

Filed on behalf of: Visa Inc.

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

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

Case No. IPR2024-00486
Patent No. 9,251,531

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. Claim Construction.....	1
A. “OVER file”	1
B. “scan”/“scanned”	2
C. “verified by an issuing agency”	2
III. Visa Has Met Its Burden for the Osborne Grounds.....	3
A. Visa Showed that the Recited Virtual Representation Was Obvious in View of Osborne	3
1. The POR Confirms that Osborne Discloses a Virtual Representation “verified by an issuing agency”	3
2. PO’s Argument Against Obviousness Fails	4
3. PO Fails to Undermine Dr. Shamos’s Testimony	6
B. Visa Showed that Osborne Teaches the OVER Engine	7
C. Visa Showed that the Dependent Claims Were Obvious.....	8
1. Claim 2.....	8
a. Generating a Second OVER File Was Obvious.....	8
b. The “invalid for use” Limitation Was Obvious.....	10
2. Claims 7 and 20.....	11
3. Claims 8 and 29.....	13
4. Claims 12-13.....	13
5. Claim 19.....	14
6. Claims 23-26 and 28-33.....	15
IV. Visa Has Met Its Burden for the Stafford Grounds.....	16
A. The Combination Satisfies the Recited “OVER File”	16
1. The Combination Teaches the Recited Virtual Representation.....	16
a. Stafford’s Key Signatures Are a “virtual representation of the credential”	16

b.	PO’s “based on” Argument Fails	18
c.	PO’s “verified by an issuing agency” Argument Fails.....	19
2.	PO’s Arguments Against Purves Fail	19
a.	PO’s Storage Argument Fails	19
b.	PO’s Verification Argument Fails.....	20
B.	A POSA Had Reason to Combine Stafford and Purves.....	21
1.	PO Misunderstands the Combination	21
2.	The Combination Does Not Undermine Security.....	23
a.	PO’s Arguments Against Images Are Unconvincing.....	23
b.	PO’s Arguments Against QR Codes Are Unconvincing.....	25
3.	PO Fails to Weigh the Combination’s Benefits.....	27
V.	Conclusion	28
VI.	Certificate of Compliance.....	29
VII.	Appendix–Petitioner’s Updated Exhibit List	30

I. INTRODUCTION

Patent Owner (“PO”) fails to rebut Visa’s showing that all claims were obvious. PO attacks Visa for not licensing PO’s patents (POR, 1-5), but this baseless smear is irrelevant to the claims’ unpatentability. Regardless, the references refute PO’s arguments at every turn. PO claims Visa copied PO’s “innovative solution” of using tokenization (*id.*), but tokenization predates PO’s patents. PO touts the patents’ issuance due to the “verified by an issuing agency” limitation (*id.*, 7-8, 10-30, 54-60), but the sole embodiment of this limitation that PO identifies in its specification mirrors what the references already taught. PO alleges problems with the Stafford-Purves combination (*id.*, 60-66), but each is belied by the evidence.

II. CLAIM CONSTRUCTION

A. “OVER file”

PO urges confirmation under the Board’s preliminary interpretation but does not dispute VISA’s construction. POR, 9; *see also* EX1047, 28:25-30:6 (Dr. Malek admitting he did not apply VISA’s constructions or opine on proper construction of any term). The Board preliminarily determined that the OVER file “encompasses a virtual representation of one or more credentials, to be used for verification of those credentials” and that Osborne’s tokens qualify as OVER files. IPR2024-00486, Paper 8 (“486-ID”), 9-10. PO treats this as requiring that the

virtual representation itself (not merely the OVER file) be used for verification of the credential, but the claims impose no such requirement. POR, 57-58. For example, verification in subsequent claim elements involves a scan associated with the OVER file, and while the OVER file “compris[es]” the virtual representation, it may encompass other things. EX1047, 30:16-31:24; EX1048, ¶27.

B. “scan”/“scanned”

PO states that no construction is necessary but does not dispute Visa’s construction or the references’ teachings of the recited scan. POR, 9.

C. “verified by an issuing agency”

PO argues that an example in the specification corresponds to this limitation. POR, 12-13 (citing EX1001, 6:22-27, 6:44-52). In this example, the OVER engine checks a driver’s license number against the DMV’s database. EX1001, 6:22-47. The database’s response includes additional information (e.g., a name/address and credential image) and indicates “the validity of the requested credential.” *Id.*, 6:47-54. PO thus admits that a virtual representation of the credential may be “verified by an issuing agency” by checking credential data against an issuing-agency database. Dr. Malek made similar admissions. EX1047, 37:24-41:1 (limitation encompasses “some kind of check”), 41:2-22 (issuer need not send verification message). These admissions confirm that the references satisfy this limitation. *Infra*, §III.A.1.

III. VISA HAS MET ITS BURDEN FOR THE OBOBNE GROUNDS

A. Visa Showed that the Recited Virtual Representation Was Obvious in View of Osborne

Visa showed that a virtual representation “verified by the issuing agency” is disclosed or rendered obvious by Osborne. 486-Pet., 21-23; *see also id.*, 23 (claims also satisfied under credential-validation interpretation). PO’s response to the first argument imposes an unrecited requirement and inadvertently admits that Osborne satisfies this limitation. POR, 12-16. PO’s additional arguments fail at every turn. *Id.*, 16-30.

1. The POR Confirms that Osborne Discloses a Virtual Representation “verified by an issuing agency”

PO has no meaningful rebuttal to Osborne’s teaching that the issuing agency may operate the token server, in which case a POSA would have understood that the issued tokens have been “verified by the issuing agency.” 486-Pet., 22-23. PO argues that this does not teach “the claimed ‘issuing agency’ verification step” (POR, 14-15), but the limitation is a characteristic, not a separately recited “step.” Regardless, Visa explained that the issuer “verifies” that the token is an official representation of the credential by generating the token and providing it to the user. 486-Pet., 22-23; EX1005, ¶¶240-42.

PO also inadvertently concedes Osborne teaches this limitation by admitting that the virtual representation has been “verified by the issuing agency” if

credential data was checked against an issuing-agency database. *Supra*, §II.C; POR, 12-13. Yet Osborne teaches this same type of check. For example, Osborne teaches obtaining “assurance” of sufficient funds from the issuer for pre-funded tokens. EX1011, ¶47 (such tokens deemed “pre-authorized”) (cited at 486-Pet., 22). Confirming funds in an account would of course involve checking account information (e.g., an account number). Osborne similarly teaches checking credential data against issuer records when adding new cards. EX1011, ¶108 (“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.”) (cited at 486-Pet., 33-34). Osborne thus teaches the same type of verification PO admits is encompassed by this limitation.

2. PO’s Argument Against Obviousness Fails

PO argues that Visa presents an unsupported “common sense” argument to supply a missing limitation. POR, 16-17; *see also id.*, 27-29 (alleging burden-shift). This mischaracterizes Visa’s obviousness case, which is grounded in Osborne’s teachings and the POSA’s understanding of logical reasons for issuer verification. Regardless, PO’s arguments against obviousness defy credulity, particularly given PO’s claim-scope admission.

The petition does not rely on “common sense” to supply a missing limitation. PO argues that common sense cannot be used as a “wholesale

substitute” for analysis and evidence. POR, 17, 21-22 (citing *Arendi S.A.R.L. v. Apple*, 832 F.3d 1355, 1362 (Fed. Cir. 2016)). But Visa’s obviousness analysis is grounded in Osborne’s teachings. 486-Pet., 21-23; *supra*, §III.A.1.

PO’s nonprecedential Board decisions are equally inapposite. POR, 17. The decisions fault petitioners for baselessly proposing numerous complicated changes, whereas Visa explains the POSA’s straightforward understanding of Osborne’s disclosure. 486-Pet., 21-23; *Apple Inc. v. Contentguard Holdings, Inc.*, IPR2015-00453, 2015 WL 4467403, at *8 (PTAB 2015); *Vermeer Mfg. v. Toro Co.*, PGR2020-00081, 2021 WL 972419, at *13 (PTAB 2021). Discussing routine practice does not transform obviousness grounded in a logical understanding of Osborne into a common-sense theory.

Even if Visa were supplying a missing limitation with common sense—and it is not—PO’s attempt to make verification seem complicated is unconvincing. The alleged history and complexity of payment systems generally are red herrings since they do not address the characteristic at issue. POR, 19-20.

Ultimately, PO’s argument does not pass the smell test. Even setting aside Osborne’s express teachings (*supra*, §III.A.1) and the myriad logical reasons for verifying tokens (EX1005, ¶¶240-41), PO’s suggestion that the token server would provide tokens **without even checking that they correspond to a valid credential** defies credulity. Even PO’s expert was unwilling to endorse this view.

EX1047, 46:11-49:1 (evasive responses regarding issuance of unverified tokens), 50:20-51:7 (linking token to valid account “possibly” desirable).

3. PO Fails to Undermine Dr. Shamos’s Testimony

Visa’s obviousness analysis is supported by Dr. Shamos’s multifaceted explanation of why unverified tokens would have been problematic and the POSA’s logical interpretation of Osborne. EX1005, ¶¶238-42. Unable to refute Dr. Shamos’s points, PO deflects and mischaracterizes.

PO does not dispute Dr. Shamos’s point that issuer verification increases confidence that the token legitimately represents the credential. EX1005, ¶241. Instead, PO claims that it cannot tell whose confidence is increased. POR, 22. But Dr. Shamos addressed concerns “for both issuers and users.” EX1005, ¶241. PO dismisses Dr. Shamos’s point as unsubstantiated by ignoring his previous citations to Osborne. EX1005, ¶¶240-42 (citing EX1011, ¶¶29, 47-48, 53, 58); EX1011, ¶47 (obtaining “assurance” of sufficient funds). Dr. Malek’s evasiveness regarding customer frustration with unverified tokens confirms Dr. Shamos’s veracity. EX1047, 49:2-11, 51:9-21.

PO’s attempt to dismiss problems caused by unverified tokens in the marketplace is equally unconvincing. PO says Dr. Shamos’s explanation of this problem does not address Osborne’s system (POR, 23), but Osborne supplies tokens in the marketplace. EX1011, Title, Abstract.

PO claims Dr. Shamos acknowledged that unofficial tokens were not problematic because customers can prove their identity during each transaction. POR, 3, 22-24 (citing EX1005, ¶¶118, 120); EX2009, ¶¶88-99. But in the quoted background testimony, Dr. Shamos discusses user authentication, not token verification. EX1005, ¶¶118, 120. Dr. Malek sought to blur the distinction between these types of security measures, citing examples of alleged “verification” in Osborne, but subsequently admitted they are all user authentications. EX2009, ¶83 (citing EX1011, ¶26); EX1047, 56:4-9, 62:12-24. Even if PO were not conflating different issues, Osborne refutes PO’s assumption that only one security technique can be used. EX1011, ¶26 (user authentication provides “additional” security).

B. Visa Showed that Osborne Teaches the OVER Engine

PO unconvincingly argues that Visa fails to identify the OVER engine in Osborne. POR, 30-33. The petition shows that the PPT’s token server satisfies all requirements of the OVER engine. PO attempts to sow confusion by selectively editing the petition, claiming it says “Osborne ‘discloses the recited OVER engine’ because ‘this [PPT] apparatus generates and verifies OVER files.’” POR, 30. But the unaltered sentence reads “**[a]s addressed in more detail below for elements 1.3 and 1.6,** this apparatus generates and verifies OVER files” (Pet., 18 (emphasis added)), and the cited discussion explains how the PPT’s **token server** satisfies

these elements. *Id.*, 21, 27-29. PO’s double-counting accusation is based on the same mischaracterization of Visa’s OVER-engine mapping. POR, 31-33.

PO attempts similar sleight of hand with Dr. Shamos’s testimony, claiming he could not identify the OVER engine in Osborne. POR, 31. But his explanation that “it depends on the implementation” reflects Osborne’s disclosure of different server configurations. *E.g.*, EX1011, ¶¶47-48 (various entities may operate token server), 117 (term server “refers generally to a computer, other device, program, or combination thereof...”).

C. Visa Showed that the Dependent Claims Were Obvious

1. Claim 2

PO disputes Visa’s showing regarding (1) generating a second OVER file and (2) the second OVER file being invalid for use on the first device. POR, 35. Both arguments fail.

a. Generating a Second OVER File Was Obvious

PO argues Osborne does not teach multiple devices and that, regardless, a second device would reuse the first token. POR, 36-38. Neither assertion withstands scrutiny.

PO argues Visa relies on “common sense” for users having two devices and cites Dr. Malek’s assertion that Osborne does not disclose multiple devices. POR, 36-37; EX2009, ¶¶104-05. But the petition identified express disclosure of “a

user's devices,” and Dr. Malek now admits he was wrong. 486-Pet., 32; EX1011, ¶¶26, 29, 116, 148; EX1047, 9:13-10:24.

PO's speculation of other possible implementations is legally and factually flawed. PO argues that the system could reuse the first token on a second device rather than generating a second token. POR, 37; *see also* EX1047, 9:13-10:24 (Dr. Malek's similar assertion). But this ignores Osborne's disclosure of device-specific tokens. 486-Pet., 32; EX1011, ¶47 (token includes single device fingerprint); *see also id.*, ¶26, 29, 148, Fig. 2B. Possible alternatives do not undermine Visa's showing that the claimed approach was obvious. *ACCO Brands Corp. v. Fellowes, Inc.*, 813 F.3d 1361, 1367 (Fed. Cir. 2016) (“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.”); *see also Honeywell Int'l, Inc. v. 3G Licensing, S.A.*, 124 F.4th 1345, 1355-56 (Fed. Cir. 2025) (even preferred alternative would not refute motivation).

PO falsely claims Dr. Shamos admitted that reusing the first token was the logical approach. POR, 37 (citing EX1005, ¶55). The cited testimony addresses providing the first token for the first device, not providing a token for the second device. EX1005, ¶55; *see also id.*, ¶292. Dr. Shamos's actual testimony (that device-specific tokens were conventional) and Osborne's disclosure of device-

specific tokens stand unrebutted. EX1005, ¶¶213-18 (citing EX1014, ¶75; EX1042, ¶66); EX1011, ¶47.

b. The “invalid for use” Limitation Was Obvious

PO resorts to mischaracterization in accusing Visa of a hindsight-driven modification to make the second token “invalid for use” in the first device. POR, 38-42. PO claims Visa relies on a modification (POR, 38), but the petition applies a straightforward interpretation of Osborne’s teachings (e.g., tying the token to a particular client fingerprint). 486-Pet., 32; EX1011, ¶¶26, 47; *supra*, §III.C.1.a; *see also* IPR2024-00488, Paper 7 at 35 (recognizing sufficiency of Osborne’s teachings for similar limitation in related patent). Regardless, Visa’s analysis is grounded in Osborne and the POSA’s perspective, not hindsight. 486-Pet., 32; EX1005, ¶¶254-55. PO claims Osborne only uses fingerprints to restrict devices to particular users (POR, 39), but Osborne teaches tying the token to a single client fingerprint (EX1011, ¶47) and using that fingerprint for authentication (*id.*, ¶26). PO claims Visa never argued that Osborne contemplates multiple devices or using a fingerprint to make the token invalid on other devices (POR, 39), but the petition belies this assertion. 486-Pet., 32; *supra*, §III.C.1.a. PO repeats its false claim—debunked above (*supra*, §III.C.1.a)—that Dr. Shamos admitted that the system would reuse the first device’s token for the second device. POR, 40-41 (citing EX1005, ¶55).

PO also baselessly disparages Dr. Shamos as having a “lack of imagination” because he supposedly overlooked the possibility of using device fingerprinting in other ways (e.g., a mismatched token could trigger additional authentication). POR, 40-41; EX2009, ¶114. But PO’s imagining of other possible approaches does not undermine the obviousness of the recited approach. *ACCO*, 813 F.3d, 1367; *Honeywell*, 124 F.4th, 1355-56. Regardless, even in PO’s imagined implementation, the second token is still “invalid for use” in the first device “for authenticating the user,” as recited, since the mismatched token requires a different authentication mechanism.

2. Claims 7 and 20

The petition demonstrated that it was obvious for the credential information to “indicate a reason for the invalid credential” in view of Osborne’s disclosure, routine practice, and the POSA’s logical interest in avoiding confusion. 486-Pet., 36. PO responds with conclusory denials and deflection.

PO offers no meaningful response to Osborne’s teaching of indicating the reason for the invalid credential (e.g., a response indicating lack of funds or too many authorization attempts). 486-Pet., 36 (citing EX1011, ¶72). PO insists this is insufficient but does not explain why. POR, 43-44. The claims do not require that the credential information indicate the reason in a particular way, so PO’s complaint is unclear.

PO baselessly dismisses Visa's obviousness case and Dr. Shamos's testimony as conclusory and unsupported. POR, 42-43. This ignores Visa's discussion of Osborne and Dr. Shamos's corroborated testimony. 486-Pet., 36. Dr. Shamos cited his background discussion, starting at ¶219, showing that the recited indication was commonplace, and he explained the reason for this conventional approach. EX1005, ¶¶264-65; *see also id.*, ¶¶219-27 (citing, *inter alia*, EX1032, 88; EX1040, 125; EX1044, ¶46).

Rather than engaging with Visa's evidence, PO offers uncorroborated speculation. PO cites Dr. Malek's unsupported claims that a user "may be embarrassed" by an indication and could "likely" figure out the reason without an indication. POR, 43 (citing EX2009, ¶¶119-20). But unsubstantiated conjecture does not outweigh Osborne's teachings or Dr. Shamos's corroborated testimony. EX1011, ¶72; EX1005 ¶¶219-27, 264-65; *Honeywell*, 124 F.4th at 1354 n.6 (testimony contradicted by record not entitled to weight). PO also cites Dr. Malek's unsubstantiated claim that transactions today are routinely denied without explanation (EX2009, ¶119), but possible alternatives do not refute Visa's showing that the recited approach was obvious. *ACCO*, 813 F.3d, 1367; *Honeywell*, 124 F.4th, 1355-56.

3. Claims 8 and 29

PO fails to rebut Visa's showing that generating "a reference to a remotely stored credential" was obvious. PO argues that Osborne teaches remote storage of programs, not data. POR, 44-45 (citing EX1011, ¶133). This misreads Osborne (which is not limited to local data storage) and treats Visa's argument as anticipation rather than obviousness. 486-Pet., 37; EX1011, ¶133. PO's narrow reading is further refuted by Osborne's discussion of distributed databases. EX1011, ¶¶147-150, Fig. 15. Moreover, Dr. Shamos's obviousness reasoning based on the conventional nature of remote credential storage is unrefuted. EX1005, ¶266; *see also id.*, ¶¶61 (discussing claim 8 and citing background discussion beginning at ¶121), 121-22 (citing EX1019). PO argues that this is a distinct theory that cannot be incorporated by reference (POR, 45), but obviousness is viewed from the POSA's perspective, which includes familiarity with conventional practice. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 417-18 (2007).

4. Claims 12-13

PO falsely accuses Visa of inconsistent mappings for the "credential identifier" in the generation request. PO argues (1) that the petition switches its credential-identifier mapping from an account number in claim 11 to a token identifier in claims 12-13 and (2) that the token identifier is not part of the generation request. POR, 46-47. Both arguments fail for the same reason: as the

petition showed, credentials in the requested token may be tokens themselves, in which case the “account” is referenced by a token identifier. 486-Pet., 38-39; EX1011, ¶¶25, Fig. 1B (token associated with multiple accounts), 40 (requests includes account identifiers), 47 (account #2 identified by token identifier).

5. Claim 19

Faced with Purves’ express teaching of including a “credential image,” PO argues that (1) Visa ignores “security concerns” and (2) Purves does not teach image storage on the user’s device. POR, 48.

PO’s security argument is vague, unsubstantiated, and wrong. PO does not say what the alleged “security concerns” are, claiming only that Dr. Shamos admitted that sending images would create problems. POR, 48 (quoting EX2016, 109:11-12). But Dr. Shamos was referring to security concerns associated with giving “all the card information” to a separate organization, not sending credential images to user devices. EX2016, 108:13-109:15. Regardless, as explained below for the Stafford grounds, sending credential images does not create security problems. *Infra*, §IV.B.2.

PO’s storage argument fares no better. PO claims Dr. Shamos admitted that Purves lacks disclosure of storing images on user devices. POR, 48 (citing EX2016, 114:5-11). But PO does not explain how “storage” relates to claim 19. Moreover, Dr. Shamos was addressing disclosure of “permanent” storage in one

embodiment, not storing credential images on user devices generally. EX2016, 112:1-114:11. Dr. Malek also admits that Purves teaches storing credential images on user devices. *Infra*, §IV.A.2.a; EX1047, 69:16-71:18 (admitting storage in RAM). Regardless, the combination includes the image with Osborne’s token, and PO does not dispute that Osborne’s user device stores the token. *Palo Alto Networks, Inc. v. Centripetal Networks, LLC*, 122 F.4th 1378, 1386 (Fed. Cir. 2024) (arguments attacking references individually lack merit).

6. Claims 23-26 and 28-33

PO claims Visa never proposed combining Purves’ “request” for the credential with Osborne. POR, 49. But the rationale refers to generating/storing new credentials “as addressed for claims 22 and 23” (which encompasses requesting the credential) and explains the applied teachings’ usefulness for adding credentials to Osborne’s wallet. 487-Pet., 35; *see also id.*, 36-37 (requesting credential part of process for adding credential); *Gen. Elec. Co. v. Raytheon Techs. Corp.*, 983 F.3d 1334, 1351-52 (Fed. Cir. 2020) (requiring separate motivation for each element “unduly dissects prior art references into collections of individual elements”). PO claims Visa does not explain *why* the request would be useful. POR, 49. But the rationale includes reasoning PO never addresses, let alone refutes. 487-Pet., 35 (discussing examples of usefulness and explaining predictable results of combining known elements).

IV. VISA HAS MET ITS BURDEN FOR THE STAFFORD GROUNDS

Visa's showings for Grounds 5-6 are largely undisputed. PO challenges only (1) that the Stafford-Purves combination teaches certain aspects of the "OVER file" and (2) the rationale to combine. POR, 51. Both arguments fail.

A. The Combination Satisfies the Recited "OVER File"

The OVER file taught by the Stafford-Purves combination includes key signatures and a credential image, both of which are a "virtual representation of the credential." 486-Pet., 61-63. The Board preliminarily disagreed with the key-signature mapping but did not express disagreement with the credential-image mapping beyond questioning the rationale to combine. 486-ID, 38-40. PO purports to agree with the Board but addresses different limitations, arguing that Stafford's key signatures are not "based on the information associated with the credential of the user" or "verified by an issuing agency." POR, 51-55. PO also attacks Purves individually. As explained below, both "virtual representation" mappings satisfy the claims, and PO's arguments are incorrect.

1. The Combination Teaches the Recited Virtual Representation

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

The Board questioned whether the key signatures are a virtual "representation" of the credential because the key signatures "do not appear to

include any information related to the credential or its contents.” 486-ID, 38-39. Respectfully, however, this is not required by the claims, and PO’s expert admits that Stafford’s key signatures represent the credential.

The claims do not impose content or formatting requirements on the virtual representation. Dr. Malek admits that “virtual representation” has its plain meaning, that “virtual” means electronic/digital, and that he did not consider whether the “representation” must depict the credential or have particular formatting. EX1047, 31:25-34:5. Dr. Shamos confirms that a “representation” need not look like or include content from the thing it represents. EX1048, ¶¶9-10. Much like a coat-check ticket “represents” the coat even though it does not look like or describe the coat, the virtual representation may represent the credential even though it does not look like the credential or describe its data. *Id.*, ¶10.

It is undisputed Stafford’s key signatures satisfy the plain meaning of a “virtual representation of the credential.” Like a coat-check ticket, the key signatures act as a stand-in for the credential and are used to retrieve credential information. 486-Pet., 61; EX1012, ¶¶116-122; EX1048, ¶¶11-12. PO disputes other limitations but not the “virtual representation” language itself. POR, 51-55 (addressing “based on” and “verified” limitations). Nor could it since PO’s expert admits that the underlying documents “are represented by IdSig1 and IdSig2.” EX2009, ¶164.

b. PO's "based on" Argument Fails

PO argues that the key signatures are not "based on the information associated with the credential of the user." POR, 52-54. This argument fails for multiple reasons.

First, PO cannot refute obviousness by attacking the references individually. *Palo Alto Networks*, 122 F.4th at 1386. The OVER file in the combination also includes a credential image (Pet., 61-63), which PO does not dispute is generated "based on the information associated with the credential of the user."

Regardless, Stafford's key signatures are generated based on the information associated with the credential in multiple ways. They are derived as a result of a request to release the credential information, and they are specifically tied to the credential information and facilitate its release. 486-Pet., 57-61 (citing, *inter alia*, EX1012, ¶¶57-58, 62, 73-79, 81, 93-95); *see also* EX1048, ¶¶13-16 (citing EX1012, ¶¶46-48, 57-59, 63-70, 72-79, 81, 88, 93-102, 117-18, 133, Fig. 2). Additionally, while "based on" does not require computational derivation, as PO argues (POR, 52-53), Stafford's key signatures are computed from information associated with the credential. As PO admits, IdSig1/IdSig2 are computed from IdPad/IdSecPad (IdPad being the one-time pad ("OTP") encrypted with the user's private key). POR, 53-54 (citing EX1012, ¶¶47-48, 95, 99). OTP, IdPad, IdSecPad, and the private key are all information "associated" with the credential

due to their association with the credential in the release process and in the system's datastores. EX1012, ¶¶57-58 (stored credential information and other associated data), 74 (credential information decrypted with private key); 486-Pet., 58-59 (citing same); EX1048, ¶¶17-18.

c. PO's "verified by an issuing agency" Argument Fails

PO argues that the issuing agency checks the credential's information rather than the key signatures. POR, 54-55. But PO elsewhere admits that this limitation encompasses checking the credential's information. *Supra*, §§II.C, III.A.1; POR, 12-13. Stafford thus teaches the same type of check PO admits is encompassed by this limitation. EX1012, ¶¶62, 65, 67; 486-Pet. 61 (citing same); EX1048, ¶¶19-22.

2. PO's Arguments Against Purves Fail

While Stafford's key signatures are enough to satisfy the virtual-representation requirement, the combination satisfies them a second way. PO argues that Purves' image cannot be a "virtual representation of the credential" because it is not stored on the client or used for verification. POR, 55-60. These arguments fail.

a. PO's Storage Argument Fails

First, it is unclear what limitation PO disputes. PO argues that the supposed lack of storage is fatal because the virtual representation is part of the OVER file,

which must be “transmitted” to the client device and associated with a “scan.” POR, 56-57 (cleaned up). But transmitting and scanning are not “storing.”

Regardless, both experts agree that Purves teaches image-storage on the client. EX1048, ¶¶23-25; EX1047, 69:16-71:18 (admitting storage in RAM); EX2009, ¶162 (admitting “transient storage”). To the extent PO is arguing that Purves lacks **persistent** storage, this is not recited and, regardless, was conventional. EX1048, ¶26 (citing EX1049, ¶24). PO’s attack on Purves individually is also irrelevant given Stafford’s undisputed teaching of client storage. 486-Pet., 62-63 (combination uses images in Stafford’s context); *Palo Alto Networks*, 122 F.4th at 1386.

b. PO’s Verification Argument Fails

PO argues that Purves’ image fails to satisfy requirements of the “virtual representation” under both the Board’s and Visa’s construction of the OVER file. POR, 57-60. Both arguments fall flat.

PO misstates the Board’s construction and imposes an unrecited requirement. PO argues that the Board interpreted OVER file to “mean” a virtual representation of credentials to be used for verification of those credentials. POR, 57. But the Board said that the OVER file “encompasses” a virtual representation; it did not equate the two. 486-ID, 9-11. PO argues that Purves does not use the image (i.e., virtual representation) to verify the credential. POR, 57-58. But this is

not a requirement of the virtual representation. *Supra*, §§II.C, IV.A.1.c; EX1048, ¶27.

PO's discussion of Visa's "OVER file" construction merely rehashes PO's image-storage argument. POR, 58-60. This argument fares no better the second time around. *Supra*, §IV.A.2.a.

B. A POSA Had Reason to Combine Stafford and Purves

Visa demonstrated multiple reasons to combine Stafford and Purves. First, Stafford expressly suggests including other information with its key signatures and using known transfer techniques. 486-Pet., 55-56, 63; EX1005, ¶¶353-54; EX1012, ¶¶106-13. Second, a POSA would have been motivated to obtain known benefits of credential images (e.g., convenience and error-reduction) and QR codes (e.g., convenience, efficiency, and reliability). 486-Pet., 56, 63; EX1005, ¶¶354-55.

PO leaves much of the rationale undisputed, arguing only that the combination is "nonsensical" and renders Stafford inoperable. POR, 60-66. But PO misreads the references and makes a deliberate effort to fail rather than approaching the combination from the POSA's perspective.

1. PO Misunderstands the Combination

At institution, the Board credited PO's distinction between one-time key signatures and Purves' virtual wallet that includes multiple payment accounts.

486-ID, 39-40. PO now goes further, arguing that using credential images to keep track of single-use items is “nonsensical” because the user would never select items after the associated key signatures are generated. POR, 60-61. PO misreads the references.

The references refute PO’s false distinction between virtual wallets and Stafford’s single-use items. Consistent with conventional practice, Purves’ wallet may include single-use items (e.g., tickets). EX1013, ¶¶54 (tickets), 102 (various account types); EX1048, ¶¶28-29 (citing EX1051, ¶¶118, 164; EX1052, 48:23-49:36). Likewise, Stafford encompasses various credential types, including payment accounts. EX1012, ¶¶53 (credential information may be “any type of information relating to an entity”), 73 (information depends on user’s purpose), 81 (information includes “bank account numbers, credit card numbers etc.”). Purves’ virtual-wallet teachings are thus applicable to Stafford. EX1048, ¶29.

PO also fundamentally misunderstands Stafford. PO assumes that the key signatures are never selected after they are generated. POR, 60-61. But PO conflates the initial setup for release (when key signatures are generated and sent to the user) and the user’s subsequent transfer of the key signatures to the recipient. EX1012, ¶31 & Fig. 2 (“process for preparing information”), ¶32 & Fig. 3 (“method of transmitting released data”), ¶¶102-05 (result of initial setup), 133-34 (user gives recipient “previously” created key signatures); EX1048, ¶¶30-31.

Multiple single-use items can be set up for release (EX1012, ¶¶74, 118), much like a physical wallet can hold multiple single-use tickets, and the items are not “spent” until the user gives associated keys signatures to the recipient. EX1048, ¶32. Using images to help identify/select items thus makes perfect sense. *Id.*, ¶33.

2. The Combination Does Not Undermine Security

PO’s security arguments do not withstand scrutiny. PO argues that the combination renders Stafford inoperable because credential images and QR codes cannot be used securely. POR, 62-66. The record exposes this transparent effort to manufacture security problems.

a. PO’s Arguments Against Images Are Unconvincing

The combination applies Purves’ teachings of using a “representative” image or a real image with confidential information obscured. 486-Pet., 62-63 (citing EX1013, ¶¶85, 122). In response, PO ignores Visa’s arguments, Purves’ teachings, and the POSA’s perspective.

PO never addresses “representative” images, and Dr. Malek’s testimony on this point is contrary to Purves. *Honeywell*, 124 F.4th at 1354 n.6 (testimony contradicted by record not entitled to weight). Dr. Malek argues that representative images convey valuable information such as the existence of an account with a particular bank. EX2009, ¶168. Yet Purves expressly teaches representative images. EX1013, ¶¶85 (panel may display image from issuer,

nickname, identifier, brand, etc.), 122 (using “template” image). This approach was conventional and viewed as sufficiently secure. EX1048, ¶¶34-35 (citing, *inter alia*, EX1053, ¶89, Figs. 1A, 4A; EX1054).

PO’s argument against obscured images is unconvincing. PO cites Dr. Malek’s discussion of a blurred image that he says can be unblurred. POR, 64-65 (citing EX2009, ¶¶167-70); *see also* 486-ID, 40 (Board expressing concern regarding obscured image). But obscuring is not limited to blurring. 486-Pet., 62 (citing EX1013, ¶¶111-12); EX1047, 78:5-79:15 (Dr. Malek admitting obfuscation includes redaction). Regardless, the basis of Dr. Malek’s testimony collapsed during cross-examination. He admitted irrecoverable redactions were possible. *Id.*, 79:16-81:2. Despite acknowledging that tools allowed for different levels of blurring, he admitted that PO’s attorneys created the blurred image and he does not know what tools or settings they used. *Id.*, 81:3-82:1; *see also id.*, 75:13-78:4 (admitting he does not recall capabilities of Purves’ exemplary tool). His testimony is also at odds with Purves, which expressly teaches using an obscured image for sensitive credentials like credit cards. EX1013, ¶122; *Honeywell*, 124 F.4th at 1354 n.6. Dr. Shamos confirms that virtual wallets routinely displayed partially obscured account information and that irrecoverable image-obscuring was commonplace and readily achieved. EX1048, ¶¶35-36 (citing EX1040, ¶158, Fig.

10A; EX1049, ¶37; EX1053, ¶¶176, 211, 352, 354, Figs. 17, 22F, 60A-B; EX1055).

PO's argument regarding unencrypted image transmission is flawed. POR, 63; EX2009, ¶¶166, 169. The claims do not require a particular form of transmission. Visa never argued that the combination was limited to unencrypted transmission. And as Dr. Malek admits, encrypted transmissions were well-known and taught by Purves. EX1047, 22:11-24:9 (admitting HTTPS long used to protect payment information), 71:19-76:14 (acknowledging Purves' encryption teachings); *see also* EX1013, ¶¶33, 131, 143, 152, 157, Fig., 25; EX1048, ¶¶37-39.

b. PO's Arguments Against QR Codes Are Unconvincing

Visa showed that applying Purves' QR-code teachings would facilitate easier, more efficient, and more accurate transfer of the key signatures from the user to the third-party recipient. 486-Pet., 55-56, 63. In response, PO manufactures nonexistent problems and misreads the references.

Sending the user QR-encoded key signatures would not introduce security risks. POR, 65-66. Regarding the Board's concern involving storing QR-encoded key signatures (486-ID, 40), Dr. Shamos confirms that storing QR-encoded key signatures is just as secure as storing non-QR-encoded key signatures. EX1048, ¶50. QR-encoded data was known to be securely transmitted and stored just like

other data. EX1048, ¶¶40, 50-51 (citing EX1043, ¶¶53, 60-61; EX1057, ¶42; EX1056, 1:5-50, 2:62-65). Nor does the QR-code-mediated transfer of the key signatures to the third-party recipient introduce security problems. EX1048, ¶52. If anything, it is more secure than Stafford. *Id.*, ¶¶52-53. Purves itself demonstrates the sufficient security of QR codes since it teaches using them for payment transactions. 486-Pet., 63; EX1013, ¶64; EX1048, ¶41.

PO's attempt to show otherwise is unconvincing. PO argues that a "user sending" unencrypted or encrypted QR codes to the third-party recipient would not work. POR, 66; EX2009, ¶176. But the combination involves conveying the key signatures to the third-party recipient via a QR-code scan, not transmitting the QR codes themselves to the third-party. 486-Pet., 55, 63; EX1048, ¶¶42-43, 49. PO argues that using Stafford's email "option"—sending the user an email with encrypted key signatures—would require the user to give their private key to the third-party recipient. POR, 66; EX2009, ¶177. But even if bodily incorporation of this "option" were required—and it is not—the user can decrypt an asymmetrically encrypted QR code just like other data. EX1048, ¶¶44-46; EX1012, ¶71 (system uses entity's public key for "secure communications between the system and the entity"). And even if asymmetric encryption of the key signatures with the user's public key were performed *before* the QR-encoding, Stafford's server already has

the user's private key. EX1048, ¶¶47-48; EX1012, ¶¶68-69, 74, 95-96. The third-party recipient thus does not need the private key as PO argues.

Dr. Malek's testimony lacks credibility for additional reasons. He criticizes user-generation of QR codes, but Visa never proposed this. EX2009, ¶174; EX1047, 27:19-28:20 (admitting he assumed combination involved user-generated QR codes); 486-Pet., 55 (QR-encoded key signatures provided to user). He argues that QR codes are designed for one-to-many communication, whereas Stafford involves one-to-one communication (EX2009, ¶175), but he now admits that QR codes can be used for one-to-one communication. EX1047, 26:12-27:6. Indeed, such use was commonplace and is taught by Purves. 486-Pet., 63; EX1013, ¶64; EX1048, ¶¶41 (citing EX1040, Figs. 10D, ¶¶92-93, 171; EX1050, 3-5), 54.

3. PO Fails to Weigh the Combination's Benefits

Even if PO had demonstrated meaningful security concerns—and it has not—PO never weighs these against the combination's well-established benefits. *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006) (given approach “often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine”). PO and Dr. Malek admit that systems balance security against user convenience (POR, 20; EX1047, 18:13-19:14), yet they never apply this perspective. Dr. Shamos confirms that, while the

combination would not undermine security, the significant benefits easily outweigh any corresponding security risk. EX1048, ¶¶55-60.

V. CONCLUSION

For the above reasons, claims 1-33 are unpatentable and should be canceled.

Respectfully submitted,

Dated: February 3, 2025

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

VI. CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. §42.24(d), the undersigned certifies that this Reply complies with the type-volume limitation of 37 C.F.R. §42.24(c). The word count application of the word processing program used to prepare this Reply indicates that the Reply contains 5,597 words, excluding the parts of the brief exempted by 37 C.F.R. §42.24(c).

Dated: February 3, 2025

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

VII. APPENDIX–PETITIONER’S UPDATED EXHIBIT LIST

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

1018	First Amended Complaint (Dkt. No. 25) <i>Cortex MCP, Inc. v. Visa, Inc.</i> , No. 5-23-cv-05720 (N.D. Cal.), <i>as filed in</i> No. 6-23-cv-00048 (W.D. Tex) (Apr. 10, 2023) (“Complaint”)
1019	Steiner et al., “Kerberos: An Authentication Service for Open Network Systems.” <i>Usenix Winter</i> (1988) (“Steiner”)
1020	Cross River, “Tokenization in Card Networks” (May 2023) (“Cross River”)
1021	U.S. Patent No. 7,014,107 to Irek Singer et al. (“Singer”)
1022	Heather Mark. “Shift4: Secure Payment Processing” (2006) (“Shift4”)
1023	Tom Arnold. “Credit Card Information Surrogate: A Method and System for using surrogates to integrate PCI-level security for legacy information systems.” (2007) (“Arnold”)
1024	Brown et al. “Microsoft Code Name ‘Geneva’ Framework Whitepaper for Developers” (2008) (“Brown”)
1025	Thakar et al. <i>PCI Compliance for Dummies</i> (2009) (“Thakar”)
1026	Ben Jackson. “Token Gestures.” <i>Digital Transactions</i> (2009) (“Jackson”)
1027	First Data. “Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance.” (2009) (“First Data 2009”)
1028	U.S. Patent Pub. No. 2009/0249082 to Ulf Mattson (“Mattson”)
1029	U.S. Patent Pub. No. 2010/0070754 to Nathan P. Leach (“Leach”)
1030	Propay Press Release. “ProPay Adds Automated Clearing House (ACH) Data Encryption And Tokenization To Its Suite Of ProtectPay Services.” (May 10, 2010) (“Propay”)
1031	Richard J. Sullivan. “The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy.” (2010) (“Sullivan”)
1032	CyberSource. “CyberSource Electronic Check Services Implementation Guide” (2010) (“CyberSource”)

1033	Visa. “Visa Best Practices for Tokenization Version 1.0.” (2010) (“Visa Best Practices”)
1034	U.S. Patent No. 8,458,487 to Gary Palgon et al. (“Palgon”)
1035	PCI Security Standards Council. “PCI DSS Tokenization Guidelines.” (2011) (“Tokenization Guidelines”)
1036	U.S. Patent Pub. No. 2011/0258122 to Daniel Jeffrey Shader et al. (“Shader”)
1037	U.S. Patent Pub. No. 2011/0320316 to Joseph R. Randazza et al. (“Randazza”)
1038	Tim Horton et al. “A Primer on Payment Security Technologies: Encryption and Tokenization.” (2011) (“First Data 2011”)
1039	U.S. Patent Pub. No. 2012/0016731 to Randy Smith et al. (“Smith”)
1040	U.S. Patent Pub. No. 2012/0150669 to Garrett S. Langley et al. (“Langley”)
1041	Guenther Starnberger et al. “QR-TAN: Secure Mobile Transaction Authentication.” <i>2009 International Conference on Availability, Reliability and Security</i> . IEEE. (2009) (“Starnberger”)
1042	U.S. Patent Pub. No. US 2011/0251892 to Kevin Laracey (“Laracey”)
1043	U.S. Patent Pub. No. 2012/0209749 to Ayman Hammad et al. (“Hammad”)
1044	U.S. Patent Pub. No. 2009/0113543 to Neil P. Adams et al. (“Adams”)
1045	Patent Scheduling Order (Dkt. No. 73) <i>Cortex MCP, Inc. v. Visa, Inc.</i> , No. 5-23-cv-05720 (N.D. Cal.) (Jan. 3, 2024) (“Scheduling Order”)
1046	United States District Courts — National Judicial Caseload Profile, https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf (March 2023)
1047	Transcript of December 12, 2024, Deposition of Dr. Sam Malek with signed Errata Sheet

1048	Reply Declaration of Michael I. Shamos, Ph.D., J.D.
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,” <i>31st Annual International Computer Software and Applications Conference</i> (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”)

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing Petitioner's Reply to Patent Owner's Response and Exhibits 1047-1057 were served on February 3, 2025, at the following electronic service addresses:

Michelle E. Armond
Douglas R. Wilson
Patrick Maloney
Yue Han
ARMOND WILSON LLP
michelle.armond@armondwilson.com
doug.wilson@armondwilson.com
patrick.maloney@armondwilson.com
amy.han@armondwilson.com
ipr@armondwilson.com

Dated: February 3, 2025

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