Paper No. 9

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

MASTERCARD INTERNATIONAL INCORPORATED
Petitioner

v.

LEON STAMBLER
Patent Owner

---

Case CBM2015-00044
Patent No. 5,793,302

---

**PATENT OWNER LEON STAMBLER'S PRELIMINARY RESPONSE TO MASTERCARD INTERNATIONAL INC.'S PETITION FOR COVERED BUSINESS METHOD PATENT REVIEW**

## TABLE OF CONTENTS

**Page**

**Page**

## TABLE OF AUTHORITIES

**Page(s)**

**FEDERAL CASES**

**Page(s)**

**FEDERAL CASES (CONT.)**

**Page(s)**

**FEDERAL STATUTES**

**Page(s)**

**OTHER AUTHORITIES**

## EXHIBITS

Ex. 2001 *Visa Inc. v. Leon Stambler*, IPR2014-00694, Paper 10, Decision, PTAB (Oct. 31, 2013)

Ex. 2002 Defendants Mastercard Incorporated and Mastercard International Incorporated's Invalidity Contentions

Ex. 2003 Meyer Claim Chart

## I. INTRODUCTION

This is the seventh post-grant petition that attempts to raise substantially the same basket of prior art against U.S. Patent No. 5,793,302 (the '302 Patent) (Ex. 1001) – where none of the prior ones led to trial institution. It is the second of two covered business method review petitions filed by Petitioner, MasterCard International Incorporated, against the'302 Patent. MasterCard filed its first on October 24, 2014 (CBM2015-00013). The -00013 petition presents the same prior art presented here (Davies, Nechvatal, Fischer and Piosenka), except that MasterCard has added one additional reference to the present petition (Meyer). MasterCard already knew about the Meyer reference when it filed the -00013 petition. *See* Ex. 2002 at 15 (the same Meyer reference listed in MasterCard's July 11, 2014 district court invalidity contentions). In fact, it had already charted it. Ex. 2003. Patent Owner Leon Stambler filed his Preliminary response in the -00013 proceeding on February 4, 2015. However, on March 30, MasterCard sought permission to withdraw the -00013 petition (without opposition by Mr. Stambler).

In turn, the -00013 petition presented the identical prior art – with identical arguments – of five previous non-instituted *inter partes* review petitions, four of which settled[1] and one of which went to a full institution decision. Concerning the latter, Visa Inc. filed a petition (IPR2014-00694) that presented the same invalidity

[1] The settled matters are: IPR2013-00341, IPR2013-00409, IPR2014-00244 and CBM2014-00129.

arguments against the same group of claims (51, 53, 55 and 56) using the same Davies, Nechvatal, Fischer and Piosenka references as Petitioner's -00013 petition. On October 31, 2014, the Patent Trial and Appeal Board (PTAB) denied institution on patentability grounds. *Visa Inc. v. Stambler*, IPR2014-00694, Paper No. 10 (Oct. 31, 2014), Ex. 2001.

The Board should not institute a covered business method review. First, for the same reasons as explained in *Conopco, Inc. v. Procter & Gamble Co.*, IPR2014-00628, Paper No. 23 (March 20, 2015), the Board should exercise discretion under 35 U.S.C. §§ 324(a) and 325(d) to end this series of repetitive petitions. Second, MasterCard has not shown that U.S. Patent No. 5,793,302 (the '302 Patent) (Ex. 1001) is a covered business method patent, and has not met the more likely than not standard required by Patent Office regulations to demonstrate that at least one of the claims challenged in the petition is unpatentable. 37 C.F.R. § 42.208(c).

## II. OVERVIEW OF U.S. PATENT 5,793,302

The Stambler '302 Patent discloses novel methods to authenticate parties and information involved in transactions. Ex. 1001, Col.1, ll. 15-21. An overview of the funds transfer embodiments illustrated by FIGS. 6-8 of the '302 Patent follows. These embodiments demonstrate the enrollment of a payment originator (FIG. 6), the creation of a check (FIG. 7), and the redemption and verification of the check (FIGS. 8A and 8B). Although the embodiments of FIGS. 6-8 are described in the context of creating and authenticating a paper check, the '302 Patent explains that these embodiments (and the disclosed concepts) apply equally to electronic funds transfers and a "paperless/cashless" transaction system, which completes "funds transfer" transactions "entirely electronically." Ex. 1001, Col. 5, ll. 28-30; Col. 24, ll. 4-29.

FIG. 6 illustrates enrollment of an originator at his bank. First, the bank verifies the originator's identity and the originator provides personal information (e.g., a tax ID number ("TIN")). Ex. 1001, Col. 4, ll. 2-11. Then the bank opens an account and creates a file for the originator, and the originator selects a secret personal identification number ("PIN"), which is irreversibly coded and transferred to the bank. Ex. 1001, Col. 4, ll. 13-51. The coded PIN is later used by the originator and the originator's bank to generate cryptographic keys used to code or uncode funds transfer instructions (e.g., a check).

FIG. 7 illustrates a method for generating a check. Ex. 1001, Col. 4, ll. 52-53. First, the originator inputs funds transfer information (e.g., the originator's TIN, the recipient's TIN, an amount, and other information) into a computer or terminal. Ex. 1001, Col. 44. ll. 53-60. The originator then inputs his PIN, which is irreversibly coded to produce a coded PIN. Ex. 1001, Col. 5, ll. 3-6. The coded PIN, together with information related to the funds transfer recipient (e.g., the recipient's TIN), are coded together to generate a cryptographic key called the "joint key" or "joint code." Ex. 1001, Col. 5, ll. 3-15. The joint key is then used to code the funds transfer information to generate what the '302 patent calls a "variable authentication number" ("VAN"). Ex. 1001, Col. 5, ll. 9-22. The VAN and other funds transfer information are imprinted on the check. Ex. 1001, Col. 5, ll. 25-34.

FIGS. 8A and 8B illustrate methods for redeeming a check generated according to FIG. 7. Ex. 1001, Col. 5, ll. 55-58. In FIG. 8A, the check recipient first enters his PIN into a bank terminal. Ex. 1001, Col. 5, ll. 62-66. The PIN is irreversibly coded and transmitted along with other information (e.g., the recipient's TIN) to the recipient's bank. Ex. 1001, Col. 5, ll. 66-6:40. The recipient's bank accesses the recipient's file using his TIN and verifies his identity with his coded PIN. *Id*. This is an example of entity authentication (i.e., identity verification) — if the PIN is incorrect, the authentication fails. Ex. 1001, Col. 6, ll.

38-40. If the recipient's identity is verified, the recipient's bank transfers the information from the check to the originator's bank. Ex. 1001, Col. 6, ll. 43-45.

In FIG. 8B, the originator's bank receives the funds transfer instructions and the VAN from the recipient's bank, which is requesting authorization to pay. Ex. 1001, Col. 6, ll. 43-45. Using the originator's TIN, the originator's bank accesses the originator's file and retrieves information used to derive the originator's coded PIN. Ex. 1001, Col. 6, ll. 46-55. The originator's bank's system generates a joint key by coding the originator's coded PIN (derived by the bank) with the recipient's TIN. Ex. 1001, Col. 6, ll. 66-7:2. The originator's bank then uses that joint key to uncode the VAN included with the check and compares the resulting information with the received funds transfer instructions. Ex. 1001, Col. 7, ll. 2-11; FIG. 8B, uncoder 58, comparator 60. If they match, the funds transfer instructions are presumed to be unaltered (data integrity authentication) and to have come from the originator (data origin authentication). Ex. 1001, Col. 7, ll. 16-20. Alternatively, and as a pertinent embodiment supporting the claims at issue, the system authenticating the funds transfer information generates a new VAN by coding the received funds transfer information with the separately generated joint key. Ex. 1001, Col. 7, ll. 12-15. This newly generated VAN is compared with the received VAN to authenticate the check. *Id*. If the VANs match, the funds transfer instructions are presumed to be unaltered and to have come from the originator. Ex. 1001, Col. 7, ll. 16-20.

The ’302 Patent also discloses credential issuing and authentication systems and methods. *See, e.g.*, Ex. 1001, Col. 8, l. 45-Col. 13, l. 39, Col. 17, l. 1-Col. 20, l. 42. The specification explains that the disclosed systems and methods “would be useful for all types of credentials and records; for example, motor vehicle registrations, social security cards, passports, birth certificates and all types of identification cards or personal storage media.” Ex. 1001, Col. 8, ll. 55-60. In the disclosed credential issuing and authentication embodiments, information in a credential is secured through the use of a variable authentication number (VAN). The operation of the disclosed systems and methods for issuing and authenticating credentials is similar in many ways to the operation of the disclosed funds transfer embodiments described above (*e.g.*, use of a joint code and VAN).

## III. CLAIM CONSTRUCTION

Patent Owner agrees with Petitioner that claim construction must proceed under traditional canons, not under the “broadest reasonable interpretation” framework. This is because the ’302 Patent is expired. As shown below, Petitioner misstates several of the constructions it proffers, and omits several others that are needed for complete resolution of the issues.

### A. Credential

In the present petition, different from its petition in the -00013 proceeding, Petitioner presents no construction of "credential." In the -00013 proceeding, Petitioner argued that credential should be construed as "a document or information obtained from a trusted source that is transferred or presented *to establish the identity of a party*." Patent Owner asserts credential should be construed as "a document or information obtained from a trusted source that is transferred or presented *for purposes of determining the identity of a party*." Patent Owner has adopted a court's reasoning to reach this construction. Ex. 1018 at 2.

The only apparent difference between the parties' positions is whether a credential is transferred or presented "to establish the identify of a party" or "for purposes of determining the identity of a party." Patent Owner's construction on this point is consistent with the exemplary credentials identified in the '302 patent, such as identification cards. Ex. 1001, Col. 8, ll. 55-60. It is accurate to say that an identification card is "transferred or presented for purposes of determining the identity of a party." Once received, the receiving party may use the credential to make a determination regarding the credential holder's identity. However, in many cases, the receiving party may not consider the credential sufficient to make a determination (much less "establish the identity of a party," which has been Petitioner's construction). The receiving party requires additional identification information (*e.g.*, a bank asking for two pieces of identification information). Thus,

a single credential does not necessarily "establish" identity, which has been Petitioner's construction.

### B. Sequence of Method Steps

The proper sequence of the method steps of claim 51 should be construed. The PTAB has already agreed with Patent Owner on this point, and denied a request by Visa, Inc. to institute proceedings based in part on this claim construction. Ex. 2001, *Visa Inc. v. Leon Stambler*, IPR2014-00694, Paper 10, Decision, PTAB (Oct. 31, 2014).

A method claim must be performed in the order in which the steps are written to the extent that, as a matter of logic or grammar, the order exists in the claims. In *Loral Fairchild Corp. v. Sony Electronics Corp.*, 181 F.3d 1313, 1321 (Fed. Cir. 1999), the claim language itself indicated that the steps had to be performed in their written order because the second step required the alignment of a second structure with a first structure formed by the prior step. *See also Mantech Envtl. Corp. v. Hudson Envtl. Servs., Inc.*, 152 F.3d 1368, 1375-76 (Fed. Cir. 1998) (holding that steps of a method claim performed in their written order because each subsequent step referenced something logically indicating that the prior step had been performed).

Here, the first step (51a) is "receiving funds transfer information," *et cetera*. The second step (51b) is "generating a variable authentication number (VAN) using at least a portion of the *received* funds transfer information" (emphasis

added). Thus, the first step must be finished for the second step to begin. Logically, a party cannot "generate a [VAN] using ... the *received* funds transfer information" (step 51b) until after the funds transfer information is actually received (51a).

### C. VAN

The correct construction of VAN is not Petitioner's "a variable number resulting from a coding operation that can be used in verifying the identity of a party or the integrity of information or both." Instead, the term VAN should be properly construed as:

> an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both, the value generated by coding information relevant to a transaction, document, or thing with either a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing

Variable authentication number ("VAN") is a term coined by the Patent Owner and inventor Mr. Stambler. Where, as here, a claim term has no understood meaning in the art, the proper construction is the definition given the term in the specification. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005).

The PTAB should adopt Patent Owner's proposed construction because it gives VAN the meaning assigned to it by the specification.[2]

First and foremost, the patent only describes creating the VAN by coding information with a key or other input (e.g. the joint key). Patent Owner's proposed construction recognizes that the term "variable authentication number" is defined not only by how it is used, but also by how it is created. The specification teaches creating a VAN in only two ways: (1) by coding information with either a joint key (or code); or (2) "generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the [joint key]." *See, e.g.*, Ex. 1001, Col. 2, ll.9-17; Col. 5, ll. 9-25; and Col. 11, l. 65-Col. 12, l. 2. How the VAN is created defines what it is. The proper construction of VAN must reflect that the VAN is created by coding information to be authenticated "with either a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing." *See* Ex. 1001, Col. 2, ll.9-17; Col. 5, ll.9-25; and Col. 10, ll. 42-45 (assigning a number to a party

[2] The prior institution decision, Ex. 2001, IPR2014-00694, Paper No. 10 at 7-8, adopted Petitioner's construction, but only "for purposes of the decision," and arguably in dictum because the VAN construction did not affect the non-institution outcome.

for use in creating a joint key); Col. 11, ll.15-20 (the VAN / joint key is created using information "***related to***" the parties).

The PTAB should reject Petitioner's construction because it disregards that the term "VAN" was coined by Mr. Stambler. Notably Petitioner's construction ignores that whether an encoded variable number falls within the scope of "VAN" depends not only on how it is used, but how it is created. Petitioner's construction arguably does not require the VAN to be created by coding information with a key or other input, which is contrary to the specification's disclosure. Consequently, Petitioner's construction is overbroad and encompasses information that Mr. Stambler clearly considered outside the scope of a VAN. For example, Mr. Stambler discloses a coded personal identification number (PIN) as separate and distinct from the disclosed VAN. *See* Ex. 1001, Col. 5, ll. 3-35. Petitioner's proposed construction, however, reads on the disclosed coded PIN, which is "an encoded variable number that can be used in verifying the identity of a party." *See* Ex. 1001, Col. 4, ll. 43-46: ("CPN represents coded authentication information since it is a coded form of the PIN, and since it is used in other parts of the system to authenticate the user ....").

### D. Error Detection Code

The correct construction for "error detection code" should be: "the result of applying an algorithm for coding information that, when applied to original information, creates coded information wherein changes to the original information

can be detected without complete recovery of the original information." Petitioner seeks no construction in this proceeding. Patent owner's follows the Court's construction in one of the later claim construction orders. *See, e.g.*, *Stambler v. ING Bank FSB*, Case No. 2:10-cv-00181-DF-CE, Dkt. No. 365, at 24-25 (E.D. Tex. Sept. 28, 2011) (Memorandum Opinion and Order); Ex. 1016 at 24-25.

**E. Trusted Party Or Entity**

Petitioner does not offer a construction for "trusted party." Claim 51 contains the phrase "a credential being previously issued by a trusted party." The term "trusted entity," which is synonymous with "trusted party," has been construed by the United States District Court for the Eastern District of Texas on multiple occasions as "an entity / party that has the authority, as recognized by participants in the relevant system or method, to establish or confirm a party's identity." Ex. 1018 at 3. This construction is consistent with the intrinsic record and should be applied in this proceeding.

In claim 51, the "trusted party" issues a "credential." A "credential" is a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party. An exemplary credential is a passport. Ex. 1001, Col. 12, ll. 22-25. Thus, it seems undisputed that "trusted party" must, prior to issuing a credential, establish or confirm the identity of the party to whom the credential is being issued. And the trusted party must in

fact be trusted by the participants in the relevant system or method to have authority to issue valid credentials.

### F. Coding

Petitioner does not offer a construction for "coding," but the concept of coding is built into both parties' construction of VAN. The patent specification and the prosecution history specially define coding. First, the specification introduces the "coder" of Figure 1 by noting that it is a hardware component or a functional block of a computer program. Ex. 1001, Col. 3, ll. 30-36 (describing FIG. 1). It further describes the coding entity as a "device utilizing a known algorithm, such as the Data Encryption Standard (DES)." Ex. 1001, Col. 3, ll. 38-39. Second, confirming the device-oriented nature of the coding operation, the applicant stated during prosecution, in discussing the "present invention" of the newly added claims that became the issued patent claims: "Such transactions are carried on *entirely electronically*, the participant's bank accounts, are credited and debited automatically." Ex. 1011 at 306-07. Therefore, coding is:

> Using an entirely electronic device that is either a hardware component or a computer running a functional block of a computer program to transform information by applying a known algorithm.

## IV. THE PETITION SHOULD BE DENIED UNDER 35 U.S.C. §§ 324(a) AND 325(d) BECAUSE SUBSTANTIALLY THE SAME PRIOR ART AND ARGUMENTS WERE BEFORE THE PATENT OFFICE, AND BECAUSE THE DIRECTOR HAS DISCRETION TO REJECT SEQUENTIAL PETITIONS THAT MODIFY ARGUMENTS IN RESPONSE TO A PREVIOUS DENIAL OF INSTITUTION

The PTAB should deny review of this seventh nearly duplicative petition, which is the second by Petitioner.

The PTAB recently addressed and confirmed its authority, in its sound discretion, to deny review of successive post-grant challenges by the same party. Citing the benefit of "remov[ing] an incentive for petitioners to hold back prior art for successive attacks, and protect[ing] patent owners from multifarious attacks on the same patent claims," the PTAB explained its discretion to deny "'follow-on' second petitions [filed] in order to 'correct deficiencies noted' by the Board in decisions that deny a first petition. . . ." *Conopco, Inc. v. Procter & Gamble Co.*, IPR2014-00628, Paper No. 23, at 5. As the PTAB also explained, it strives to eliminate incentives that "allow petitioners to unveil strategically their best prior art and arguments in serial petitions, using our decisions on institution as a roadmap, until a ground is advanced that results in review – a practice that would tax Board resources and force patent owners to defend multiple attacks." *Id.*

This is precisely the taxing situation that Mr. Stambler and the PTAB face now. Here, after Mr. Stambler fended off at least one meritless petition at great expense (Ex. 2001, IPR2014-00694), MasterCard brings its -00013 and -00044

CBM petitions. The present petition contains a whole section explaining how it will use the claim construction from the prior VISA IPR institution-denial decision (Ex. 2001, IPR2014-00694, Paper No. 10), using the identical prior art presented there (plus Meyer). (*See* Paper No. 7 at 16-17). Throughout its current -00044 petition, MasterCard left no doubt that it relied on the prior institution decision as a "roadmap." In its own words:

- "The Davies reference, however, does disclose exactly what the Board in the IPR Decision stated was missing from that petition's submission." (*Id*. at 17).

- ". . . [P]etitioner submits that this disclosure . . . provides what the Board stated was missing in the IPR Decision." (*Id*. at 17-18).

- "Accordingly, Meyer discloses what the Board in the IPR Decision considered to be missing from the Davies reference . . . ." (*Id*. at 22, 51, 57, 59).

- "According to the Board's IPR Decision, 'at least a portion of the receiving step must precede the generating step…." IPR Decision 12. As explained in the Diffie Declaration, this is exactly what Davies discloses . . . ." (*Id*. at 28).

MasterCard's conduct therefore falls squarely within the category of "taxing" conduct that the PTAB wants to dissuade.

Nor does the presentation of additional prior art (Meyer) excuse MasterCard's strategy. The petitioner also brought different prior art in its

*Conopco* petition. The PTAB reasonably inferred that Conopco had such prior art all along. Here, there is no need to stretch and make an inference. MasterCard undeniably had Meyer months before it filed its first petition, the October 24, 2014 -00013 proceeding, having disclosed the Meyer reference in its July 2014 invalidity contentions in the District Court litigation. Ex. 2002, at 15. In fact, MasterCard had already charted Meyer. Ex. 2003.

Additional reasons make MasterCard's tactic more eggregious than what motivated the PTAB to issue the *Conopco* ruling. MasterCard filed the present follow-on CBM petition solely to attack patent claims based on prior art unpatentability over five prior art references. *MasterCard could have filed the present petition as an IPR petition.* It must have calculated that filing as a CBM (rather than an IPR) endows it with tactical advantages against Mr. Stambler – an individual inventor. For filing a CBM (and not IPR) petition, MasterCard receives larger page limits and, should it lose after a PTAB trial, a more forgiving district court estoppel against it raising similar future district court arguments. In district court proceedings, MasterCard also receives the advantage of a nearly automatic stay (which inures only to CBM petitions, not IPR petitions). Petitioner should not be rewarded for masking one type of petition as another, just to endow itself with procedural benefits against an individual inventor seeking relief from Petitioner's infringement.

For the foregoing reasons, under the discretion of the PTAB within 35 U.S.C. §§ 324(a) and 325(d), the PTAB should deny this seventh sequential petition (the second by MasterCard itself).

## V. THE PETITION SHOULD BE DENIED BECAUSE OF LACK OF STANDING

### A. The '302 Patent Is Not A Covered Business Method Patent

Petitioner also bears the burden of "demonstrate[ing] that the patent for which review is sought is a covered business method patent." 35 C.F.R. § 42.304(a). Petitioner's petition for post-grant review of the '302 Patent under § 18 of the AIA must be denied because § 18 applies only to covered business method (CBM) patents and Petitioner has failed to and cannot meet its burden because the '302 Patent is not a CBM Patent. A CBM patent is "a patent [for a non-technological invention] that claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service." AIA § 18(d)(1) (emphasis added); *see also*, 37 C.F.R. § 42.301.

According to the Office in its decision in *SAP Ametica, Inc. v. Versata Development Group, Inc.,* CBM2012-00001, Paper 36, at 21-22 (PTAB Jan 9, 2013), a CBM patent includes "activities that are financial in nature, incidental to a financial activity or complementary to a financial activity." Patent Owner notes that this interpretation is broader than the actual language in AIA § 18(d)(1). More

recently in *Apple Inc. v. Sightsound Technologies, LLC*, CBM2013-00019, Paper 17, at 11-12 (PTAB Oct. 8, 2013), the Office elaborated that "a financial product is an agreement between two parties stipulating movements of money or other consideration now or in the future."

Even with such a broad definition of a CBM patent, the '302 Patent is not encompassed by this definition. First, the claimed inventions of the '302 Patent are not "financial products." The '302 Patent is directed to a transaction system for authenticating parties and a transaction, document or thing involving the parties *when one or more of the parties is not present*. Ex. 1001, Col. 1, l. 43-Col. 2, l. 4.

Even though the claims being challenged by Petitioner recites terms such as "transfer", "funds", and "account", the claims are directed to authenticating the parties and the instrument of the transaction. *See,* Ex. 1001, Abstract.

Moreover, the '302 patent was classified by the USPTO in Class 340, which is defined as "subject matter, not elsewhere classified, relating to communication by means which are in part or in whole electrical." USPTO Classification Definitions, 340-1 (November 2012). Notably, the '302 patent was not classified in Class 705, which is defined as appropriate for financial methods. *Id.* at 705-1.

Further, the USPTO never asserted a rejection under 35 U.S.C. § 101 against any of the claims of the '302 patent during prosecution of the application from which the '302 patent matured. Thus, the USPTO determined that the claims included patentable subject matter, and were not attempting to claim any abstract

ideas or natural principles, or methods that could be accomplished using paper and pencil or in an inventor's own mind.

The '302 patent cannot possibly be eligible for CBM review because it is not a business method patent. Rather, the '302 Patent solves a technical problem with a technical solution, and is patentable over the prior art based on a technological innovation.

### B. Claims 51, 53 and 55-56 Of The '302 Patent Are Directed To A Technological Invention

The definition of "covered business method patent" in AIA § 18(d)(1) expressly excludes patents for "technological inventions." *See also* 37 C.F.R. § 42.301(a). To determine whether a patent is for a technological invention, it is necessary to consider "whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art; and solves a technical problem using a technical solution." 37 C.F.R. § 42.301(b).

#### 1. The Challenged Claims Recite A Technological Feature That Is Novel And Unobvious

Petitioner cites to the Office Patent Trial Practice Guide for its two-part test for determining whether the claimed subject matter as a whole recites a novel and non-obvious feature. Petitioner's argument fails for several reasons.

##### (a) Petitioner Has Not Demonstrated That The Claimed Inventions Of The '302 Patent Recite The Use Of Known Prior Art Technology

Petitioner's statement that "a patent is not a technological invention if it merely combines known technology in a new way to perform data processing operations" is the only support proffered to support its assertion that the claims of the '302 Patent do not recite a novel and non-obvious technological feature. Paper No. 7, at 6. Notably, Petitioner's expert, Mr. Diffie, does not support this statement.

Petitioner also argues, unsupported by Mr. Diffie, that the specification describes using "conventional building blocks for computer or communications systems" (*Id.* at 7), but then admits that the claims themselves do not recite those building blocks. *Id*. at 8. Such inconsistency is typical of the Petition.

The claims of the '302 patent do not merely recite known uses of conventional building blocks or systems. Rather, Claim 51, the only independent claim challenged, recites a method wherein a transfer of funds from one party's account to another party's account is effected only if at least a portion of the received funds transfer information and a variable authentication number (VAN) generated from the at least a portion of received funds transfer information are determined to be authentic. The at least a portion of received funds transfer information is determined to be authentic using the VAN and information from a credential issued to one of the parties.

Simply using a computer to carry out a method does not automatically characterize that method as a "data processing" operation. The claimed method

does not simply add, subtract or sort information. Rather, the claimed method generates a VAN from information received, and then, applying an intelligent decision making process, determines if the received information and VAN are authentic, only authorizing a transfer of funds if both the received information and the VAN are authentic.

The claimed method provides for authenticating both the received funds transfer information and the identity of the parties, even if one of the parties is absent. Petitioner's simplistic example set forth on pages 8-9 of the Petition (also unsupported by Mr. Diffie), misses the mark because, among other shortcomings, it equates "credential information" with account information in a bank ledger (a non-public document). Paper No. 7, at 9. As discussed, a credential is "a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party." A bank ledger cannot be a "credential" because it is not transferred or presented for purposes of determining the identity of a party; thus information copied from the bank ledger cannot be the "credential information" of the challenged claims. *See,* Ex. 1018 at 2.

**(b) The PTAB Previously Determined That Technological Features Of The Challenged Claims Are Novel And Unobvious Over Most of the Same Prior Art Cited In The Petition**

The technological features of the challenged claims of the '302 patent have previously been found novel and unobvious over most of the same prior art that is

asserted in this Petition. In *VISA, Inc. v. Leon Stambler*, IPR2014-00694, the PTAB denied institution of trial based on VISA's assertion that claims 51, 53, and 55-56 of the '302 patent were anticipated by Davies, and rendered obvious in view of Davies and Nechvatal, and Davies, Fischer and Piosenka, determining that VISA had failed "to demonstrate a reasonable likelihood of prevailing on its challenge to the patentability of claims 51, 53, and 55-56 of the '302 Patent". *See* Ex. 2001, at 2-3, 18. *Compare* Paper No. 7, at 10; with Ex. 2001, at 2-3. Indeed, the arguments presented in IPR2014-00694 are virtually identical to the arguments presented in the pending Petition.

As already discussed, Petitioner used the IPR decision as an improper "roadmap," and contends that it has found portions of the same basket of references that meet the PTAB's claim construction requirements. Even if this is a permitted tactic, Petitioner is not correct that it has plugged any gaps. Petitioner now points to the ATM embodiment within Davies as the primary reference. *See* Paper No. 7, at 29 (pointing to excerpt at Ex. 1004 at 330-31 where a "message 'is signed and returned to the ATM.'"). Petitioner shifts ground because the PTAB held that the "cheque" embodiment did not respect the ordering required by claim 51 ("receiving" before "generating"). But as will be discussed in detail below, the ATM embodiment stands even further from the scope of claim 51 than did the "cheque" embodiment. Most obviously, claim 51 requires both an "account of a first party" and an "account of a second party" to be involved in the claimed

method, within each of the preamble, the "receiving" step and the "transferring" step. *See* Ex. 1001. The ATM transactions Petitioner points to in Davies involve an account of only ***one*** party – the person withdrawing currency. *See* Ex. 1004 at 331 (noting that "ATM request" is a distinct "transaction type" from "customer cheque," and involves solely an ATM to "release the money" to the customer).[3] Mr. Stambler discusses even further distinctions later in this Preliminary Response.

Nor does the addition of the Meyer reference help Petitioner refute that the claimed technological features of claim 51 are novel and nonobvious. As will be discussed in detail below, Petitioner relies on unlinked and distinct embodiments within Meyer, but primarily relies on a discussion of a particular point of sale transaction involving a "grocer." In this transaction, Meyer never indicates that the transaction information ("Mreq") includes anything about an "account of the

[3] Petitioner mistakenly and misleadingly argues that Mr. Stambler himself has conceded that ATM cash withdrawal meets the entire "transferring" step. Paper No. 7, at 34, 62-63 (citing Ex. 1021 at 4-5). In fact, Mr. Stambler argued for the breadth of the disembodied word "transferring" (that it includes more than crediting and debiting). That argument did not negate other material limitations of the claim (such as first and second accounts). The district court in the underlying proceeding acknowledged as much. Ex. 1015, at 9 ("Plaintiff further submits he has not proposed that paper money transactions are encompassed by the term but rather has cited such embodiments to show the broad meaning of the word 'transferring' as used in the patents-in-suit.").

second party." Ex. 1022, at 477. Nor would it have to – a grocer's point of sale system may have hard-wired links into a funds transfer network such that a ***customer*** would never have to indicate that the grocer is the intended recipient of funds. The Petition sidesteps this problem by pointing to "suitable routing information" within the transaction request as if this satisfies the "second party" limitation. Paper No. 7, at 41. But Meyer's context makes clear that such "routing information" is of the ***customer*** account (*i.e.,* that of the "first party") so that the "acquirer [bank] (HPC X)" may know how to find the customer's "issuer [bank] (HPC Y)." Ex. 1022, at 477. The "routing information" is not related to a second account.

These are only a few distinctions. Mr. Stambler raises them here solely to address the threshold question of CBM standing, and particularly the question "whether the claimed subject matter as a whole recites a technological feature *that is novel and unobvious over the prior art*; and solves a technical problem using a technical solution." 37 C.F.R. § 42.301(b) (emphasis added). Mr. Stambler addresses yet additional distinctions in later sections of this Preliminary Response.

**(c) Conclusion**

For the reasons set forth above, Patent Owner submits that not only does the claimed subject matter as a whole recite a technological feature, that feature is novel and unobvious over the prior art.

### 2. Petitioner Has Failed To Establish That The Challenged Claims Do Not Recite A Technical Solution To A Technical Problem

As stated in 35 C.F.R. § 42.304(a), the Petitioner bears the burden of "demonstrate[ing] that the patent for which review is sought is a covered business method patent." One of the elements in demonstrating that a patent is a CBM patent is "whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art; and *solves a technical problem using a technical solution*." 35 C.F.R. § 42.301 (emphasis added).

Notably, even though Petitioner asserts that the challenged claims contain nothing but a collection of old elements, Petitioner completely ignores the technical features that the USPTO itself found to be novel during prosecution of the application that matured into the '302 patent. Petitioner's argument is flawed because the predicate to understanding how the claims of the '302 patent recite a technical solution is to understand the technical problem being solved by those claims. Neither Petitioner nor Mr. Diffie, Petitioner's Expert, identify any problem at all.

#### (a) The Technological Problem Solved By The Challenged Claims Of The '302 Patent

The technological problem solved by the claimed inventions of the '302 patent is specifically set forth in the Background of the Specification of the '302 patent. Prior to the advent of electronic communication of documents, the parties

to a transaction, and the documents being exchanged between those parties, were authenticated using "special forms, official stamps and seals, and special authentication procedures . . . ." *Ex.* 1001, Col. 1, ll. 34-36. Even these measures, however, could not entirely prevent ingenious individuals from discovering ways to circumvent or evade such systems. *Id.* at ll. 40-42.

The introduction of computers and computer communications provide an improved measure of security, as it is now possible to verify documents and transactions more quickly that before. "However, with the elimination of the human factor, verification of the identi[ties] of the parties also became more difficult." *Id.* at ll. 48-50.

As noted in the '302 patent, there is thus "[a] pressing need . . . for business transaction, document processing and record access systems which can assure the identity of the parties and the accuracy of the information involved in the transaction." *Id*. at ll. 50-54.

The technical problem solved by the '302 patent is summarized by the statement:

> The security problems described above have been handled with some degree of success in systems involving a single party transaction where the party is present. For example, during the use of an automatic teller machine, the customer is the sole party involved and is present in person. However, until the present invention, it has not been possible to verify the identity and to secure the interests of all

parties to multi-party transactions and, in particular, absent parties to a transaction.

Ex. 1001 at Col. 1, l. 63-Col. 2, l. 4 (emphasis added).

**(i) The Technological Problems Arise From The Use Of Technology**

The use of technology itself, that is, using computers and computer communications, gives rise to particular problems that did not exist previously in the non-technological world. For example, when verification depended on the use of special forms and seals, each party to a transaction was required to appear before someone authorized to authenticate the identity of the party. *Id.* at Col. 1, ll. 23-50.

While passwords and other security mechanisms have been developed to ensure that a party using a computer system to exchange documents with another party is at least a person authorized to use the transmission system, "it has not been possible to verify the identity and to secure the interests of all parties to multi-party transactions and, in particular, absent parties to a transaction." *Id.* at Col. 1, l. 63-Col. 2, l. 4.

Thus, the technological problem arises from the use of computer and computer communications which, even using passwords and/or other security schemes, does not provide a way to identify an absent party to a transaction.

Notably, Petitioner provides no basis for its assertion that "no new technology components were required to enable this authentication" other than attorney argument. Noticeably lacking is any comment by Mr. Diffie concerning any of the technology components described in the '302 patent, old or new.

The '302 patent was the first to offer a technical solution to this technical problem. As will be discussed below, the claimed inventions of the '302 patent are not mere automations of a non-technical problem. The problem was technological in nature given the technology in use in prior art authentication systems. The '302 Patent uses technology to solve the above identified problem.

**(b) The Technological Solution Provided By The Challenged Claims**

To properly understand the technological solution of the claimed inventions, one must take proper notice of the meaning of the terms of the claims. For example, challenged claim 51 recites generating a variable authentication number (VAN). As discussed above regarding the proper construction of the term VAN, the concept of coding is built into both Petitioner and Patent Owner's construction of that term. The patent specification and prosecution history specifically define that a "coder" is used in the generation of the VAN. Moreover, Patent Owner, during prosecution of the application claim that matured into challenged claim 51 stated that "[s]uch transactions [as the transfer of funds from one account to

another] are carried on entirely electronically, the participant's bank accounts, are credited and debited automatically." Ex. 1011 at 306 (emphasis added).

Thus coding, an integral part of generating a VAN, is accomplished electronically, using a hardware component or a computer running a functional block of a computer program to apply an algorithm to transform information.

The system is programmed to automatically determine whether the at least a portion of the received funds transfer information is authentic by "using" the VAN and credential information contained in a credential issued by a trusted party to one of the parties to the funds transfer. The system then makes an intelligent decision concerning the authenticity of the VAN and the at least a portion of the received funds transfer information before transferring any funds from one account to another.

As explained in the specification, the generation of a VAN requires encoding of information, and reading the VAN (using the VAN) also requires decoding or unencoding of information contained in the VAN. Even if, as Petitioner argues, these steps are done by "conventional coders and decoders" (*See, e.g.*, Petition at 7), the determining step of claim 51 is accomplished using a computer under control of a special program that determines the authenticity of the VAN and the portion of received funds information. Ex. 1001, FIGS. 7, 8A and 8B; Col. 4, l. 52-Col. 8, l. 44. Thus, the computer or system becomes a specially tasked machine that carries out a non-generic task that requires an intelligent

decision to be made. This intelligent decision is carried out automatically and electronically, thus providing the technological solution to the problem of authenticating both parties when one of the parties is absent.

### C. Conclusion

For all of the reasons set forth above, Petitioner has not met its burden to demonstrate that the ’302 patent is a covered business method patent. Petitioner has failed to show that the ’302 patent is “financial in nature, incidental to a financial activity or complementary to a financial activity,” much less “an agreement between two parties stipulating movements of money . . . .” *See, e.g., SAP Ametica, Inc. v. Versata Dev. Group, Inc.,* CBM2012-00001, Paper 36, at 21-22; *Apple Inc. v. Sightsound Tech., LLC,* CBM2013-00019, Paper 17, at 11-12. Petitioner has also failed to show that the ’302 patent does not provide a technological solution to a technological problem. Accordingly, Petitioner lacks standing to request Covered Business Method Patent review of the ’302 Patent, and the Petition should be denied.

## VI. ORDINARY SKILL IN THE ART

Patent Owner submits that a person of ordinary skill in the art for the patents-in-suit would likely have the following educational background and experience: (1) undergraduate education in mathematics, physics, computer science, electrical engineering or similar technical subject; and (2) either post-graduate education in networking, cryptography, or other discipline encompassing

information theory, or equivalent experience with applications involving communication of financial, military, medical or similarly sensitive data over secure and non-secure networks.

## VII. PETITIONER HAS NOT SHOWN THAT IT IS MORE LIKELY THAN NOT THAT AT LEAST ONE OF THE CLAIMS CHALLENGED IN THE PETITION IS UNPATENTABLE

As stated in 37 C.F.R. § 42.208(c), to institute a post grant review, a petition must "demonstrate that *it is more likely than not* that at least one of the claims challenged in the petition is unpatentable." As explained in more detail below, Petitioner fails to meet its burden for any of the challenged claims.

### A. Each Of The Challenged Claims Is Patentable Under One Or Both Of 35 U.S.C. §§ 102 and 103

#### 1. Claims 51, 53 and 55 Are Not Anticipated By Davies

##### (a) Explanation Of The Davies Reference

Since Petitioner almost entirely relies on its arguments concerning the Davies reference, it is important to discuss it in detail. Four of the five asserted invalidity grounds depend on Davies as either the sole or primary reference. Davies (published in 1989) is essentially a textbook containing discrete and separate examples, disembodied from one another. Davies discloses diverse encryption and authentication methods, many of which are not enabled, to purportedly authenticate and approve Electronic Funds Transfer Point-of-Sale (EFT-POS) debit card transactions and Automated Teller Machine (ATM) cash withdrawal approvals. Davies also contains discussion of one use of Public Key cryptography

in a section not tied to any example. *See* Ex. 1004 at 254-55. Petitioner's previous attack (in the CBM2015-00013 proceeding) relied mainly on the Davies disclosure of an "electronic cheque." *See id.* at 328-30[4]. Since that failed when the PTAB denied Visa's IPR petition, now Petitioner shifts most of its focus to the ATM embodiment. *See id.* at 330-31; *see also* Paper No. 7, at 29 (showing Petitioner relying on "ATM" embodiment when explaining claim charts). This Preliminary Response discusses all of these in detail.

First, Davies describes two principal types of Point-Of-Sale ("POS") systems. Online systems involve a consumer interacting with a merchant with the intent of purchasing goods or services. In these online scenarios, the merchant swipes the card at a merchant terminal and asks the consumer to enter a secret PIN. For offline POS systems, Davies describes one approach using an electronic "cheque" that is entered into a terminal for processing. The cheque (the previous focus of Petitioner's anticipation theory in the -00013 proceeding) is an electronic document that was previously prepared by the consumer. Offline POS transactions

[4]Patent Owner notes that Petitioner has used the original pagination of Davies, Meyers and other documents rather than using the pagination of the Exhibit, as required by 37 CFR 42.63(d)(2)(i). To avoid confusion, Patent Owner refers to Petitioner's pagination rather than the pagination of the Exhibits.

were formulated so as to process a set of electronic cheques in a batch after they had been entered in a terminal.

**(i) Online Processes in Davies**

In a basic example not relied upon in the Petition, Davies discloses secure online payment services for point-of-sale ("POS") consumer transactions. *See id.* at 311-321. The amount of the transaction, referred to as the "payment amount," is displayed at the POS prior to the consummation of the transaction:

> The sequence of operation is that a sale is agreed between the customer and merchant and the payment amount is displayed for the customer's approval. The customer then passes his card through the card reader on the point-of-sale terminal (usually a simple swipe reader) and enters his PIN on a keyboard attached to the terminal.

*See Id.* at 312. This is similar to contemporary uses of debit cards to buy, for example, groceries.

Davies extends the basic online concepts to a Point-Of-Sale Electronic Funds Transfer ("EFT-POS") system based on public key cryptography. Petitioner relies on this example, but (as explained below) does not attempt to match it to each claim limitation. This system extends the functionality of the POS systems described in Davies, Ex. 1004 at 311-321, in that authentication of the financial transaction capitalizes on a different mechanism. *See id.* at 321-324. The EFT-POS terminal interacting with a consumer at a merchant location has public keys corresponding to the card issuer's processor and a key registry:

> Figure 10.20 shows the secret and public keys held by the main entities which take part and the relationship between them. For example, skT is the secret key held in the terminal and pkT is the corresponding public key held by the acquirer. These keys are *generated by the terminal during its initialization*. Similarly the acquirer, card issuer and key registry *each generate a pair of keys and make the public key known to others*, as shown in the figure.
>
> When any of these entities requires an authentic public key it is received in a message from the card registry containing the key, the identifying data and a digital signature using the registry's key. Before using any public key for the first time, each entity checks its signature in this certificate which it has received. Terminals receive their certificates from the acquirer when they need them.

*See id*. at 322 (emphasis added). Thus, in the EFT-POS example, certificates are used to distribute a party's public key. But the certificates are not transferred or presented by an entity for purposes of determining that entity's identity, which is required under the proper construction of credential.

Davies does not disclose any instance where a party gets its own certificate from the key registry (*i.e.* a party is not issued its own certificate by the key registry). And it does not appear that there is any reason for the key registry to provide a party with its own certificate – the party already holds its own public key. As set forth in Davies, Ex. 1004 at 322, a party generates its own public key and registers it with the key registry.

### (ii) Offline Processes in Davies

The electronic cheque described by Davies is the embodiment that Petitioner previously tried to read on each claim limitation, in its -00013 petition. It remains a focus of petitioner's arguments in this -00044 petition, and thus continues to merit attention. It is equivalent to a bank check. The bank for the electronic cheque is the one holding the account of the customer, against which a debit transaction will be made when a consumer "writes" a new cheque. Davies discloses authentication mechanisms for the "electronic cheque" based on public key cryptographic methods, though employment of a "key registry" within this embodiment is mentioned only for one of the three named participants in the transaction (the "bank").

There are three separate sections in the Davies electronic cheque: (1) the payment information consisting of items 9 through 15, including a signature of those elements by the customer, item 16; (2) the customer identity information, consisting of items 5 through 7, plus a signature of those elements by the issuing bank, item 8; and, (3) the "issuing bank" identity information, consisting of items 1 through 3, plus a signature of those elements by an unidentified / unknown key registry authority, item 4. The consumer starts with a cheque containing items 1-8 and then "writes" cheques as required by filling out items 9-15 and signing the latter items using the consumer's own private key. After this signing, it is used as a means of payment with a merchant. *See id.* at 329.

The bank identity information (items 1 through 3) is digitally signed by the private key of an unidentified / unknown "key registry." The issuing bank information includes the issuing bank's own public key. The customer identity information (items 5 through 7) is digitally signed by the private key of the issuing bank. The customer identity information includes the customer's own public key for use in cheque issue steps.

When a consumer wishes to issue a cheque, he/she determines transaction parameters, such as the amount of the cheque, and generates a digital signature of the payment information using the customer's private key. The signature is stored as item 16 in Davies. *See id.* at Figure 10.22. Davies discloses more detail about the bank and customer identity sections of the cheque than the payment information section:

> The implementation of an electronic cheque requires technically little more than a digital signature facility with a key registry to authenticate public keys. A hierarchy of keys is proposed in which a registry authenticates the bank's public key and the bank authenticates the customer's public key. In order to allow the content of the cheque to be validated with a minimum of data beyond the cheque itself it should contain all the items listed in Figure 10.22. These items fall into three sections. The first is, in effect, a certificate by the key registry which authenticates the bank's public key. It also includes an expiry date so that the bank need not worry that an old signature is being used after it has expired. Anyone can verify the bank's public

> key using the signature and the public key of the key registry, which is available in many different places to avoid falsification. The key registry could be the central bank of a country, for example.

*See id.* at 328. As just quoted, only the bank's public key (not the customer's) receives treatment by the unidentified key registry. The only purported "certificate" on the cheque is that which authenticates the bank's public key. Importantly, the cheque itself does not identify the key registry who issued the bank's "certificate."

A customer can issue an electronic cheque by signing the cheque using the customer's private key. The private key belonging to the customer is described as being held on an "intelligent token or 'smart card.'" *See id.* at 329. Davies contains almost no disclosure of what is done with the customer's signature, except that a merchant "can verify" it. *See id.* at 330. Other, detached parts of Davies mention using a public key to transform the signature into its original "plaintext." *See id.* at 254-55. Thus, these unrelated portions of Davies do not disclose the merchant verifying a received customer signature by regenerating the signature using the cheque's variable information. The merchant's inability to regenerate the signature is not unexpected – the merchant does not possess the customer's secret key and could not do so. The merchant must instead decode the customer's signature using the public key of the customer.

The merchant, however, does not have a basis to rely on the customer's public key because the customer information (items 5-7) is signed by the customer's bank, and the customer's bank's information (items 1-3) is signed by an unidentified "key registry." Because the check itself does not identify the key registry, the merchant lacks critical information (the correct key registry's public key) to verify the bank information (items 1-3). And because the bank's "certificate" cannot be verified, neither can the customer's public key.

Nowhere does Davies disclose a customer receiving *from a trusted party* a certificate with the customer's own public key. While the customer sees his or her own public key in section 2 of the cheque (which he/she presumably generated him/herself some earlier time), nowhere does Davies disclose the issuing bank (who "signs" the customer information in section 2 of the cheque) being a trusted party in this transaction. Finally, nowhere does Davies disclose the customer presenting anything in the customer identity section of the cheque to determine the customer's identity. The customer information is there instead to merely associate a public key of the customer with the customer.

**(iii) ATMs in Davies**

The concept of an "electronic cheque" disclosed by Davies leads to a disclosure of dispensing cash at an ATM terminal. *See id.* at 331. The customer can deliver an electronic cheque to the terminal and receive cash in return:

> The ATM checks the signature, to avoid passing ineffective messages in to the system. If it is correct, the 'cheque' passes via the payer bank, A, to the card issuer bank, B. Here the signature is checked and the customer's account examined and, if everything is in order, debited. A payment message signed by B is sent to A. The message and its signature are checked and if all is well an authorization goes to the ATM to release the money.

*See id.* at 331. But this is not the same cheque. It is one that lacks a "second party" account identifier. As just indicated above, the parties involved are the customer, the payer bank (dispensing the cash) and the card issuer bank processor. The payer bank, replacing the merchant in other scenarios, is credited with the amount of the transfer. Like all conventional ATM transactions, the ATM transactions Petitioner points to in Davies involve an account of only ***one*** party – the person withdrawing currency. *See id.* (noting that "ATM request" is a distinct "transaction type" from "customer cheque," and involves solely an ATM to "release the money" to the customer).[5]

### 2. Davies Does Not Anticipate

The PTAB previously denied institution because the cheque embodiment did not satisfy the sequence whereby the "receiving" step must occur before the

[5] As explained in note 3, above, Petitioner's misleading argument that *Mr. Stambler* somehow ratified that ATM withdrawals include both a "first" and "second" party to a "transfer" should be rejected.

"generating" step. This mooted any need to reach additional distinctions. According to this analysis, the bank "receives" the cheque ***after*** a digital signature (the putative VAN) was made on it, not before. That a cheque was complete unto itself before the bank received it doomed the Davies invalidity attack.

With this "roadmap" now provided by the PTAB, MasterCard tries (but fails) again. In this proceeding, MasterCard shifts the focus from the ***bank's*** receipt of a completed cheque to the substeps that the ***consumer*** takes to formulate his or her own signature. This happens when the consumer provides the transaction information to the consumer's own "token" or "intelligent smart card." But MasterCard simply creates more problems for itself in repudiating its previous Davies assertions. For instance, the consumer in Davies gives the bulk of the cheque information to his or her own "intelligent smart card" to perform such digital signature processing. Under MasterCard's theory, this means that the consumer would "receive" the funds transfer information from himself or herself. But this ignores that nothing is "received" if it does not change hands. Consider that one cannot "receive" a physical object by simply passing it from one hand to another. Thus, MasterCard's effort to correct one logical flaw simply leads to another.

In the meantime, Davies also does not anticipate for several additional reasons that the PTAB did not need to reach in the previous institution decision. It does not disclose the "credential" of claim 51. It does not disclose that what

Petitioner calls a credential was "issued by" a trusted party. And it does not disclose, in the ATM embodiment, the involvement of an account of a second party. Therefore, the Petition fails to show that it is reasonably likely that Davies anticipates claims 51, 53 or 55.

### (a) The Petition Erroneously Conflates Numerous Unrelated Embodiments

At the outset, Petitioner's discussion and application of Davies conflates different unrelated disclosures. For example, the Davies section of the Petition begins by discussing Davies' description of funds transferred from Ann's bank account to Bill's (Paper No. 7, at 24, discussing Ex. 1004, Davies p. 285), but also the electronic cheque embodiment (*Id.* at 24-25). It then without explanation refers to yet a different section of Davies, to discuss the nature of key registries. (Paper No. 7, at 25, discussing Ex. 1004, Davies pp. 276-77). On the next page, the Petition meanders to a discussion of the ETF-POS embodiment, and its idiosyncratic discussion of public key generation and registration. (Paper No. 7, at 25-26, discussing Ex. 1004, Davies p. 322). In fact, Petitioner's claim charts that purport to show anticipation by Davies (Paper No. 7, at 24-34) do not settle on a single particular embodiment within Davies to attempt to map onto the claim limitations. This alone is fatal.

A single embodiment from a prior art reference must contain every claim limitation, arranged as in the claim, for there to be anticipation. Neither the courts

nor the PTAB permit mixing and matching from separate unrelated disclosures within a prior art reference. *Synqor, Inc. v. Artesyn Techs., Inc.*, 709 F.3d 1365, 1375 (Fed. Cir. 2013) ("Even if the Mweene Thesis discloses each discrete element of each claim Defendants assert is anticipated, the thesis does not disclose those elements arranged as required by the claim."); *Net MoneyIn, Inc. v. Verisign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) ("Thus, it is not enough that the prior art reference discloses part of the claimed invention, which an ordinary artisan might supplement to make the whole, or that it includes multiple, distinct teachings that the artisan might somehow combine to achieve the claimed invention."); *In re Arkley*, 455 F.2d 586, 587 (CCPA 1972) ("Thus, for the instant rejection under 35 USC 102(e) to have been proper, the Flynn reference must clearly and unequivocally disclose the claimed compound or direct those skilled in the art to the compound without any need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference."); *Printing Industries of America v. CTP Innovations*, LLC, IPR2013-00474, Paper No. 16, at 11-12 (PTAB Dec. 31, 2013) ("The court [in *Net MoneyIn*] reasoned that a prior art reference that 'includes multiple, distinct teachings that the artisan might somehow combine to achieve the claimed invention' is insufficient to show prior invention. *Id.* This principle applies here, because PIA relies on at least two distinct embodiments in Lucivero to show anticipation of claim 1."); *Ex parte Cucerzan*, Appeal 2009-008190; Appl. No. 11/094,078; Decided May 2, 2011,

citing to *Net MoneyIn* ("Because of the Examiner's reliance on multiple distinct embodiments in Shazeer, we are in accord with the Appellant that the elements of the claimed invention are not identically shown in the reference, arranged as they are in the claims."); *Ex parte Omshehe*, Appeal 2009-0883; Appl. No. 09/954,509; Decided July 14, 2009 ("such a mix[ing] and match[ing] [of] elements from Redding's two distinct authorization modes is inappropriate for a rejection based on anticipation. Therefore, the Examiner fails to show every element of the claimed invention arranged as in the claims." (Decision, p. 6.)).

As discussed below, the cheque embodiment – the main one that Petitioner actually charts, and that Petitioner apparently contends can be mixed with the ATM embodiment to build its argument – lacks many claim limitations and thus cannot anticipate.

**(b) The Cheque Embodiment Does Not Disclose the Claimed "Credential"**

The Davies cheque embodiment does not disclose a "credential" as claimed. Petitioner points to the "electronic cheque" as a whole as the "credential," and the customer's public key (item number 6) as the non-secret credential information. Paper No. 7, at 27.[6] Petitioner is incorrect.

[6] Inconsistently, the Petition also states in a different section that the "certificate" is the "credential." Paper No. 7, at 32. But this is plainly wrong, since Davies does

The electronic cheque is not transferred or presented for the purpose of determining the identity of a party. Instead, it is presented to cause the transfer of funds from a customer's account to a merchant's account. Davies states, "A terminal is needed in order to generate a cheque, sign it with the aid of the token and send it to the beneficiary." *See* Ex. 1004 at 329. Davies strongly implies, and it is natural to assume, that such cheques are negotiable instruments, and therefore by definition can be presented by anyone to anyone. By design, the "electronic cheques can be easily copied." *Id.* "The cheque is more versatile [than a smart card used for point-of-sale payment] because it can be sent to anyone who has a means of recording the data and presenting them at a bank. No secrets are present at the terminal." *Id.*

Indeed the "service provider collects the cheques and presents them in batches to its bank for payment," while likewise, the merchant's terminal "collects the cheques . . . and presents these cheques to its bank in a convenient batch." *Id.* at 330. Thus, a single cheque cannot qualify as a document or information transferred to establish the identity of a party, which in this case is the customer. Davies discloses that either the "customer" or the "merchant" / "service provider" may be in possession of the same cheque, and may each "present" it in separate instances.

---

not disclose any "customer certificate" on the cheque, only a bank certificate. Only the bank information is signed by the key registry.

This is anathema to a document used to either "determine" identity of the party transferring it.

**(c) The Cheque Embodiment Alleged "Credential" is not "Previously Issued by a Trusted Third Party"**

Nor is the cheque "*previously issued* by a trusted third party," which is a requirement of claim 51. First, it is not "previously issued" with respect to the steps of the claim. It is, in fact, generated in tandem with the "generating" step. In other words, no electronic cheque exists until payment information has been entered by the customer and a signature by the customer has been "generated." Here, at least one claim step must be performed before what Petitioner calls the credential comes into existence. Inconsistently, the Petition also states in a different section that the "customer certificate" is the "credential." Paper No. 7, at 32. But this is plainly wrong, since Davies does not disclose any "customer certificate" on the cheque, only a bank certificate. Only the bank information is signed by the key registry.

Second, using the District Court's construction, a "trusted party" is "an entity / party that has the authority, as recognized by participants in the relevant system or method, to establish or confirm a party's identity." In Davies, the "issuer" of the cheque is either the customer or the terminal of the merchant – neither of which is a trusted party. As already mentioned, Davies states, "A terminal is needed in order to generate a cheque, sign it with the aid of the token

and send it to the beneficiary." *See* Ex. 1004, at 329. This "terminal" can be a "merchant's terminal." *Id.* at 330. More generally, it is "any intelligent terminal which has the interface for connecting the token and a PIN keyboard or a pad for a dynamic (manual) signature, whichever of these is used to protect the token." *Id.* at 329. One example of such a terminal is "a theatre ticket issuing machine." *Id.*

The Petition seeks to avoid the "previously issued" problem by assuming (without revealing this assumption) that claim 51's preamble is worded differently from how it actually is. Namely, the Petition explains at length how the *public keys* within the body of the cheque are "previously issued." Paper No. 7, at 27. But that is irrelevant to the claim language. Even assuming for the sake of argument that such public keys might meet the "non-secret credential information" limitation of the preamble (a contention the Petition makes on page 27 with regard to the customer's public key), the claim does *not* call for only the "credential information" being "previously issued." Claim 51 instead calls for "a *credential* being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret" (emphasis added).

The Petition's avoidance of the "trusted party" problem is, if anything, even more troubling. Petitioner attempts to state that the public key issued to the customer and stored in a key registry means that the public key was "issued . . . by a trusted party." *See, e.g.,* Paper No. 7, at 25-27. This avoids the true question – whether the alleged *credential* (not the alleged "credential information") was

issued by a "trusted party." Even if Petitioner could skirt that deficiency, Petitioner points to nowhere in Davies disclosing that the "key registry" has any role to play with respect to the customer's public key in the cheque embodiment itself. In the cheque example, only the *bank's* public key is distributed by the key registry, not the *customer's*.

Other than these misguided attempts, Petitioner makes no effort to show that what it points to as the *credential* (the whole cheque itself) was previously issued. It cannot. And it makes no effort to show that the various terminals that actually issue such cheques are "trusted parties," again because it cannot.

**(d) The Cheque Embodiment Does Not Disclose A VAN**

Petitioner argues that, even though the "generating step" occurs after the funds transfer information is received, and requires the use of at least a portion of the received funds transfer information, that a signature on the check is a VAN. Paper No. 7, at 55. This, of course, is not possible, as Petitioner admits that the electronic cheque is pre-signed. *See* Paper No. 7, at 29; Ex. 1020, Diffie Decl. at ¶ 70. A signature already applied to the check before it is tendered cannot be a VAN that is formed from at least a portion of received funds transfer information.

Moreover, Petitioner simply concludes that, based on Petitioner's construction of VAN, that a signature qualifies as a VAN. While Petitioner relies on Diffie's Declaration for support, in reality Diffie merely describes what a digital signature or signature described in Davies is, not how such a signature is the same

as the VAN described and claimed in the '302 patent. *See* Ex. 1020, Diffie Decl. ¶ 51 (Note, although cited to, ¶ 81 refers to Meyer, not Davies; ¶ 131 refers to Nechvatal; and ¶ 153 of Diffie refers to Fischer. Combining references in this manner is not appropriate for an anticipation analysis).

Regarding the ATM embodiment described in Example II of 51(b), Petitioner does nothing more than argue that a message is signed and returned to the ATM. This statement is not supported by any reference to Diffie's Declaration. In fact, Petitioner's own claim chart states "'[t]he customer's request is formed into a message and presented to the token. Here it is signed and returned to the ATM.'" Paper No. 7, at 30. Again, this purported signature is signed using a public/private key; it is not formed from the received funds transfer information, as required by the challenged claims.

**(e) The Cheque Processed Through the ATM Embodiment Does Not Involve a Second Account**

As mentioned previously, Petitioner seeks to cure deficiencies by increasing reliance on the ATM embodiment. Petitioner points to its discussion of cheques being processed through such devices. However, these are not the same cheques at all. Davies makes it clear that the so-called cheque is simply used at an ATM to release currency. Ex. 1004 at 330-31. In contrast, claim 51 foundationally and fundamentally involves the transfer of funds between respective accounts of two

parties – a "first" party and a "second" one. At least the "second" account is missing from a cash-withdrawal scenario.

**(f) The Non-Pertinent Embodiments Also Lack Specific Claim Limitations**

As mentioned above, Petitioner failed to make any argument that any embodiment besides the cheque embodiment within Davies reads on every limitation of the challenged claims. However, even if the Board accepts Petitioner's invitation to "mix and match," other claim limitations are missing from these waived embodiments.

For the preamble limitation 51PreA, "Example I," Petitioner points to a part of Davies that merely diagrams the preexisting check clearinghouse system that had existed for decades before. Paper No. 7, at 24. Yet the Petition lacks any mention of this embodiment for the rest of its charting of claim 51. It in fact lacks virtually all claimed steps of claim 51.

For the preamble limitation 51PreB, "Example I," Petitioner chose yet a different part of Davies – one that contains a generic description of key registries and digital signatures, disembodied from any application such as funds transfers. Paper No. 7, at 25-26. It also lacks virtually all claimed steps of claim 51.

For the "generating" step (51b), "Example II," Petitioner points to Davies' ATM example. Paper No. 7, at 29-30. The substance of the citation refers to the ATM sending various transaction items to a customer's token (where a private key

is located) so that the customer might "sign" it. The Petition only contains mention of this embodiment in the rest of its charting of claim 51 at the "receiving" step (51a) and "transferring funds" step (51d). And it, too, lacks virtually all claimed steps of claim 51.

For the "determining" step (51c), "Example II," Petitioner creates a patchwork of three different citations all for one "example." Paper No. 7, at 30-31. To the extent this goes beyond the electronic cheque embodiment, it involves generic discussion of digital signatures disembodied from any financial system. It, too, lacks virtually all claimed steps of claim 51.

Finally, as mentioned, for the "transferring funds" step (51d), "Example II," Petitioner re-injects the ATM example that is otherwise largely ignored in the remaining parts of the chart. Paper No. 7, at 33.

**3. Meyer Does Not Anticipate**

Three of the five asserted invalidity grounds depend on Meyer as either the sole, primary or secondary reference. Meyer (published in 1982) is, like Davies, a textbook containing discrete and separate examples, disembodied from one another. Meyer discloses diverse encryption and authentication methods, many of which are not enabled. Petitioner had already charted Meyer long before it filed its first proceeding (CBM2015-00013), but did not cite it there. Ex. 2002, at 15; Ex. 2003. Meyer is newly asserted in this proceeding (CBM2015-00044).

The cited sections of Meyer divide into three separate embodiments. First, Petitioner cites a large page swath (pp. 429-73, cited at Paper No. 7, at 50), which in material part simply republishes a pamphlet of MasterCard itself explaining many ways that future technology might be deployed to implement PIN-based electronic funds transfers. Ex. 1022 at 429, 432-33 (*e.g.*, weighing relative merits of four-digit versus six-digit PINs). Necessarily, the focus is on point-of-sale terminals in which a consumer would not convey whose account would receive a funds transfer. Second, Petitioner cites an example of a grocer (Paper No. 7, at 38-39). Here, Meyer contemplates another framework for consumer use of PINs during electronic funds transfer for point of sale purchases. Ex. 1022, at 475-77. The grocer is already hard-wired into an electronic funds system, and there is no reason why a consumer would need to list a grocer's account during a purchase transaction. Nor is there any indication in the reference that the consumer would be able to identify the grocer's account. Finally, Petitioner cites Meyer's proposition of yet a different framework, untethered to any real world example: a generic system that involves consumer-held PINs used to extract private keys from a consumer-held card. (Paper No. 7, at 38-39, 42-43, citing Meyer at 569, 578, 583, 590-92 and 597). Petitioner points out that this private key is then used to sign transaction information, Mreq. (Paper No. 7, at 42-43 ). But this embodiment fails to disclose what components exist within Mreq. Put simply, Meyer does not

disclose there being ***both*** consumer ***and*** merchant account information within Mreq.

Thus, Petitioner's use of Meyer mirrors Petitioner's misuse of Davies. Petitioner mixes unlinked embodiments within Meyer that do not relate to one another, to stitch together what it believes will work as an anticipation contention. In fact, the distinct embodiments are incommensurable. For example, the grocer embodiment discloses that a PIN entered by a consumer will be checked against stored PINs at the consumer's issuer bank. Ex. 1022, at 477. Putting aside the profound insecurity of such a protocol (PINs stored in plaintext / traveling in plaintext over communication lines), it is simply wildly distinct from what Meyer later discloses. In the later-disclosed generic example, the PIN does not travel over communication lines in any way. Instead, *within a consumer's intelligent card,* the PIN is exclusive-or'ed with (*i.e.*, unlocks) a quantity stored on a consumer's card in order to extract a consumer's private key. Then, the private key is itself is used for conventional asymmetric encryption processes but is never transmitted. Ex. 1022, at 591-92. This shows that one part of Meyer cannot carry over into another. As discussed above, Petitioner errs to mix embodiments to construct an anticipation contention.

In short, mere disclosure of PINs, asymmetric keys, signatures and funds transfers do not make Meyer an anticipatory reference.

Additional reasons preclude Meyer from anticipating Mr. Stambler's claims, including at least the following:

**No trusted third party issuing credentials**. In addition to the above, Meyer does not disclose a trusted third party issuing any credentials. In its most pertinent disclosure, Meyer simply discloses that the consumer's bank (the "issuer") will fabricate a key pair for the consumer – $PK_c$ (public key) and $SK_c$ (private key). Ex. 1022, at 591. Petitioner asserts that it is *this* public key that constitutes the credential and/or the credential information. Paper No. 7, at 38-39. But nothing justifies labeling the consumer's bank as a trusted third party.

To read on the claimed "credential," Petitioner cites the public key algorithm discussion at Meyer page 569. Paper No. 7, at 39 (calling the referenced public key a "credential"). This, too, is wrong. The discussion at page 569 relates to what ***institutions*** might deploy by way of security when they ***communicate with each other.*** Ex. 1022, at 569 ("Each institution would have a public and private key, Pk and Sk, respectively."). Citing this language, MasterCard points to the public key assigned to an institution as the recited credential. But the "institution" is neither the first party nor the second party identified by MasterCard on the previous page, and does not have an "account" in this context. Therefore, not only is there no "trusted party" issuing credentials to a consumer, MasterCard's petition wholly fails to assert that either the first party (the customer) or the second party (the grocer) was ever issued a credential.

Petitioner also errs to contend that a public key held by a non-party institution is a credential "previously issued to at least one of the parties by a trusted party." In fact, the portion of Meyer cited by MasterCard expressly states that "each user defines his own secret key and corresponding public key." Thus, even if a public key was a credential, Meyer makes clear that the public key is created by a party itself and not issued to it by a "trusted party."

**No Account of a Second Party**. As already mentioned, Meyer's embodiments – even if they could be somehow linked – do not mention an account of a second party within the transaction information (Mreq). Mr. Stambler's claims require that an account of a second party must exist within the funds transfer information. Again, if a point of sale terminal already resides within a hard wired funds transfer network, a consumer would have no need to tell the merchant who it is, and Meyer's failure to disclose this limitation makes sense within its narrow context.

Again, Petitioner's contentions reveal the fundamental error. Petitioner's chart for element 51PreA cites exclusively the grocer example and identifies "suitable routing information" as "information for identifying the second account of the second party". Paper No. 7, at 35-37. But nothing in Meyer supports MasterCard's assertion that the "suitable routing information" identifies the grocer's account. In fact, other portions of Meyer clarify that routing information pertains to the first account of the first party, much like the "institution code" that

is the "first several digits of the personal account number." Ex. 1022, at 566. But even if the "suitable routing information" pertained to the grocer's account, it would merely identify the grocer's banking institution, and not the grocer's account. Therefore, on its own terms, Petitioner has not identified any account information of a "second party" to a funds transfer as something that is received during the steps that Meyer discloses.

**No Receipt of Funds Transfer Information**. Similar to how it treated Davies, to avoid the sequence issue that doomed Visa's IPR petition, Petitioner relies on Meyer disclosing that the intelligent smart card itself (*i.e.*, the physical object that holds a consumer's private key) "receives" funds transfer information to make a signature (a putative VAN). Paper No. 7, at 39-41. While it is true that Meyer discloses the intelligent smart card holding the private key, and performing the calculations to construct a signature, the person operating the card is the same individual who provides it with the funds transfer information. Just as with Davies, it makes no sense to assert that the consumer "receives" the funds transfer information from himself or herself. Again, shifting something from one hand to another does not indicate "receipt" by the person doing the shifting.

Further, Petitioner relies on Diffie, its expert, only for the propositions that a public key is a credential and a key distribution center ("KDC") is a trusted party, and that a customer's public key would qualify as credential information. Paper

No. 7, at 39. As stated previously, a public key cannot be both a credential, as that term is used in the '302 patent, and credential information.

Notably, Petitioner includes not a single reference to Diffie's Declaration to support its argument that Meyer teaches generating a VAN. Moreover, Petitioner and Diffie both misperceive Meyer; Meyer clearly states KDC merely stores public/private keys that are provided to the KDC by a user; the KDC is not a trusted party that issues the keys. Ex. 1022 at 578.

For the foregoing reasons, Petitioner does not succeed in overcoming any gaps in its previous petition (in the -00013 proceeding) to assert Meyer against Mr. Stambler's claims 51, 53, 55 and 56.

#### 4. Claims 51, 53, 55 and 56 Are Not Obvious Under Davies in View of Meyer

Since neither Davies nor Meyer anticipate for all the reasons shown above, their combination cannot render the claims obvious. The absence of a claim element within the prior art combination forecloses an obviousness ground. *See, e.g.*, *Fresenius USA, Inc. v. Baxter Int'l, Inc.*, 582 F.3d 1288, 1301-1302 (Fed. Cir. 2009); *CFMT, Inc. v. Yieldup Int'l Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003); *In re Royka*, 490 F.2d 981, 985 (CCPA 1974); *Petter Inv., Inc. v. Hydro Eng'g, Inc.*, 2009 U.S. Dist. LEXIS 81003, at *29-30 (W.D. Mich. Sept. 8, 2009); *Cynosure, Inc. v. Cooltouch Inc.*, 660 F. Supp. 128, 132, 134-35 (D. Mass. 2009); *Oxford Gene Tech. Ltd. V. Mergen Ltd.*, 345 F. Supp. 2d 431, 437 (D. Del. 2004).

Petitioner's obviousness combination depends on the premise that the ***only*** claim limitation missing from Davies is the proper sequencing of the "receiving" step occurring before the "generating" step. Paper No. 7, at 50-51. Petitioner asserts that Meyer – in a section not otherwise relied upon – discloses a sequencing of receiving funds transfer information before generating a message authentication code (a MAC). *Id.* Petitioner concludes that a person of skill in the art would be motivated to augment the teachings of Davies with this purported proper sequencing. *Id.* Petitioner's premise is flawed. As shown above, more is missing in Davies (and Meyer) than the claimed sequencing.

Even putting the flawed premise aside, Petitioner's argument fails on its own terms. Petitioner points to the disclosure in Meyer of an "originator" (*i.e.,* a consumer) creating his or her own MAC at the outset of a transaction. Paper No. 7, at 51 (citing Ex. 1022, at 457-58). This does not reflect any kind of "receipt" of funds transfer information before a generating step. As already discussed, a person cannot "receive" such information from himself or herself – that makes no sense.

The obviousness attack contains additional flaws. For example, Petitioner cites no evidence – only conclusory statements – that any reason or motivation existed to combine any aspect of Davies with any aspect of Meyer. Paper No. 7, at 50-51 That is not sufficient. *Synopsis, Inc. v. Mentor Graphics Corp.*, IPR2012-00041, Paper No. 16, at 14 (22 Feb. 2013) (dismissing obviousness challenge where petitioner "does not clearly provide analysis" and "has not provided

sufficient reasoning or facts"). Nor could any such evidence reasonably be expected to exist. Meyer is a 1982 textbook that teaches a variety of data security concepts. Davies is a 1989 textbook that also teaches a variety of data security concepts. Each is a whole encyclopedic reference unto itself. Neither purports to reveal any gap in its teachings that might be filled by consulting any other reference.

Dependent claims 53 and 55 do not need additional analysis because Petitioner does not seek to apply any disclosure from Meyer to augment its preexisting Davies contentions as to those claims. Claim 56 is different. Petitioner does contend that parts of Meyer read on the added requirements of that claim. In particular, Petitioner contends that the second VAN (named VAN1 in claim 56) exists in Meyer as the "secret card parameter, SKc*." Paper No 7, at 48-49. However, Petitioner has mismatched its own contentions once again. Claim 56 requires that VAN1 be used "to secure at least a portion of ***the credential information*** to the at least one party." In its claim 51 contentions, as discussed previously, Petitioner has alleged that Meyer's discussion of a ***public*** key amounts to the claimed credential information, in order to meet the requirement of the claim 51 preamble that it be non-secret. But in its claim 56 contentions, the non-secret requirement fell by the wayside, since Petitioner now points to something undisputedly "secret" (*i.e.*, SKc*) as the alleged credential information. As discussed before, this quantity within Meyer resides on a consumer's card, and

when exclusive-or'd with the secret PIN, yields the secret key SKc. Therefore, Meyer does not disclose the added feature of claim 56, supplying yet one more reason why the Davies/Meyer combination does not render any claims obvious.

### 5. Claim 55 Is Not Obvious Under Davies or Meyer In View Of Nechvatal

The Petition next asserts that Davies in view of Nechvatal renders obvious claim 55. Paper No. 7, at 66-68. The Petition is not correct. The Petition does not establish a reasonable likelihood that this ground will succeed. The added material in Nechvatal does not disclose the claim elements demonstrated to be missing, above. And the Petition does not assert a proper "reason to combine" that would allow the combination in the first place. The PTAB declines to institute review on obviousness grounds when the cited secondary references do not make up for the deficiencies in the primary reference. *See, e.g., Square, Inc. v. Cooper*, IPR2014-00156, Paper No. 9, at 20 (15 May 2014).

For claim 55, Petitioner's chart cites alleged hashing technologies in *all three* references, but those technologies so charted are alleged to read on the limitation of claim 55 in the same way. In other words, the combination does not add anything, if one takes Petitioner's contentions at face value. Thus there would be no reason to make the combination. The mere fact that elements separately existed in the prior art would not render an invention obvious. *Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1354 (Fed. Cir. 2013). For obviousness, there must be

proof of a legally sufficient "reason to combine" as well. *Id.* (where reason to combine is absent, cannot assume artisan would be "awakened" to modify prior art); *Synopsis, Inc. v. Mentor Graphics Corp.*, IPR2012-00041, Paper No. 16, at 14 (22 Feb. 2013) (dismissing obviousness challenge where petitioner "does not clearly provide analysis" and "has not provided sufficient reasoning or facts"); *Square, Inc. v. Cooper*, IPR2014-00158, Paper No. 8, at 30 (15 May 2014) (dismissing obviousness challenge where primary reference already had the capabilities that the secondary reference would provide with its added disclosures).

The PTAB declines to grant, and dismisses, petitions that are based on incorrect or insufficient showings under these applicable legal standards. *See generally Synopsis*, IPR2012-00041, Paper No. 16. It should do so here as well. Just because Davies or Meyer and Nechvatal might overlap in certain teachings does not suggest that there are reasons that would have motivated a combination. In fact, the opposite is true. Where each reference is *hermetic, effective on its own terms, and self-contained*, with no gaps that need to be plugged and no invitation to search for improvements, there is no reason to combine. *Accord, Square, Inc. v. Cooper*, IPR2014-00158, Paper No. 8, at 30.

### 6. Claim 56 Is Not Obvious Under Davies or Meyer In View of Fischer And Piosenka

Finally, regardless of the outcome of the rest of the Petition, the PTAB should at least deny the request to institute trial over claim 56. Petitioner only challenges dependent claim 56 on a single ground. Petitioner's attack is a three-reference combination, with Davies serving as the primary reference and Fischer and Piosenka allegedly supplying secondary reference material.

For the legal reasons cited in the above section concerning the combination of Davies or Meyer and Nechvatal, trial should not be instituted when the proposed secondary references do not make up for the gaps in the primary reference. That is the case here.

Petitioner cites Fischer's disclosure of a way to validate a public key contained within a certificate. Paper No. 7, at 70 (citing a message sender's certificate having "a hierarchy of all certificates and signatures by higher authorities that validate the sender's certificate."). This means that Petitioner focuses on a section of Fischer having nothing to do with the claim limitations of claim 51 (the parent claim) noted to be missing from Davies above. As for Piosenka, Petitioner solely relies upon the disclosure of declining access if authentication is unsuccessful. Paper No. 7, at 70-71. This, too, has nothing to do with claim 51's missing limitations from Davies. As previously stated, when the cited secondary references do not make up for the deficiencies in the primary

reference, the PTAB will not institute a trial on that ground. *Square, Inc. v. Cooper*, IPR2014-00156, Paper No. 9, at 20.

The asserted "reason to combine" is also insufficient. Petitioner proffers no explicit argument regarding a "reason to combine." Petitioner simply cites Exhibit 1020, the Diffie Declaration ¶ 158. Paper No. 7, at 69.

Diffie paragraph 158 merely asserts that Fischer discloses using "signatures by higher authorities" to verify a sender's certificate. That simply begs the question. The Diffie Declaration does not give any explanation why a person of skill in the art at the time of Mr. Stambler's inventions would have had a reason to add hierarchical signature validation to what Davies discloses. Thus, the Diffie Declaration amounts to rank hindsight speculation. Davies is self-contained, and does not portray itself as needing any improvement in this regard.

Likewise, Diffie paragraph 174, regarding Piosenka, merely states that when "the certificate signature or the message signature does not verify successfully, the recipient denies the transaction." But again, why go to Piosenka for such a thing if it is already there in Davies? Petitioner does not explain.

## VIII. CONCLUSION

For at least the foregoing reasons, the serial attacks against Mr. Stambler's '302 patent must stop. The PTAB may use its discretion to do so. Independently, '302 patent is not a covered business method patent. Moreover, Petitioner has failed to show that it is more likely than not that any of claims 51, 53, or 55-56, the

only claims challenged in the petition, will be found unpatentable. Therefore, Patent Owner respectfully requests that the Petition for covered business method patent review of the ’302 patent be denied.

Dated: April 10, 2015

/s/ Robert P. Greenspoon
Robert P. Greenspoon, *Lead Counsel*
(Reg. No. 40,004)
Flachsbart & Greenspoon, LLC
333 N. Michigan Ave., Suite 2700
Chicago, IL 60601
Telephone: (312) 551-9500

/s/ John K. Fitzgerald
John K. Fitzgerald, *Back Up Counsel*
(Reg. No. 38,881)
RUTAN & TUCKER, LLP
611 Anton Boulevard, 14th Floor
Costa Mesa, California 92626
(714) 661-5100

Joseph C. Drish (agent), *Back Up Counsel* (Reg. No. 66,198)
Flachsbart & Greenspoon, LLC
333 N. Michigan Ave., Suite 2700
Chicago, IL 60601
Telephone: (312) 551-9500

Counsel for Patent Owner, Leon Stambler

**CERTIFICATE OF SERVICE**

I hereby certify that on this 10th day of April, 2015, true and correct copy of the foregoing Patent Owner Leon Stambler's Preliminary Response to MasterCard International Inc.'s Petition for Covered Business Method Patent Review, was served, in accordance with the parties' electronic service agreement, by electronic mail upon the following lead and backup counsels of record for Petitioner MasterCard International, Incorporated:

| | |
|---|---|
| Robert C. Scheinfeld<br>Eliot D. Williams<br>BAKER BOTTS LLP<br>30 Rockefeller Plaza,<br>New York, NY 10112<br>robert.scheinfeld@bakerbotts.com<br>eliot.williams@bakerbotts.com | |
| | |

Dated: April 10, 2015

/s/ Robert P. Greenspoon

Robert P. Greenspoon, *Lead Counsel*
(Reg. No. 40,004)
Flachsbart & Greenspoon, LLC
333 N. Michigan Ave., Suite 2700
Chicago, IL 60601
Telephone: (312) 551-9500