to encrypt data before sending it to the user (who decrypts the data with their private key), that same process can be used with QR-encoded data. For example, the QR-encoded data may be encrypted with the user's public key and sent to the user, who can then decrypt it with the corresponding private key to yield the original QR-encoded data (which can be presented to the third-party recipient for scanning as I previously discussed). The

third-party recipient does not need the user's private key in this scenario, as Patent Owner argues.

47. Contrary to Dr. Malek's argument, a POSITA also would have recognized that using QR codes of encrypted key signatures would work. Instead of addressing encryption of a QR code (i.e., QR encoding the key signatures first, then encrypting the QR-encoded data), as Patent Owner does, Dr. Malek discusses QR encoding of an encrypted key signature (i.e., encrypting the key signatures first and then QR encoding the encrypted data). In particular, Dr. Malek argues that a POSITA would have understood that "a QR code encoding the encrypted IdSig1 and IdSig2 values … would be utterly useless because the user could not present the QR code to the recipient without also providing the recipient with the user's private decryption key, which would also thwart Stafford's security protection for the user." EX2009, ¶177 ("Without that private decryption key enabling recovery of IdSig1 and IdSig2, the QR code encoding the encrypted hash values would be useless to the recipient.").

48. But even if the combination were limited to QR encoding of the already-encrypted key signatures, as Dr. Malek assumes, Dr. Malek is incorrect that this would require the third-party recipient to be given the user's private key. The third-party recipient in Stafford does not perform the analysis of the key signatures; rather, the recipient simply submits the key signatures to the system,

which then performs the analysis before releasing the credential. *E.g.*, EX1012, ¶¶115-122. What Dr. Malek appears to have overlooked is that, in Stafford, **the system has a copy of the private key**. EX1012, ¶¶68-69 (discussing user submission of private key), 74 ("At this stage the system requests for the member to submit their User_priv_key1 via a process explained previously."), 95-96 ("Transmission of User_priv_key1 to the system 100 is conducted within an SSL or similar secure method e.g. (dual authenticated SSL, SSH or other secure protocol."). Accordingly, there would be no need for the third-party recipient to be given the private key even in the implementation assumed by Dr. Malek. The third-party recipient would simply pass along the received key signatures to the central system, just as in Stafford alone.

49. Dr. Malek's point about QR codes not simplifying Stafford's email transmission is misplaced. He states that a POSITA "would not have used QR codes to simplify this already simple email transmission of encrypted codes and bypassed one of Stafford's security protocols (encryption of the hash values) to accomplish it." EX2009, ¶176. I addressed the flawed basis of Dr. Malek's comment regarding the supposedly "bypassed" security protocol above. As to his point about "simplify[ing]" the email transmission, Dr. Malek appears to misunderstand the combination. The email in Stafford's example is used to send the key signatures **from the system to the user**, not to the third-party recipient. On

the other hand, the QR-code-mediated communication in the combination simplifies the conveyance of the key signatures **from the user to the third-party recipient**. For example, a POSITA would have recognized that allowing the third-party recipient to simply scan a QR code to obtain the signatures is much easier and less error-prone than having the third-party recipient manually enter the key signature characters. Dr. Malek therefore is not addressing the stated combination or its benefits.

50. I understand that the Board also expressed concerns regarding the use of QR codes in the combination. In particular, the Board stated, "QR encoding the key signature would entail the additional storage of QR encoded key signature data, with associated additional risk to key signature security." 486-ID, 40. Respectfully, however, a POSITA would not have viewed the combination's use of QR codes as introducing a meaningful security risk to key signature security. Stafford already teaches storing key signatures on the user's device (since it describes displaying the key signatures on the user's device, which involves storage at least in transient memory such as RAM, or emailing the key signatures to the user). EX1012, ¶97. Storing QR-encoded key signatures is just as secure as storing non-QR-encoded key signatures. QR codes are a simply a different way of encoding data, and an attacker is no more or less able to hack a user's device and gain access to QR-encoded key signatures in the device's memory than non-QR-

encoded key signatures in the device's memory. QR codes were routinely used to encode sensitive information, and it was well known that the same security mechanisms used to protect data generally (e.g., encryption) are applicable to QR-encoded data. *See, e.g.*, EX1043 (Hammad), ¶¶53 (discussing encryption of QR code), 61 (discussing QR encoding of encrypted data); EX1057 (Ishida), ¶42 (discussing QR encoding of encrypted data); EX1056 (Chu), 1:5-50 (discussing barcode/QR code background, including use of QR codes for data transfer and use of encryption with QR codes), 2:62-65 (discussing encrypted message QR code); EX1043 (Hammad), ¶60 (discussing use of QR code "embedding the PAN").

51. As with storage, transmitting QR-encoded key signatures to the user's device would have been just as secure as transmitting non-QR-encoded key signatures to the user's device. A POSITA would have understood that security mechanisms for transmitting non-QR-encoded data are equally applicable to transmitting QR-encoded data. This includes email transmission of asymmetrically encrypted data, as in Stafford's optional example (EX1012, ¶97), or other typical forms of encrypted transmissions. Moreover, as I explained in the previous section, Purves also teaches encrypting transmissions to secure the data in-transit. EX1013, ¶¶131, 143, 152 (discussing secure web traffic using "HTTPS, SSL, and/or the like"), 157 (cryptographic server components allow for "encryption and/or

decryption of provided data" including symmetric and asymmetric encryption/decryption), Fig. 25.

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.

53. Thus, at every stage of the process—including transmission of the key signatures from the server to the user's device, storage on the user device's memory, and the conveyance of the key signatures from the user to the third-party recipient—the combination is just as if not more secure than Stafford itself.

54. Therefore, in my opinion, a POSITA would not have viewed the combination's use of QR codes as introducing a meaningful security risk, certainly not a risk that would outweigh the substantial benefits. *See also infra*, §IX.E (benefits outweigh risks).

E. **The Combination's Substantial Benefits Outweigh Any Actual Security Concerns**

55. In addition to wildly exaggerating security risks, or inventing them altogether, Patent Owner also never gets around to weighing security risks against convenience and error-reduction, as a POSITA would have. Instead, Patent Owner treats the combination as if it has no benefits based on the mistaken arguments that there is nothing for the user to keep track of with credential images and that using QR codes breaks Stafford's operation. *Supra*, §§IX.B, IX.D. With those mistakes corrected, it is clear that a POSITA would have viewed the benefits of the combination as vastly outweighing any corresponding security risk.

56. Patent Owner argues that the combination is nonsensical and introduces catastrophic security problems, but as I previously explained, those arguments are based on misapprehensions of the references, misapprehensions of the combination that was actually proposed, and a failure to consider the POSITA's familiarity with conventional security techniques. *Supra*, §§IX.A-D. Conventional security techniques were viewed as providing sufficient protection, even for sensitive information such as financial data, as I explained above. *Supra*,

§IX.C-D. There is nothing about the use of these conventional security techniques in combination with Stafford's teachings that would have made them any less effective.

57. Patent Owner's arguments also do not consider the importance to a POSITA of the system being user-friendly and less susceptible to user error. As I explained in my original declarations, a POSITA would have expected the application of Purves' teachings in combination with Stafford to provide these benefits and therefore would have been motivated to make the combination. For example, a POSITA would have recognized that having users and third-party recipients deal directly with raw key signatures, as disclosed in Stafford, was far from ideal in terms of convenience and the potential for user error. The substantial benefits of the combination in this respect would have been viewed as a significant improvement that would easily outweigh any actual security concerns associated with credential images and QR codes. That is why credential images were commonly used to manage even sensitive credentials and QR codes were commonly used to transfer sensitive data, as Purves itself demonstrates. EX1013, ¶¶64, 122. A POSITA thus would have recognized that any actual security risks associated with the combination's use of representative credential images would have been reasonably mitigated by standard data security techniques and greatly outweighed by the vast improvements in terms of convenience and usability.

X. Concluding Statement

58. Relying on my education, experience, skill, and training in the relevant field of art, and after reviewing the materials identified above, it is my opinion that all claims of the Challenged Patents are unpatentable.

XI. Jurat

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

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

Executed on February 3, 2025.

By: Michael Ian Shamos

Michael Ian Shamos