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 RESPONSE TO MASTERCARD INTERNATIONAL INC.'S PETITION FOR COVERED BUSINESS METHOD PATENT REVIEW

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

USPTO Proceedings

I. INTRODUCTION

The Institution Decision (Paper No. 10) carefully and correctly noted that institution of trial was preliminary, and was based solely on the record as it then existed. Now that the record has been more fully developed – including numerous deposition admissions from MasterCard's hired expert and clarifications of the prior art from Mr. Stambler's – the PTAB should conclude that MasterCard did not meet its burden of proving invalidity of the last remaining asserted grounds. For the reasons that follow, Mr. Stambler respectfully requests that the PTAB affirm the validity of claims 51, 53, 55 and 56 over MasterCard's remaining prior art.

II. REASSERTION OF LACK OF CBM STANDING

Mr. Stambler understands that the PTAB rejected his argument from the Preliminary Response that there is no Covered Business Method jurisdiction over his '302 Patent. Mr. Stambler also understands that the issue is preserved for appeal without further presentation, based on recent Federal Circuit case law. To the extent necessary, Mr. Stambler continues his objections to PTAB jurisdiction over these proceedings because his patent does not qualify as a business method patent.

III. RELEVANT BACKGROUND ABOUT THE '302 PATENT

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.

As will be shown, Figures 8A and 8B (with their related written description text) convey the most important intrinsic evidence concerning the dispositive claim construction issues in this case. That is because the sole independent claim under review – claim 51 – refers to a "method for authenticating the transfer of funds." The patent directly links the teachings of Figure 8B to "the authentication process when the check is presented to be cashed." Ex. 1001, Col. 3, ll. 5-6; Col. 5, ll. 55-58. MasterCard's expert essentially agreed that Figure 8B and its related text provides the Section 112 written description support for claim 51. Ex. 2005, at 18:20-22 ("It appears to me that all four of those steps are performed in figure 8B that we've just been looking at in Stambler's embodiment.").

It is helpful to start discussion with events that occur before the actual (and crucial) claimed funds transfer authentication process. 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 "the authentication process when the check is presented to be cashed." Ex. 1001, Col. 3, ll. 5-6; Col. 5, ll. 55-58. In FIG. 8A, the check recipient first enters his PIN into a bank or home terminal. Ex. 1001, Col. 5, ll. 62-66. That terminal "communicates via a network of the banks involved in the transaction." Ex. 1001, Col. 5, ll. 57-58. 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*. 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.

Significantly, FIG. 8B illustrates that all of the steps of claim 51 take place at the originator's bank. Ex. 2005, at 18:1-20:15. The originator's bank receives the funds transfer instructions and the VAN from the recipient's bank, which is requesting authorization to pay (claim 51's "receiving" step, to be discussed below). Ex. 1001, Col. 6, ll. 43-45. Using the originator's TIN (*i.e.*, non-secret credential information, as conceded by MasterCard's expert, Ex. 2005, at 20:16-22:1), 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 may use that joint key to uncode the VAN included with the check and compare 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.

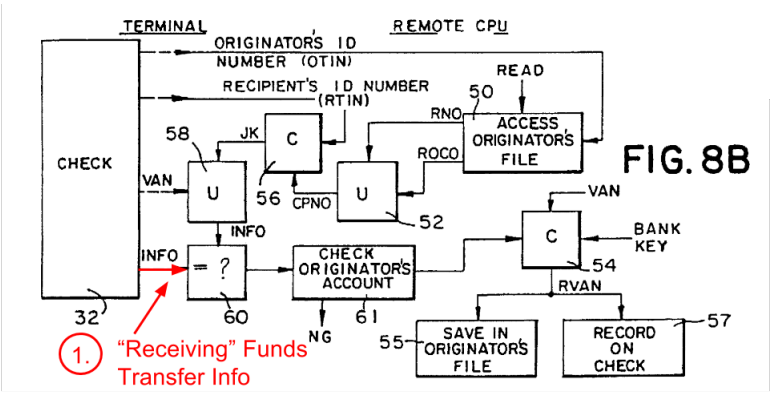
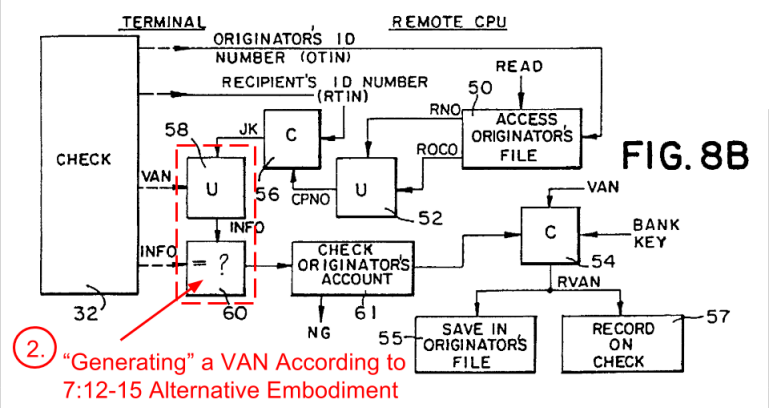


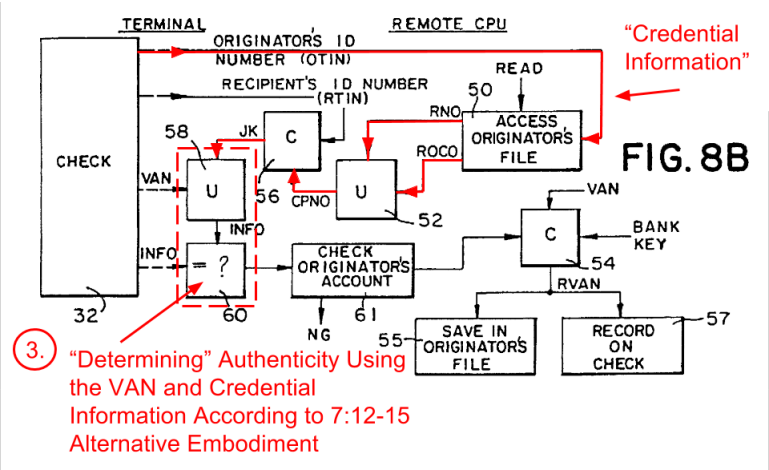
FIG. 8B

Up to this point in the discussion, the originator's bank in Figure 8B has not "generated" a VAN (claim 51's "generating" step), since the main embodiment instead "uncodes" (*i.e.*, decrypts) an already-received VAN to verify the funds transfer information. But the written description immediately fills this gap. A fully-described alternative embodiment supports the claims at issue – the originator's

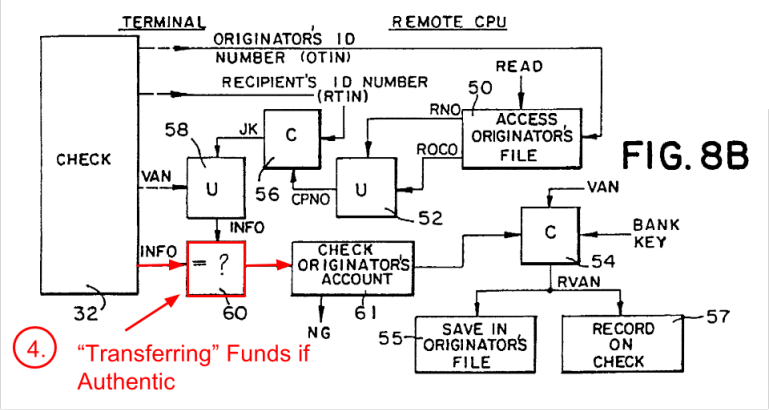
bank authenticates the received funds transfer information by actually "generating" a new VAN as part of the Figure 8B workflow. Under this alternative, the system authenticating the funds transfer information ***generates a new VAN*** (a process distinct from uncoding a received VAN) by coding the received funds transfer information with the just-described joint key. Ex. 1001, Col. 7, ll. 12-15; *see also* Col. 2, ll. 26-29.



This newly generated VAN is compared with the received VAN to authenticate the check (*i.e.*, claim 51's "determining" step). *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. In cases where the originator's bank of Figure 8B has determined that everything is authentic (and after inspection to find if sufficient funds are available), the originator's bank transfers the funds (*i.e.*, claim 51's "transferring" step). Col. 7, ll. 28-30.



Again, it cannot be stated too strongly that the originator's bank (Figure 8B) performs all of the steps of claim 51, a single entity, and that this supplies the sole Section 112 support for claim 51. Ex. 2004, at ¶¶ 29-34, 61-67; Ex. 2005 at 18:20-19:5. Nowhere does the '302 Patent describe or enable a funds transfer authentication process where the four steps of claim 51 divide up among multiple entities. Ex. 2004, at ¶¶ 61-67. MasterCard's expert could not identify any part of the '302 Patent that describes dividing up those steps among more than one entity. Ex. 2005, at 19:7-20:15.

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).

IV. CLAIM CONSTRUCTION

Patent Owner agrees with MasterCard and with the Institution Decision (Paper No. 10, at 7-8) that claim construction must proceed under traditional canons, not under the “broadest reasonable interpretation” framework. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005). This is because the ’302 Patent is expired. As shown below, MasterCard misstates several of the constructions it proffers, and omits several others that are needed for complete resolution of the issues. In addition, the Institution Decision omitted construing several requested terms, and for the term it decided in MasterCard’s favor

("VAN"), it mistakenly used the "broadest reasonable interpretation" framework. *See* Paper No. 10, at 8 ("We agree with Petitioner, and adopt this construction as the broadest reasonable interpretation for purposes of this decision."). The continuation of the proceedings permits the PTAB to correct this error.

For convenience, here is the text of claim 51, reproduced:

> 51. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, 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, the method comprising:
>
> receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount;
>
> generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;
>
> determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and
>
> transferring funds from the account of the first party to the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

A. Steps of Claim 51 All Practiced by a Single Entity

MasterCard does not address the crucial (and dispositive) question of whether a single entity must be involved in performance of each claim step. The intrinsic and extrinsic evidence both demand that claim 51 be construed to require the involvement of a single entity across the board.

As just described, MasterCard's expert conceded that the written description only discloses a single entity (the originator's bank) performing all acts of the authentication method (including the receiving, generating, determining and transferring steps). It is hornbook claim construction law that "claims cannot be of broader scope than the invention that is set forth in the specification." *On Demand Machine Corp. v. Ingram Indus., Inc.*, 442 F.3d 1331, 1340 (Fed. Cir. 2006); *see also Phillips*, 415 F.3d 1316; *Retractable Techs., Inc. v. Becton, Dickinson & Co.*, 653 F.3d 1296, 1305 (Fed. Cir. 2011) ("In reviewing the intrinsic record to construe the claims, we strive to capture the scope of the actual invention, rather than strictly limit the scope of claims to disclosed embodiments or allow the claim language to become divorced from what the specification conveys is the invention."). Similarly, if a claim term "is susceptible to a broader and narrower meaning, and the narrower one is clearly supported by the intrinsic evidence while the broader one raises questions of enablement . . ., [the court] will adopt the narrower of the two." *Digital Biometrics v. Identix, Inc.*, 149 F.3d 1335, 1344 (Fed. Cir. 1998).

By way of example, in *On Demand*, the Court held that the specification "repeatedly reinforces" that the usage of the term "customer" described a retail customer for printing services, not other buyers such as resellers. 442 F.3d at 1340.

The Federal Circuit held that the "invention that is set forth in the specification" excluded non-retail customers from that claim term. *Id.*

Here, the claim language itself is conclusive evidence that claim 51 must involve one entity's involvement in each of the enumerated acts, commensurate with the Figure 8B embodiment. First, the total four-step claim is denoted "***a*** method for a authenticating the transfer of funds," not multiple methods that combine to reach that result. Every step must be part of that single authentication method. At its heart is the "determining" step, where an authentication comparison is made. Whatever entity performs the "determining" step must therefore perform such step as part of one overall authentication and transfer process. Thus, whoever performs the "determining" step must also perform each of the rest of the steps. The claim makes no suggestion of dividing this work, nor does the specification teach how to do so.

The grammatical structure of the claim as a whole backs this up. A prior PTAB panel has already held that the "receiving" of funds transfer information must precede the "generating" of a VAN using at least a portion of such information. Ex. 2001, *Visa Inc. v. Leon Stambler*, IPR2014-00694, Paper 10, Decision, (P.T.A.B. Oct. 31, 2014). This already "glues together" the first two steps into a sequence. There is similar "glue" as between the second and third steps ("generating" and "determining"). "Generating" acts on at least a portion of the

received funds transfer information to make the VAN. And then "determining" carries forward assessment of "***the*** at least a portion of the received funds transfer information." This emphasized definite article establishes an antecedent basis. The claim denotes that the identical chunk of information used for "generating" must be in play during the step of "determining" – not some different chunk of information that underwent an intervening communication or transformation. In Figure 8B, according to the alternative embodiment noted at Col. 7, ll. 12-15, this "generating" act involves generating a new VAN to compare with a candidate VAN sourced from somewhere else (*e.g.*, the originator).

If there were any doubt, it is resolved by synthesizing two undisputed facts – (1) that the only supporting disclosure for claim 51 shows that a single entity performs all four steps (the "originator bank" in Figure 8B), and (2) that the '302 Patent does not enable one of ordinary skill in the art to practice a single authentication method with those four named steps occurring in a divided way. Ex. 2004, at ¶¶ 29-34, 61-67; Ex. 2005 at 18:20-19:5. As already cited, the law requires restricting claim scope to that which the inventor enabled, when only a single embodiment is disclosed. *Digital Biometrics*, 149 F.3d at 1344. Here, if a hypothetical first entity "received" and "generated," but then a second hypothetical entity "determined" authenticity based on what was just "generated," the claim omits explaining how the "generated" item got to the second place where it could

be inspected for the "determining" step. Ex. 2004, at ¶¶ 61-67.

Finally, this single-entity claim construction harmonizes with related legal principles governing how to apply claims to candidate instrumentalities (whether for infringement or validity purposes). It is axiomatic that the test for anticipation is identical to the test for direct literal infringement. *Polaroid Corp. v. Eastman Kodak Co.*, 789 F.2d 1556, 1573 (Fed. Cir. 1986) ("that which infringes if later anticipates if earlier") (quoting *Peters v. Active Mfg. Co.*, 129 U.S. 530, 537 (1889)). Anticipation is the mirror image of infringement, such that the inquiry as to anticipation is symmetrical with the inquiry as to literal infringement. *Lewmar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 748 (Fed. Cir. 1987).

On remand from the Supreme Court, the Federal Circuit recently clarified "divided infringement" principles in *Akamai Techs., Inc. v. Limelight Networks*, 797 F.3d 1020 (Fed. Cir. 2015) (*en banc*). Under *Akamai*, a single entity is chargeable with all of the method steps performed by others only if (1) it directs or controls the performance of the others' acts, or (2) together the entities form a joint enterprise. *Id.* at 1022. Direction or control will include when a party conditions use of a service upon the separate party's performance of specific method steps, ***and*** establishes the manner or timing of the other party's performance. *Id.* at 1024. Under the facts of *Akamai*, there was a contract in evidence between the entities showing that Limelight established the manner or timing of its customers'

performance of specific steps. *Id.* at 1024-25.

Under these principles, whether or not multiple actors can practice claim 51 as a matter of claim construction, Mr. Stambler will show later in this Response that the record lacks evidence that the acts of multiple entities in the prior art may be combined to argue anticipation.

B. Credential

Patent Owner asserted in his Preliminary Response that a 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 adopted a court's reasoning to reach this construction. Ex. 1018 at 2. MasterCard did not offer a competing construction in this CBM.

Unfortunately, the PTAB did not address the dispositive "credential" claim construction in its Institution Decision. Patent Owner requested rehearing on this basis (Paper No. 12), but the Rehearing Decision still did not provide a claim construction (Paper No. 15). Controlling Federal Circuit law holds that omitting a claim construction that might resolve the entire dispute constitutes a legal error.

> The parties present two different plain-and-ordinary-meaning definitions of "contain": "enclose" versus "restrain (radially)." As such, ***the court must construe the term.*** *See O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1361 (Fed. Cir. 2008)

("A determination that a claim term 'needs no construction' or has the 'plain and ordinary meaning' may be inadequate when a term has more than one 'ordinary' meaning or ***when reliance on a term's 'ordinary' meaning does not resolve the parties' dispute."***).

LifePort Scis. LLC v. Endologix Inc., No. 12-1791-GMS, 2015 U.S. Dist. LEXIS 91246, at *13-14 (D. Del. July 9, 2015) (emphasis added). The continuation of the proceedings permits the PTAB to correct this error.

Patent Owner's construction of "credential" is consistent with the exemplary credentials identified in the '302 patent, such as passport and identification cards. Ex. 1001, Col. 8, ll. 55-60. In these embodiments, a credential 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.

Notably, Mr. Stambler's construction is very similar to the construction proposed by MasterCard in an earlier CBM Petition regarding Mr. Stambler's '302 patent. In CBM2015-00013, MasterCard proposed 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." Thus, the only difference between the two constructions is whether the credential is "transferred or presented *for purposes of determining the identity of a party*" (Mr. Stambler's

position) or "transferred or presented *to establish the identity of a party*" (MasterCard's position). Although Mr. Stambler believes his proposal is more accurate, for purposes of this proceeding only, he is willing to move forward under MasterCard's construction.

C. Information for Identifying the Account of the Second Party

MasterCard offers no construction of "information for identifying the account of the second party." Patent Owner is inclined to agree that a plain meaning construction is appropriate. However, MasterCard's misapplication of the claim language to the Davies reference suggests that a formal construction is needed. Namely, under its plain meaning, this claim term does not cover a mere name, without more, of a second party. It must denote "information that is used to identify an account of the second party."

Three different courts adopted this very construction in prior contested proceedings. *See, e.g.,* Ex. 1013, at 23-24; Ex. 1014, at 13; Ex. 1015, at 41-43. As will be discussed below, this construction is dispositive of the entire proceeding and therefore must be analyzed by the PTAB.

D. VAN

As noted above, the PTAB mistakenly applied the "broadest reasonable interpretation" framework to the construction of VAN, leading it to adopt MasterCard's construction. Paper No. 10, at 8. Patent Owner does not challenge

this construction for present purposes. However, Patent Owner contends that additional construction is necessary for the proper disposition of CBM-standing issues.

Namely, this construction relies on the concept of "coding." MasterCard does not offer a construction for "coding," but the concept of coding is built into the Institution Decision's 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 within the concept of a VAN 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.

Without explanation, the Institution Decision did not respond to this requested construction. The continuation of proceedings permit the PTAB to correct this error.

E. Error Detection Code (claim 55)

The correct construction for "error detection code" in claim 55 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." MasterCard seeks no construction in this proceeding. Patent Owner's follows the Court's construction in one of the later claim construction orders. *See* Ex. 1016 at 24-25. MasterCard's expert agreed that it would be appropriate to use Patent Owner's construction (though he denied that his opinions would need to be revisited to address it). Ex. 2005, 95:16-97:20.

F. The VAN1 Being Used to Secure at Least a Portion of the Credential information to the at Least One Party (claim 56)

The correct construction of the "secure" phrase in claim 56 is "the VAN1 being used to verify or determine that the at least a portion of the information stored or contained in the credential is associated with the at least one party." At least one prior court decision endorsed and approved this as an agreed construction in contested infringement litigation. Ex. 1017, at 2. MasterCard offers no

construction. It will become clear that it is dispositive for claim 56 issues that VAN1 must be ***used*** in this construed fashion.

V. THE DAVIES REFERENCE

Every single invalidity ground depends on Davies as either the sole or primary reference. Thus, it is important to discuss the Davies reference in detail. Davies (published in 1989) is essentially a textbook containing discrete and separate examples, often unrelated to one another. Davies purports to disclose an Electronic Funds Transfer Point-of-Sale (EFT-POS) debit card transaction system and an Automated Teller Machine (ATM) cash withdrawal system. 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. MasterCard's previous attack (in the CBM2015-00013 proceeding) relied mainly on the Davies disclosure of an "electronic cheque." *See id.* at 328-30[1]. Since that failed when the PTAB denied Visa's IPR petition, MasterCard has shifted its focus to the ATM embodiment. *See*

[1]Patent Owner notes that MasterCard 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 MasterCard's pagination rather than the pagination of the Exhibits.

[2] MasterCard conflates this cheque disclosure with the ATM embodiment.

[3] The Institution Decision applied this principle to dismiss one of MasterCard's

id. at 330-31; *see also* Paper No. 7, at 29 (showing MasterCard relying on "ATM" embodiment when explaining claim charts).

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 MasterCard's anticipation theory in the -00013 proceeding) is an electronic document that was previously prepared by the consumer. Offline POS transactions were formulated so as to process a set of electronic cheques in a batch after they had been entered in a terminal.

Online Processes in Davies

In a basic example not relied upon in the Petition, Davies discloses 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. MasterCard relies on this example, but does not attempt to match it to each claim limitation. The Institution Decision permitted the institution of trial solely based on Davies examples matched to each claim limitation (the "cheque" and "ATM" examples on pp. 328-31). Paper No. 10, at 14-16.

The EFT-POS system extends the functionality of the POS systems described in Davies, Ex. 1004 at 311-321, in that purported 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. *See id*. at 322. 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.

Offline Processes in Davies

The electronic cheque described by Davies is relied on by MasterCard in its Petition.[2] 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 the "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 already 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, the cheque is used as a means of payment with a merchant. *See id.* at 328-29.

[2] MasterCard conflates this cheque disclosure with the ATM embodiment.

MasterCard's expert agreed that the "payee identity" (*i.e.*, ***not*** account-determination information for the payee) is one of the fields the customer fills in when using the cheque. Ex. 2005, 62:1-8. He could not recall if there was any disclosure within Davies of a payee account number or a payee account identifier used for field 13 of the cheque ("payee identity"). Ex. 2005, 71:8-15. In fact, nothing in the Davies cheque is used (or usable) to identify and authenticate an account of the payee, even when the payee has been specified by name. Ex. 2004, at ¶¶ 48-50, 84.

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.

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 in field 16 in Davies. *See id.* at Figure 10.22. The customer's private key is described as being held on an "intelligent token or 'smart card.'" *See id.* at 329. It is important to note that MasterCard's expert conceded that his claim application depends on the physical token, held by the check-writer, as a first entity who

practices the "receiving" and "generating" steps of claim 51, whereas a merchant's remote bank allegedly performs the "determining" and "transferring" steps of the claim. Ex. 2005, 81:23-84:18. This Response will later address why such a "divided anticipation" theory cannot succeed.

Davies discloses that a merchant "can verify" the customer's signature. *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 decrypt the customer's signature using the public key of the customer.

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 cheque itself does not identify the key registry, the merchant has to go outside the cheque to verify the bank information (items 1-3). And because the bank's "certificate" can only be verified, if at all, by a key registry whose role is not explicitly defined, neither can the customer's public key.

Davies is a textbook, and as such concerns itself with teaching pedagogy more than systems-enablement. It is therefore not surprising that even more is missing that one would need in a real world system. For example, the cheque contains a serious forgery vulnerability. One can see this by considering that the payee's identity (*e.g.*, a merchant) is not included on any alleged "certificate" on the cheque, and no consideration is given on the back-end (during interbank communications) to using a trusted party to verify payee identity.

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. MasterCard's expert first swore that he had no knowledge of how the 16-field data structure of the "cheque" could distinguish between conventional two-party payments, point-of-sale transactions, and ATM transactions. Ex. 2005, 73:5-20. However, once confronted with the disclosure of field 10, named "transaction type," he agreed that field 10 "is going to control whether the customer check is to be utilized as a person-to-person check versus an ATM request." *Id.*, 73:18-25. He also agreed that "an ATM request could be a code that goes into field 10 that indicates that some of the other fields might be optional for this usage." *Id.*, 74:1-4. He further agreed that "the population of usable fields in the format of 10.22 can differ as between a customer check transaction type and an ATM transaction type." *Id.*, 78:2-7.

In fact, Davies contains no disclosure of any use of the "payee" field (field 13) when the ATM functionality is specified. Ex. 2004, at ¶¶ 76, 100. The payee field (no. 13) would be unused in the ATM case, and would have neither a party's name nor anything used to identify a funds-receiving party's account. *Id.* Instead, the customer can deliver the ATM-modified 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 Ex. 1004. at 331. Again, when used as an ATM message, no "payee" is needed or used. This is fatal to MasterCards reliance on this embodiment because MasterCard's petition relies upon this (unused) "payee identity" field as containing "information for identifying the account of the second party."

To the extent MasterCard claims that the payer bank is the "payee" in the Davies ATM disclosure, there is no disclosure in Davies as to how the customer would be able to input information for identifying the account of this payer bank.

Indeed, there is no reason to believe that the customer even knows who the "payee" bank is, and there is no disclosure or reason for the customer to know the "information for identifying the account of" this party. This is not unexpected – if a person uses an ATM to withdraw cash, he / she (1) probably does not know the bank standing behind the ATM if it is a "generic" ATM without a bank identifier; and (2) even if a bank is identified, does not know the account number of the bank standing behind the ATM transaction that is credited in the transaction.

As just mentioned, ATM functionality is not the same as cheque functionality. It is one that lacks a disclosure of "information for identifying the account of the second party." The ATM transactions MasterCard 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).

As also just pointed out, Davies is a textbook that does not purport to enable its readers to build an actual secure system for real world use. Features of the ATM embodiment show additional vulnerabilities. For instance, in Figure 10.23 on page 331, Davies takes care to show interbank messages being signed on the return trip (when a decision has been made to dispense cash). But Davies discloses no interbank signature facility on the outbound trip (before the cash-dispensing

decision is made, and where one would be most concerned with malicious eavesdroppers and attackers).

VI. CLAIMS 51 AND 53 ARE NOT INVALID AS ANTICIPATED BY DAVIES

The Institution Decision allowed MasterCard to proceed with a single anticipation argument for claims 51 and 53 – Davies. When the proper claim constructions are applied, and when Davies is properly analyzed, it becomes clear that MasterCard has failed to meet its burden of proving anticipation of claims 51 and 53. Notably, the Institution Decision did not reach or address many of the reasons why MasterCard's arguments fail.

At the outset, MasterCard's application of Davies and claim charts conflate 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) and also the electronic cheque embodiment (*Id.* at 24-25). The Petition then shifts to a different section of Davies, pertaining to 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). Significantly, MasterCard'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. Although the Board noted that "cheque" and "ATM" embodiments are related, there are important differences between the types of transactions at issue that will be described below.

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.[3] *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

[3] The Institution Decision applied this principle to dismiss one of MasterCard's anticipation grounds, but without explanation did not apply it in connection with the Davies anticipation ground. Paper No. 10, at 19-20.

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 Indus. of Am. v. CTP Innovations*, LLC, IPR2013-00474, Paper No. 16, at 11-12 (P.T.A.B. 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 No. 2009-008190 (B.P.A.I. 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 No. 2009-0883 (B.P.A.I. 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.)).

Each Davies embodiment cited by MasterCard lacks many claim limitations and thus cannot anticipate.

A. Davies Does Not Disclose a Single Entity That Performs All Four Method Steps

As discussed above, MasterCard (via its expert) has conceded that it combines the actions of two entities to cover the four method steps of claim 51 – "receiving," "generating," "determining," and "transferring." MasterCard argues that the "receiving" and "generating" steps are performed by the physical smart-card "token" that is possessed by a customer of a bank. And MasterCard argues that a remote bank performs the "determining" and "transferring" steps. Davies does not anticipate because the four method steps are not performed by a single entity.

Here, the undisputedly correct claim construction demands that claim 51 covers a single entity's actions, A to Z. First, claim 51 recites a single "method for authenticating the transfer of funds," with four steps that are inextricably (if not grammatically) glued to one another in a manner that requires a single entity to perform the one method. The intricate and precise use of antecedent bases for calling out claimed concepts proves the point (*e.g.*, the first "the" in the "determining" step). Likewise, MasterCard's expert conceded that the preferred embodiment's instance of claim 51 (Figure 8B, where a "new VAN" is generated) shows only one entity performing all of the steps. Neither MasterCard nor its expert came forward with evidence or argument that the '302 Patent enables any

broader scope than such a single-entity method, despite the fact that it is MasterCard who carries the burden of proof in a CBM proceeding.

Notably, Davies does not disclose a single entity that performs all steps of claim 51. This is because Davies employs public key cryptography to purportedly authenticate funds transfer information. Specifically, the issuer bank in Davies receives the "cheque" that contains a digital signature. This received digital signature was generated by the customer on his/her token using a private key. Rather than generate a new signature for comparison to that which is received on the "cheque," the issuer bank decrypts the received digital signature for verification. Why doesn't the issuer bank instead re-generate the digital signature? The answer is simple: the issuer bank cannot regenerate the digital signature because it lacks the customer's private key that was used to generate the signature. MasterCard's expert agrees. Ex. 2005, at 82:3-8. Only the Davies customer is capable of generating this signature because only the customer possesses the private key. Instead, to authenticate the funds transfer information, the issuing bank uses the customer's public key to decrypt the funds transfer information. This is the inherent nature of public key cryptography.

The point is simple – Davies does not disclose a single entity that performs all four of the method steps claimed by Mr. Stambler. In the funds transfer embodiment of Figure 8 – and claim 51 –the same key is used to create the VAN

and to re-generate the VAN for authentication. The Davies "cheque" and "ATM" embodiments use a private key to generate a digital signature and a public key to decrypt the digital signature.

B. Whether or Not the Claim Construction Requires One Entity To Practice All of the Steps, the Two Relevant Entities in Davies Are Not a Proper Combined Entity for Anticipation Purposes

Even if the proper claim construction could be brushed aside, the law regarding claim application cannot. Under *Akamai*, a single entity is chargeable with all of the method steps performed by others only if (1) it directs or controls the performance of the others' acts, or (2) together the entities form a joint enterprise. 797 F.3d. at 1022. Direction or control will include when a party conditions use of a service upon the separate party's performance of specific method steps, ***and*** establishes the manner or timing of the other party's performance. *Id.* at 1024.

Here again, MasterCard did not even attempt to present evidence or argument showing that the multiple entities in the targeted Davies examples meet this standard. There is no evidence in Davies whereby a person of ordinary skill would understand that a merchant or card issuer bank in the disclosures on pp. 328-31 has established the manner or timing of its customers' unilateral decision to deploy their "token" to generate their "cheque" or access their ATM. *Id*. That would, in fact, make no sense. It goes without saying that banks do not direct or

control what their customers do, and do not act in a "joint enterprise" in the sense needed for multiple-entity claim coverage.

C. A Party Does Not Receive Information From Itself / "A Credential Being Previously Issued" Is Not Satisfied

As set forth above, claim 51 is intended to cover an authentication system whereby the authenticating bank verifies a received VAN by regenerating a new VAN for comparison. This requires that the both the originator and the authenticating bank use the same secret key to generate the VAN. In Davies, the authenticating bank verifies a received signature created with a private key by decrypting that signature using the corresponding public key. As set forth above, MasterCard's attempt to read the public key authentication scheme of Davies on claim 51 leads to problems for MasterCard, such as it having to relying on two parties to perform the receiving, generating, determining, and transferring steps. But this is not the only "square peg / round hole" problem confronting MasterCard.

Indeed, MasterCard is left in the precarious position of arguing that the bank's customer "receives" funds transfer information from itself. If this position sounds unnatural, that's because it is. A person of ordinary skill in the art would not think of a party being capable of receiving information from itself. If I move a $20 bill from my right hand to my left, or to my wallet, have I received funds? The obvious answer is "no."

The first step of claim 51 involves "receiving funds transfer information, including [specific funds transfer information]…" The second step involves "generating a variable authentication number (VAN) using at least a portion of *the received funds transfer information*…." The claims clearly require that the "receiving" step be performed prior to the "generating" step, because the "generating" step is performed "using at least a portion of the "*received funds transfer information*." For this reason, the PTAB adopted the determination from IPR2014-00694, requiring "that at least a portion of the receiving step must precede the generating step." Patent Owner submits that the entire "receiving step must occur and that there is no basis in the claim language to require that only part of the funds transfer information is "received" prior to "generating." Specifically, the "receiving" step states "receiving funds transfer information, including…," thus indicating the "received funds transfer information" includes all of the specifically listed elements that follow. Next, the "generating" step occurs, using "at least a portion of the *received funds transfer information*." Patent owner submits that the "received funds transfer information" refers back to the specific information included in the "receiving step," and must therefore include all of the information listed.

Notwithstanding the foregoing, the PTAB has indicated its agreement that at least some of the information must be received prior to generating. As MasterCard

points to the customer's "token" as performing the generating, MasterCard must show that some of the funds transfer information is received prior to the token generating the digital signature MasterCard points to as the VAN. MasterCard and its expert point to the customer's actions of inputting funds transfer information into the customer's own intelligent token. Again, this requires the customer to receive information from himself / herself. This makes little sense.

MasterCard also ignores that Items 1-8 on Davies the electronic check are not variable. Ex. 1004, at 328 ("These first two sections of the cheque are constants which appear on every cheque…"). As such, they are already contained on the intelligent token before it is every received by the customer, much like many of the fields on a conventional paper check. Notably, among these pre-set fields is field 5, customer identity. This is significant because "customer identity" is what MasterCard points to as satisfying "information for identifying the account of the first party" limitation. Thus, the static "customer identity" is already present on the token, and MasterCard has failed to show that the step of "receiving funds transfer information, including at least … ***information for identifying the account of the first party***" is satisfied.

To the extent MasterCard argues that the "information for identifying the account of the first party" occurs when the token is programmed by the customer's bank, another problem arises. Specifically, the preamble of claim states that prior

to the method being performed, "a credential being previously issued to at least one of the parties." MasterCard points to the customer's certificate stored in the electronic check as the claimed "credential." There is no disclosure stating that this "credential" is created, much less *issued* to the customer, prior to the "customer identity" (part of the funds transfer information) being programmed into the token. Indeed, the "customer identity" is part of any certificate, and it is absolutely necessary for the token to be programmed with the customer's certificate (including the "customer identity") prior to it being "issued" to the customer. Thus, it is seemingly impossible for the "customer identity" (information for identifying the account of the first party) to be received by the token after the customer is issued the token containing the customer's certificate. Logically, it can't happen – the token must already be programmed before it is given to the customer. Davies certainly fails to supply any disclosure that would support MasterCard on this critical point.

In sum, a party cannot receive funds transfer information from itself. It makes little sense to read the portion of Davies where the customer inputs certain funds transfer information into his / her own device as satisfying the receiving. In any event, the customer does not input "customer identity" (information for identifying the account of the first party) into the token – it is already included in the token when it is provided to the customer. And lastly, the claim requires the

"credential" to be issued prior to the "receiving step." Because "customer identity" (what MasterCard points to as part of the "credential") is in fact part of the "credential," logically the certificate cannot be issued prior to receiving the information for identifying the second party. All of these problems stem from MasterCard attempting to invalidate claim 51 with disclosure of a public key authentication system.

D. Credential

As mentioned above, neither the Institution Decision nor the Rehearing Decision construed or applied the "credential" claim term. Absence of the claimed "credential" is a yet another independent reason why Davies does not anticipate.

The Davies cheque embodiment does not disclose a "credential" as claimed. MasterCard points to the "electronic cheque" as a whole as the "credential," and the customer's public key (field number 6) as the non-secret credential information. Paper No. 7, at 27.[4] MasterCard is incorrect.

As set forth above, a "credential" must be transferred or presented for the purpose of determining the identity of a party. For example, the '302 patent lists a

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

passport as an exemplary credential. Ex. 1001, Col. 8, ll. 54-57. A passport is a document issued to a party by the US government (the trusted party). A party may transfer or present his/her passport for purposes of determining or establishing his/her identity. The party to whom the passport is transferred (e.g., a custom agent) may make a determination as to the presenting party's identity. Mr. Stambler proposed to enhance a credential using a VAN to secure credential information. The electronic cheque is not transmitted for this purpose.

The Davies electronic cheque is presented to cause the transfer of funds from a customer's account to someone else. 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 credential because it is not a

document or information transferred to establish the identity of a party, which in this case is the customer. Indeed, at the time the cheque is verified by the customer's bank, the customer is not present or otherwise in communication with his/her bank. The customer's bank is not attempting to verify the customer's identity, but instead verifying that the check originated from the customer. This is not a situation where the customer is transferring his/her digital certificate to a receiving party in order to have his/her identity established or determined.

Indeed, the digital certificates described in Davies are not used for this purpose. The "certificate" on the face of the cheque consists of "customer identity" (field 5), "customer public key" (field 6), "expiry date" (field 7), and "signature of 5-7 by bank" (field 8). Even if these fields were presented to a bank, they would not be useful to establish the customer's identity. While a customer could sign a message using his/her *private* key, which would be verified using the customer's corresponding public key, the private key is not even on the document that MasterCard points to as the credential. And the "private key" is by its very nature "private." It is not "transferred or presented" to anyone and thus does not satisfy the claim limitation of "the credential being non-secret." The private key is always kept secret and is used by the customer's token to sign messages. The token protects the private key through use of a PIN. This is very different from the use of a credential, such as a passport, which a party "transfers or presents" to another

party for purposes of determining the identity of the presenting party. Indeed, if two parties (one the customer and one an imposter) presented the Davies certificate to the customer's bank, how could the bank use the certificate to determine identity? It couldn't. Only the use of the private key would allow the customer's bank to determine which party is in fact the customer, and in such circumstance the parties would need to be present (or in communication with) the bank so that it could make a determination of identity contemporaneously with the presentment.

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. This is anathema to a document used to either "determine" identity of the party transferring it. MasterCard's expert agreed:

> Q. So the payee will take the Davies check and at some point have to present it to his own bank, the recipient's bank, right?
>
> A. Yes

> Q. At that moment where the payee presents that electronic check, with fields 1 through 16 to his recipient's bank, he's not using that check to identify himself with fields 1 through 16, is he?
>
> A. I don't believe so.

Q. And then when the recipient's bank goes and presents to the originator bank to make sure that the funds can be transferred, that recipient bank is not using fields 1 through 16 to identify itself to the originator bank, right?

A. No, because there is no identification, whether reliable or not, on the check of the recipient bank, only of the recipient.

Ex. 2005, 69:22-70:13.

Nor is the cheque "*previously issued* by a trusted third party," which is a requirement for the credential of claim 51. First, it is not "previously issued" with respect to the steps of the claim. In fact, under MasterCard's theories, it is 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 MasterCard calls the credential comes into existence.

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. MasterCard 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." The cheque pointed to by MasterCard as the "credential" is issued by the customer's token.

Other than these misguided attempts, MasterCard 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 cheque itself is used to determine the identity of a party, again because it cannot. Finally, MasterCard makes no effort to show that the cheque itself was issued by a trusted party, again because it cannot.

E. Davies Does Not Disclose Information for Identifying the Account of the Second Party

Claim 51 foundationally and fundamentally involves the receipt of information for identifying two accounts – "information for identifying the account of the first party" and "information for identifying the account of the second party." Thereafter, claim 51 recites a transfer of funds between these two accounts – "transferring funds from the account of the first party to the account of the second party." Davies fails to disclose "information for identifying the account of the second party."

As mentioned previously, MasterCard now seems to rely primarily on Davies' ATM embodiment. MasterCard 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. And MasterCard's expert confirmed that an ATM transaction does not require the same fields among fields 1-16 to be used. Ex. 2005, 74:1-4; 78:2-7. At least the payee identity is missing from a cash-withdrawal scenario. Ex. 2004, at ¶¶ 76, 100. Necessarily, this means that there is nothing to

meet the claim element of "information related to the account of the second party."[5]

To the extent MasterCard claims that in the ATM transaction the "payee identity" is the same as the "customer identity," another fatal problem arises. Specifically, the customer's account (account of the first party) would be debited, and cash would be dispensed to the customer at the ATM. But the "payee identity" would not correspond to an account that is to be credited in the ATM transaction. Thus, there would be no "transferring funds" between two accounts (*i.e.* there would be a debit of the customer's account followed by a transfer of cash to the customer).

Although not argued MasterCard's petition, to the extent MasterCard argues that the ATM embodiment involves a transfer of funds between the customer's account and an account at the "Payer bank A" that is presumably controlling the ATM shown in Davies Figure 10.23, this argument was also fail . In this scenario,

5 To the extent MasterCard argues that the "account of the second party" is supplied by the ATM handling the transaction, this is not disclosed by Davies or argued by MasterCard in its petition. Nor would this invalidate the claim because account information supplied by the ATM would take place after the customer's token signed the transaction request (thus, failing the sequencing requirement of the claim).

the "account of the second party" would be the account of Payer bank A, meaning that the customer would need to input "information for identifying the account of [Payer bank A]" in the electronic check to satisfy claim 51. Davies is silent as to how the customer requesting the ATM transaction would have any information as to an identity of any account at "Payer bank A." Nor would one expect the customer requesting an ATM transaction to have any information concerning the account at the "Payer bank A" that may be credited in the transaction. Davies and (MasterCard's petition) fail to demonstrate that this limitation is present in the ATM embodiment disclosed in Davies.

Even the basic party-to-party cheque in Davies fails to meet this claim limitation. A person's name (field 13, "payee identity") is not the same thing as information for identifying that person's account. Ex. 2004, at ¶¶ 47-51, 84. The Davies disclosure paints the scenario of a "merchant" receiving an electronic cheque, presumably meaning that the merchant is named as the "payee." Ex. 1004, at 328-30. Common sense dictates that people who write checks to merchants have utterly no idea how to identify the merchant's bank account information, much less know who the merchant's bank really is. For example, a person purchasing goods at Wal-Mart has no idea who Wal-Mart's bank is, much less information for identifying Wal-Mart's account at this unknown bank. This makes it inconceivable that the Davies EFT-POS embodiment discloses "information for identifying the

account of the second party," which must be construed to be "information that is used to identify an account associated with the second party."

VII. CLAIMS 51, 53, 55 AND 56 ARE NOT INVALID AS OBVIOUS OVER DAVIES AND MEYER

MasterCard's obviousness combination of Davies with Meyer fares no better. It depends on the premise that the ***only*** claim limitation of claim 51 missing from Davies is the proper sequencing of the "receiving" step occurring before the "generating" step. Paper No. 7, at 50-51. MasterCard 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.* MasterCard concludes that a person of skill in the art would be motivated to augment the teachings of Davies with this purported proper sequencing. *Id.* MasterCard's premise is flawed. As shown above, more is missing in Davies than the claimed sequencing.

Even putting the flawed premise aside, MasterCard's argument fails on its own terms. MasterCard 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. A person cannot "receive" such information from himself or herself – that makes no sense.

There are even more reasons why these obviousness theories fail.

A. The Petition Does Not Use Meyer to Assert Obviousness of Claims 53 and 55, and Does Not Offer a Theory of Obviousness by Davies Alone

First, dependent claims 53 and 55 should not need additional analysis because MasterCard does not seek to apply any disclosure from Meyer to augment its preexisting Davies contentions as to those claims. In this regard, respectfully, the Institution Decision made a clear mistake about claim 55 that the PTAB now has the opportunity to correct. The Institution Decision agreed with Patent Owner that Davies does not anticipate claim 55. Paper No. 10, at 17 (noting Davies "suggests indirectly" error detection codes, but does not explicitly disclose them). However, the Institution Decision then preliminarily determined that the combination with Meyer taught the limitations of claim 55. *Id.* at 20. The flaw here is that the PTAB failed to appreciate that neither MasterCard nor its expert cited Meyer to map onto the limitations of claim 55. Therefore, whatever was missing when the PTAB rejected a contention of anticipation of claim 55 over Davies remained missing within the combination of Meyer plus Davies over claim 55. The combination with Meyer does not add anything to the failed claim 55 anticipation contention, and this combination logically should be rejected.

B. Citations to Meyer Do Not Overcome the Gaps in Davies

Second, since Davies does not anticipate for all the reasons shown above, its combination with Meyer 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).

C. Meyer Does Not Disclose the Elements of Claim 56

Third, with respect to claim 56, Meyer does not even map onto the added dependent claim limitations.

MasterCard contends that parts of Meyer read on the added requirements of that claim. In particular, MasterCard 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, MasterCard is clearly mistaken. Claim 56 requires that VAN1 be used "to secure at least a portion of *the credential information* to the at least one party." Claim 51's preamble holds that the "credential information" must be non-secret. But in MasterCard's claim 56 contentions, the non-secret requirement fell by the wayside, since MasterCard now points to something undisputedly "secret" (*i.e.*, SKc*) as the thing that is secured. 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.

At his deposition, MasterCard's expert tried to skirt the problem. For the first time he asserted that "securing" a secret private key necessarily means that the mated public key is thereby secured as well, even if no cryptographic operation occurs on the public key. Ex. 2005, 48:5-8. This completely overlooks that, as properly construed, VAN1 must be "used to verify or determine" the association of credential information with a party. But in these Meyer disclosures, SKc* (the putative VAN1) is simply used to store the secret key in an intelligent smart card in a form other than clear text, to prevent capture by an enemy. Page 49 of the Petition also misquotes Meyer – suggesting that SKc* is something that the "issuer checks." Paper No. 7, at 49. That is clearly wrong. The cited portion of Meyer makes it clear that the issuer does not even have SKc*. Ex. 1022, at 597. Instead, the issuer looks at a collection of different information (not SKc*) to make an inference about the user's possession of the correct secret SKc* number. *Id.* (mentioning authenticating a message by testing its digital signature with a forward-encoding based on a *public* key PKb).

In short, MasterCard's contentions about Meyer mapping onto claim 56 try to put the proverbial square peg into a round hole. A secret number such as SKc*

cannot be VAN1, since it cannot be used to verify or determine the association of some different nonsecret information with a particular party.

D. MasterCard Offers Insufficient Reasons to Combine, and the Evidence Refutes that Any Such Reason Exists

If all of that were not enough, the obviousness attack contains additional fatal flaws. For example, MasterCard 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 (Feb. 22, 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. Indeed MasterCard's expert had no explanation for why Davies did not explicitly bring the targeted Meyer disclosures into the Davies text itself, when Davies cited and was clearly aware of the Meyer reference. Ex. 2005, 52:13-54:7.

Mr. Stambler recognizes that the Institution Decision cited a block quotation from the Petition that it preliminarily considered to contain the required "reason to

combine" evidence. Paper No. 10, at 21. This excerpt asserts that when references have "similar purpose" and "overlapping teachings," that "confirms" a motivation to combine. The law is actually ***the opposite*** of MasterCard's position, and thus ***the opposite*** of what the Institution Decision initially concluded. In fact, when two references "independently accomplish similar functions" and each "operates effectively, a person having ordinary skill in the art, who was merely seeking to [better perform the overlapping function], would have no reason to combine the features of both [references] into a single device." *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1369 (Fed. Cir. 2012).

This legal principle only makes sense. When a reference describes a system that is self-contained and accomplishes its objective, it gives no impetus to do more. *Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1325, 1334 (Fed. Cir. 2013) ("self-contained" system "accomplished its objective and provided no suggestion to broaden that objective," hence gave no reason to combine); *see also Smartflash LLC v. Apple, Inc.*, 2015 U.S. Dist. LEXIS 18414, at *48-51 (E.D. Tex. Jan. 5, 2015) ("similar purposes of both references" insufficient to establish why a person of skill in the art would be motivated to combine). Whatever parts of the earlier Meyers reference that might have been intriguing to a person of skill in the art like Davies many years later, Davies already explicitly incorporated. *See* Ex. 2005,

52:13-54:7. Whatever remained would have been of insufficient interest to motivate any combination. Ex. 2004, at ¶¶ 114-117.

For all of these numerous reasons, the Davies and Meyer combination fails to support obviousness of claims 51, 53, 55 or 56.

VIII. CLAIM 55 IS NOT INVALID AS OBVIOUS OVER DAVIES AND 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 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.

For claim 55, MasterCard's chart cites alleged hashing technologies in *both* references (Davies *and* Nechvatal), 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 MasterCard'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 (P.T.A.B. Feb. 22, 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 (P.T.A.B. May 15, 2014) (dismissing obviousness challenge where primary reference already had the capabilities that the secondary reference would provide with its added disclosures). As already cited, the fact of overlapping disclosures ***refutes*** a reason to combine; it does not support it. *Kinetic Concepts*, 688 F.3d at 1369. 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 (P.T.A.B. May 15, 2014).

The clincher is that MasterCard's expert acknowledged the facts that show the prior art teaching away from adding a hash or one-way function (the putative error detection code of claim 55) to the funds transfer authentication of claim 51. MasterCard's theory has always been that adding a one-way hash increases signing efficiency. Paper No. 10, at 23, citing Paper No. 7, at 67. However, MasterCard's expert conceded (as he must) that the funds transfer messages of claim 51 are short messages already. Ex. 2005, 23:14-20; 25:17-22. After some obstruction, he then had to acknowledge that Davies teaches applying such techniques instead to ***long***

messages, and that the rationale of improving signing efficiency actually ***does not exist*** for short ones like funds transfer messages:

Q. And on page 264 of Davies, under the heading in the middle of the page, let me read some words, actually three sentences I'll read into the record. "The function H(M) reduces a message of arbitrary length to a number of a convenient and standard length for the purpose of signature. It could equally well be used as a preparation for calculating an authenticator. It can even be used by itself to authenticate a large message." Do you see those words in Davies?

A. I do.

Q. Is that the Davies disclosure you were referring to in your declaration page -- paragraph 135 where you said that Davies discloses that hash values are one-way functions on the transaction information may be used as an intermediate step in generating signatures on messages?

A. I think it was more broadly through the text than that.

* * *

Q. Okay. Now, the words of the excerpt that I just read into the record and pointed you to in that Davies suggests a one-way hash to ***reduce*** a message length, right?

A. ***Yes***.. . . .

* * *

Q. You've used the language in your declaration about increasing signing efficiency. Do you recall that?

A. No, I don't, but --

Q. Improving signing efficiency, paragraph 136.

A. Okay. I thought you said improve the performance of cryptographic operations, is that what you're referring to?

Q. If you read through all the way to the end of the paragraph 136 --

A. Yes, would improve the signing efficiency, yes.

Q. The improvement in signing efficiency occurs when you're dealing with a very large message, that's when the one-way hash really improves signing efficiency?

A. The efficiencies grow with the size of the message, ***yes***.

Q. So there will become a message so small the efficiency doesn't improve and, in fact, it becomes extra overhead for the process?

A. You'd have to work at it, but ***yes***.

Q. So for this rationale of improving signing efficiency, that's not a rationale for applying a one-way hash that would apply to ***a short message like fund transfer messages***?

A. I think in that case, your thinking would not be dominated by the

improvement in efficiency, speed, cost, ***yes***.

Ex. 2005, 32:20-33:21; 37:18-38:22 (emphasis added). Mr. Stambler's expert agrees – the prior art actually teaches away from adding the limitations of dependent claim 55 to claim 51. Ex. 2004, at ¶¶ 118-119. Mr. Stambler's inventiveness brought the respective ideas together. Therefore, the evidence shows that claim 55 would not have been obvious.

IX. CLAIM 56 IS NOT INVALID AS OBVIOUS OVER DAVIES, FISCHER AND PIOSENKA

Finally, regardless of the outcome of the rest of the Petition, the PTAB should at least reject the attack on claim 56. MasterCard challenges dependent claim 56 here on a single ground. MasterCard'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 before, there can be no invalidity when the proposed secondary references do not make up for the gaps in the primary reference. That is the case here.

MasterCard 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 MasterCard 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 reject the invalidity assertions that use that ground. *Square, Inc. v. Cooper*, IPR2014-00156, Paper No. 9, at 20 (P.T.A.B. May 15, 2014).

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 ¶¶ 158-60, 174. Paper No. 7, at 69-71.

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 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? MasterCard does not explain.

Mr. Stambler recognizes that the Institution Decision asserted that the content of the Petition at pages 69-71 contains the required "reason to combine." Paper No. 10, at 26. However, closer inspection reveals that this "showing" in MasterCard's papers really just amounts to a collection of observations on what the respective references disclose. It fell far short of stating a true "reason to combine." This is the very definition of "begging the question."

The following annotation of that precise set of MasterCard statements proves the point:

> **Quote from the Petition in the Institution Decision:** "A person of ordinary skill in the art would be motivated, at the time of the effective filing date of the '302 Patent, to combine the teachings of Davies with the teachings of Fischer for securing messages, end-to-end. . . ."

Patent Owner Rebuttal: This sentence solely states a conclusion, not a rationale.

> **Quote from the Petition in the Institution Decision:** "It would also be obvious for a person of ordinary skill in the art to augment the authenticated

electronic funds transfer mechanisms using digital signatures, which is taught by Davies, with the counter signature of Fischer, as this would allow for the electronic funds transfer transaction using a chain of authority, where each higher level approves any commitment/signature made at a lower level. . . ."

Patent Owner Rebuttal: This sentence solely states what the combination of Fischer with Davies might do once made ("allow for the electronic funds transfer transaction using a chain of authority," etc.), not why a person would have a reason to do it in the first place.

Quote from the Petition in the Institution Decision: "A person of ordinary skill in the art would be motivated, at the time of filing the application to which the '302 Patent claims priority, to augment the verification of message signatures and public keys, as taught by the combination of Davies and Fischer, with the denial of request upon failure to verify the user's credential, as taught by Piosenka."

Patent Owner Rebuttal: This sentence solely states a conclusion, not a rationale.

In short, MasterCard presented no true evidence, and no cogent argument, supporting a "reason to combine." Ex. 2004, at ¶¶ 120-124. Its presentation of this issue is no better than similar presentations rejected by the Federal Circuit as insufficient. *E.g.*, *InTouch Techs., Inc. v. VGO Comm's, Inc.*, 751 F.3d 1327, 1349 (Fed. Cir. 2014) (criticizing expert who simply "opined that all of the elements of the claims disparately existed in the prior art, but failed to provide the glue to combine these references."). The "jigsaw puzzle" approach by MasterCard does not "explain what reason or motivation one of ordinary skill in the art at the time of the invention would have had to place these pieces together." *Id.*

X. CONSTITUTIONAL CHALLENGE

For preservation purposes, Mr. Stambler also objects that these proceedings violate the Article I Separation of Powers doctrine, as well as his Seventh Amendment right to a jury trial on adjudications of patent validity. Mr. Stambler respectfully requests dismissal on these grounds as well.

A patent, upon issuance, is not subject to revocation or cancellation by any executive agent (*i.e.*, the USPTO or any part of it, such as the PTAB). *McCormick Harvesting Mach. Co. v. C. Aultman & Co.*, 169 U.S. 606, 609 (1898). While *ex parte* reexamination has so far been held to avoid a Separation of Powers bar (*see Patlex Corp. v. Mossinghoff*, 758 F.2d 594 (Fed. Cir. 1985)), that decision rested

on classification of the patent right in an invalidity context as a "public" right, and in so doing reached a result contrary to the controlling *McCormick* decision.

Later statements by the Supreme Court confirm that a "public" right in the context of the "public rights exception" is solely one for which the claim could have historically been determined exclusively by either the executive or legislative branches. *Stern v. Marshall*, 131 S. Ct. 2594, at 2611-14 (2011); *see also Thomas v. Union Carbide Agric. Prods. Co.*, 473 U.S. 568, 591-92 (1985) (applying public rights exception to Federal pesticide law). This does not encompass challenges to a patent's validity, particularly challenges that are *inter partes* in nature and brought in an adjudicative forum by a civil opponent seeking to evade liability for patent infringement. Only a judicial proceeding under Article III may properly revoke a patent in such a context, if at all.

By participating in these proceedings further, Mr. Stambler does not waive his Article I Separation of Powers or his Seventh Amendment objection. He specifically reserves all of his rights.

XI. CONCLUSION

Given its expert admissions and the facts otherwise of record, MasterCard fell far short of meeting its burden to prove claims 51, 53, 55 or 56 invalid. Mr. Stambler respectfully requests that the PTAB issue a Final Written Decision

upholding their validity, or otherwise dismissing these proceedings for the reasons stated.

Dated: October 21, 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 21st day of October, 2015, a true and correct copy of the foregoing Patent Owner Leon Stambler's 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 Eliot D. Williams BAKER BOTTS LLP 30 Rockefeller Plaza, New York, NY 10112 robert.scheinfeld@bakerbotts.com eliot.williams@bakerbotts.com	

Dated: October 21, 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