

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INCORPORATED
Petitioner

v.

LEON STAMBLER
Patent Owner

Case Number CBM2015-00044
Patent 5,793,302

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	Page
I. PRELIMINARY STATEMENT	1
II. CLAIM CONSTRUCTION	2
A. Claim 51 Is Not Limited to a Single Entity	2
B. Credential	9
C. Information for Identifying the Account of the Second Party	9
D. VAN	10
E. Error Detection Code	11
III. CLAIMS 51 AND 53 ARE ANTICIPATED BY DAVIES	11
A. Petitioner Does Not Rely On “Unrelated” Disclosures of Davies.....	11
B. Claim 51 Is Not Limited to a Single Entity	13
C. Davies Discloses a Single Entity Performing All Steps of Claim 51	13
D. Davies Discloses the Claim Elements “Receiving Funds Transfer Information” and the “Credential Being Previously Issued”	14
E. Davies Discloses A “Credential”	16
F. Davies Discloses Information Identifying the Account of the Second Party	18
IV. ALL OF THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	20
A. Claim 51 Is Obvious Over Davies or Meyer Individually, and Over Davies and Meyer Combined.....	20
B. Claim 53 Is Anticipated and Obvious.....	22
C. Claim 55 Is Obvious Over Davies Combined with Meyer and/or Over Davies Combined with Nechvatal	22
D. Claim 56 Is Unpatentable.....	24
1. Claim 56 is Obvious Over Davies In View of Fischer and Piosenka ..	24
2. Claim 56 is Obvious Over Davies In View of Meyer	25
V. CONCLUSION	25

EXHIBITS

- Ex. 1001 U.S. Patent No. 5,793,302
- Ex. 1004 D. W. Davies *et al.*, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer* (1989)
- Ex. 1005 James Nechvatal, Public-key Cryptography (NIST Special Publication 800-2) (April 1991)
- Ex. 1013 Memorandum Opinion and Order dated April 9, 2010 from *Leon Stambler v. JPMorgan Chase & Co.*, 08-cv-204 (E.D. Tex.)
- Ex. 1014 Memorandum Opinion and Order dated September 24, 2010 from *Leon Stambler v. Merrill Lynch & Co., Inc.*, 08-cv-462 (E.D. Tex.)
- Ex. 1015 Claim Construction Order dated December 27, 2010 from *Leon Stambler v. Amazon.com*, 09-cv-310 (E.D. Tex.)
- Ex. 1016 Memorandum Opinion and Order dated September 28, 2011 from *Leon Stambler v. ING Bank*, FSB., 10-cv-181 (E.D. Tex.)
- Ex. 1018 Previous Constructions of Claim Terms of the ‘302 Patent
- Ex. 1020 Declaration of Professor Whitfield Diffie (“Diffie Declaration”)
- Ex. 1022 Carl H. Meyer *et al.*, *Cryptography: A New Dimension in Computer Data Security—A Guide for the Design and Implementation of Secure Systems* (1982)
- Ex. 1023 Deposition of Seth Nielson, Ph.D. (Dec. 8, 2015)
- Ex. 2005 Deposition of Whitfield Diffie (Oct. 2, 2015)

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Akamai Techs., Inc. v. Limelight Networks</i> , 797 F.3d 1020 (Fed. Cir. 2015) (<i>en banc</i>)	13, 14
<i>BMC Res., Inc. v. Paymentech, L.P.</i> , 498 F.3d 1373 (Fed. Cir. 2007)	6
<i>Boston Scientific Scimed v. Cordis Corp.</i> , Appeal No. 2014-008135, 2015 WL 883933 (P.T.A.B. Feb. 27, 2015)	21
<i>Broadcom Corp. v. Emulex Corp.</i> , 732 F.3d 1324 (Fed. Cir. 2013)	21
<i>Connell v. Sears, Roebuck & Co.</i> , 722 F.3d 1542 (Fed. Cir. 1983)	20
<i>Corning Inc. v. DSM IP Assets B.V.</i> , Case No. IPR2013-00046, slip op. (P.T.A.B. May 1, 2014) (Paper 81)	10
<i>Epos Techs. Ltd. v. Pegasus Techs. Ltd.</i> , 766 F.3d 1338 (Fed. Cir. 2014)	4
<i>In re Fulton</i> , 391 F.3d 1195 (Fed. Cir. 2004)	23
<i>Kara Tech. Inc. v. Stamps.com Inc.</i> , 582 F.3d 1341 (Fed. Cir. 2009)	5, 11
<i>Kinetic Concepts, Inc. v. Smith & Nephew, Inc.</i> , 688 F.3d 1342 (Fed. Cir. 2012)	21
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	22
<i>MBO Labs, Inc. v. Becton, Dickinson & Co.</i> , 474 F.3d 1323 (Fed. Cir. 2007)	4

CBM2015-00044	
Patent No. 5,793,302	
<i>McCarty v. Lehigh Valley R.R. Co.</i> ,	
160 U.S. 110 (1895).....	4
<i>MCM Portfolio LLC v. Hewlett-Packard Co.</i> ,	
No. 2015-1091, 2015 WL 7755665 (Fed. Cir. Dec. 2, 2015)	2
<i>Mobotix v. E-Watch</i> ,	
Case No. IPR2013-00334, slip op. (P.T.A.B. Jan. 10, 2014) (Paper	
18)	24
<i>Phillips v. AWH Corp.</i> ,	
415 F.3d 1303 (Fed. Cir. 2005) (<i>en banc</i>)	4, 10
<i>Tehrani v. Hamilton Med., Inc.</i> ,	
331 F.3d 1355 (Fed. Cir. 2003)	5
OTHER AUTHORITIES	
37 C.F.R. § 42.6(a)(3)	10

I. PRELIMINARY STATEMENT

Patent Owner's argument relies on the flawed premise (repeatedly asserted in its response) that all steps of the challenged claims must be performed by a single entity. *See, e.g.*, Paper 16, at 4, 7, 9-14. Patent Owner concludes that: "Davies does not anticipate because the four method steps are not performed by a single entity." *Id.* at 31-33. But there is no such requirement in the claims, and the '302 Patent's specification describes just the opposite.

Indeed, in the preferred embodiment (and only embodiment illustrated in the patent figures¹), the claimed steps are performed by *different* entities — precisely as in the prior art. Patent Owner and its expert are forced to read the claims to exclude this preferred embodiment to reach their erroneous conclusion that the claims are not anticipated.² Moreover, even assuming *arguendo* that all steps of the claim had to be performed by a single entity, Davies discloses this.

Patent Owner's other arguments rely on a flawed understanding of the disclosures in the prior art. When properly understood, the prior art teaches the claim limitations, rendering the challenged claims unpatentable. Petitioner's arguments regarding the disclosures of the prior art are supported by the testimony

¹ Ex. 1023, at 44:12-45:18, 51:18-53:3 ("No, I guess they do not have any examples of comparing two VANs in the figures that I can find.")

² *Id.*

of Whitfield Diffie, who first proposed the idea of public key cryptography³ — the foundation technology for digital signatures⁴ — which enabled the funds transfer techniques disclosed in the Davies and Meyer references. Mr. Diffie’s testimony confirms that the claims are unpatentable. The Board should confirm its Institution Decision (Paper 10) and find the Challenged Claims unpatentable.⁵

II. CLAIM CONSTRUCTION

A. Claim 51 Is Not Limited to a Single Entity

Rather than contend that claim 51 as written is patentable, Patent Owner attempts to re-write the claim in the guise of claim construction, arguing that all of the claim’s method steps must be performed by a single entity. *See, e.g.* Paper 16, at 4, 7, 9-14 (“The intrinsic and extrinsic evidence both demand that claim 51 be construed to require the involvement of a single entity across the board.”). Patent Owner’s argument is without merit.

³ Ex. 1023, at 19:21-20:6, 22:17-25.

⁴ Patent Owner’s expert teaches Mr. Diffie’s techniques to his students. Ex. 1023, at 19:13-20:6, 22:17-25.

⁵ Patent Owner’s arguments regarding the constitutionality of this proceeding are meritless and precluded by controlling law. *See MCM Portfolio LLC v. Hewlett-Packard Co.*, No. 2015-1091, 2015 WL 7755665, at *8-9 (Fed. Cir., Dec. 2, 2015).

As to the intrinsic evidence, Patent Owner argues that the ‘302 Patent describes only a single embodiment, where all steps of the claims are performed by a single entity. Paper 16, at 7 (“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”); *id.* at 12 (“the only supporting disclosure for claim 51 shows that a single entity performs all four steps (the ‘originator bank’ in Figure 8B)”). Neither the facts nor the law support Patent Owner.

As to the specification, Patent Owner argues: “Significantly, FIG. 8B illustrates that all of the steps of claim 51 take place at the originator’s bank.” *Id.* at 4. But Figure 8B shows precisely the opposite, as Patent Owner’s own admission — on the very next page of its response — concedes. There, Patent Owner admits that Figure 8B does not disclose “claim 51’s generating step” because nowhere in Figure 8B is a VAN “generated.” *Id.* at 5. Figure 8B shows that the originator’s bank “‘uncodes’ (*i.e.* decrypts) an already-received VAN.” *Id.* The VAN shown in Figure 8B is generated at the originator’s computer, not at the *originator’s bank*. Ex. 1001, 4:52-5:28 (“the originator generates a check ... at the originator’s terminal or computer” by generating the “VAN and at least a portion of the information relevant to the transaction,” which are “imprinted on the check”). Because of this, Patent Owner’s own expert was eventually forced to argue that claim 51 does *not* cover the authentication process shown in Figure 8B.

Ex. 1023, at 37:24-39:9, 44:12-45:18, 51:18-53:3 (“Q. So that embodiment [multi-entity performance] is the one that is actually shown in Figure 8B, right? ... A. Yes, that appears to be correct. ... Q. And this is the embodiment that you’re saying is not covered by the claims? A. Yes”).

Instead, according to Patent Owner’s expert, claim 51 covers only the “alternative[]” embodiment described in a mere single sentence in the specification, and not shown in any Figures. *Id.* at 45:4-18 (citing Ex. 1001, at 7:12-15). Thus, Patent Owner and its expert contend that the claims should be interpreted to *exclude* the preferred embodiment shown in the figures. This would be legal error. *See MBO Labs, Inc. v. Becton, Dickinson & Co.*, 474 F.3d 1323, 1333 (Fed. Cir. 2007) (“[A] claim interpretation that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct.”); *see also Epos Techs. Ltd. v. Pegasus Techs. Ltd.*, 766 F.3d 1338, 1347 (Fed. Cir. 2014).

Moreover, even if the patent only disclosed the “alternative” embodiment (that Patent Owner’s expert contends practices claim 51), Patent Owner’s claim construction argument would fail as a matter of law. As the Federal Circuit sitting *en banc* has cautioned, “although the specification often describes very specific embodiments of the invention, we have repeatedly warned against confining the claims to those embodiments.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (*en banc*); *see also id.* at 1312 (quoting *McCarty v. Lehigh Valley R.R.*

Co., 160 U.S. 110, 116 (1895)) (“if we once begin to include elements not mentioned in the claim, in order to limit such claim ..., we should never know where to stop.”); *Kara Tech. Inc. v. Stamps.com Inc.*, 582 F.3d 1341, 1347-48 (Fed. Cir. 2009) (“The claims, not specification embodiments, define the scope of patent protection. The patentee is entitled to the full scope of his claims, and we will not limit him to his preferred embodiment *or import a limitation from the specification.*”) (emphasis supplied). Accordingly, Patent Owner is incorrect as a matter of law to suggest that the claim should be limited to a particular embodiment from the specification. The focus must remain on the claim language.

Here, nothing in the language of claim 51 requires that all steps be performed by a single entity. In fact, the steps say nothing at all about what entity performs them. Ex. 1001, at 33:16-36; Ex. 2005, at 19:7-17. Accordingly, they need not be performed by a single entity. *Tehrani v. Hamilton Med., Inc.*, 331 F.3d 1355, 1362-63 (Fed. Cir. 2003) (holding claimed step of “measuring” need not all be performed by the device performing other claimed steps, because the claim did not “specif[y] that the [device] must do the measuring”). Notably, the applicant knew how to restrict the claimed steps to being performed by a particular entity. For example, the preamble to claim 51 requires that the credential be issued “*by a trusted party.*” Ex. 1001, at 33:18-19 (emphasis supplied). In contrast, the steps in the body of the claim were broadly written and avoid restricting themselves to

performance by any particular entity. *See BMC Res., Inc. v. Paymentech, L.P.*, 498 F.3d 1373, 1379-81 (Fed. Cir. 2007) (“this court will not unilaterally restructure the claim” where the patent owner “could have drafted its claims to focus on one entity”). Accordingly, Patent Owner’s argument that the steps must be performed by a single entity is legally flawed.

Similarly, the extrinsic evidence does not support Patent Owner. As an initial matter, Patent Owner’s expert, Dr. Nielson, is not qualified to provide an opinion about the meaning of claim terms (or even knowledgeable about how claims should be construed). Ex. 1023, at 56:12-57:17; *id.* at 55:11-56:11. Even if the Board were to consider his opinions, his reasoning is flawed. According to Dr. Nielson, claim 51 should be interpreted to require that all steps are performed by a single entity because “that’s all I see described in the specification.” *Id.* at 46:18-47:8. This ignores, however, the preferred embodiment (and only embodiment depicted in the figures), which (as discussed above) involves the claim steps being performed by different entities. His flawed conclusion seems to be due to his misunderstanding of the specification. For instance, he was confused about which entities performed the various steps depicted in the figures, *id.* at 75:1-76:17, and his opinion was based on the assumption that the VAN must be transmitted securely, whereas the specification describes the opposite, *id.* at 83:17-86:17.

Dr. Nielson's only other argument in support of his reading of the claims seems to be that both the "receiving" and "determining" steps operate on "funds transfer information." *Id.* at 49:3-24. But he does not explain why two different entities could not both operate on the same information, in the manner shown and described in the preferred embodiment of the '302 Patent.⁶ Moreover, Dr. Nielson appeared to abandon this argument during his deposition — reverting to the purported lack of specification support to justify his position. *Id.* at 66:21-67:22 ("the language of the claim doesn't necessarily prohibit dividing it up, but ... there's not enough written description to know how to do that.").⁷

Patent Owner further argues that Petitioner's expert "conceded that the written description discloses a single entity (the originator's bank) performing all acts of the authentication method." Paper 16, at 10. This mischaracterizes Mr. Diffie's testimony, and lacks factual support. Mr. Diffie testified only that *Figure 8B* showed steps being performed by the originator's bank. Ex. 2005, at 18:12-19:5 (Q. ... in what we've just seen at Figure 8B, would you agree...). But the claims are not limited to the activities depicted in Figure 8B which, Petitioner

⁶ Figures 7 and 8 use reference identifiers (VAN) and (INFO) to show that the identical VAN and INFO imprinted by the originator on the check (FIG. 7) are transmitted to the originator's bank (FIG. 8B). Ex. 1001, at 6:40-45.

⁷ Dr. Nielson later seemed to reverse course again. Ex. 1023, at 69:20-70:14.

agrees, is directed to depicting the steps occurring at the originator's bank. By limiting its questioning of Mr. Diffie to Figure 8B, Patent Owner avoided obtaining testimony about related Figures 6, 7, and 8A. It is those figures (together with Figure 8B) that are described by the patent as depicting "a check transaction system in accordance with a first embodiment of the present invention." Ex. 1001, at 3:1-6.

Indeed, the claimed step of generating the VAN is not shown in Figure 8B at all, as both Patent Owner and its expert admit. Paper 16, at 5 (relying on the "written description" to "fill[] this gap" in disclosure); Ex. 1023, at 39:5-9, 40:25-41:42:12 ("Column 5, which is referring to Figure 7, describes the creation of the VAN..."). Notably, when Patent Owner's counsel asked Mr. Diffie if the patent *anywhere* disclosed the claimed steps being performed by different entities, Mr. Diffie responded only that he would "need to read through the whole embodiment." Ex. 2005, at 20:6-15. Patent Owner never gave Mr. Diffie the opportunity to do so. As to the proper claim interpretation, Mr. Diffie was unequivocal: "there is no requirement in claim 51 that the steps all be performed by the same entity." *Id.* at 19:7-17.

Accordingly, Patent Owner's argument should be rejected. Instead, the claims should be read to cover both the preferred embodiment (where the claim

steps are performed by different entities), and the alternative embodiment (where the claim steps may be performed by a single entity).

B. Credential

As an initial matter, MasterCard denies Patent Owner's suggestion that the term "credential" is dispositive to this Trial. *Cf.* Paper 16, at 14. Patent Owner accepts the construction that petitioner offered in CBM2015-00013. *Id.* at 16. Patent Owner, however, may also be attempting to import an additional, unstated limitation to this construction that the credential must be "transferred or presented for purposes of determining the identity of *the presenting party*." *Id.* at 40-41. Such a construction is improper at least because the specification states that the invention permits verification of the identity of "absent parties to a transaction." Ex. 1001, at 2:1-4, 4:67-5:2.

C. Information for Identifying the Account of the Second Party

Patent Owner argues that this claim term "does not cover a mere name ... of a second party." Paper 16, at 16. Although this argument is irrelevant to the proceeding, as nothing in the prior art cited by Petitioner involves the use of a "name,"⁸ Patent Owner's argument should be rejected. Patent Owner relies on three prior District Court opinions that expressly reject the argument Patent Owner is now making. *Id.* (citing Ex. 1013, at 23-24; Ex. 1014, at 13; and Ex. 1015, at

⁸ Davies uses a party's "identity" to locate his/her account. Ex. 1004, at 328, 331.

41-43). Each of those opinions adopt a construction under which any information used to identify an account of the second party, which would include a “mere name,” is sufficient. *See, e.g.*, Ex. 1013, at 24 (“this claim does not require specific account identification. Moreover, the information required need only be ‘for identifying,’ not ‘that identifies.’”). Patent Owner does not explain why a name, if used to identify an account, could not satisfy this claim element.

D. VAN

Patent Owner does not challenge the construction of this term, but argues further construction is necessary for CBM standing purposes. Paper 16, at 16-17. Patent Owner’s response fails to raise an issue of CBM standing, instead purporting to incorporate by reference arguments made in its preliminary response. *Id.* at 1. The Rules expressly forbid incorporation of arguments from one document into another. 37 C.F.R. § 42.6(a)(3). Accordingly, Patent Owner’s argument is waived. *See Corning Inc. v. DSM IP Assets B.V.*, Case No. IPR2013-00046, slip op. at 2 n.2 (P.T.A.B. May 1, 2014) (Paper 81) (“We ... consider only arguments made in the [Patent Owner] response itself”). Even if this construction were considered on the merits, it should be rejected as an improper attempt to rewrite the claims to include a requirement that the VAN be generated “entirely electronic[ally]”. *See Tehrani*, 331 F.3d at 1362-63 (method steps need not be performed “automatically” by a hardware device). *See also supra* p. 4-5 (citing

Phillips, 415 F.3d at 1323 (“we have repeatedly warned against confining the claims to [specification] embodiments”)).

E. Error Detection Code

In its prior litigation, Patent Owner has proposed different constructions of this term, which has led prior courts to adopt slightly different constructions. *See* Ex. 1018, at 2. Mr. Diffie adopted the construction proposed by Patent Owner in the *Amazon* litigation, which was adopted by that court. *Compare* Ex. 1020, at 4 *with* Ex. 1015, at 51. Patent Owner now proposes the construction that it offered in the subsequent *ING* litigation, which was adopted by that court. *Compare* Paper 16, at 18 *with* Ex. 1016, at 25. At his deposition, Mr. Diffie credibly explained why the *Amazon* construction was more accurate, but concluded that the difference in constructions made no difference to this case. Ex. 2005, at 94:25-97:20.

III. CLAIMS 51 AND 53 ARE ANTICIPATED BY DAVIES

Petitioner disputes the majority of Patent Owner’s characterizations of Davies, but addresses only the most relevant points of disagreement below.

A. Petitioner Does Not Rely On “Unrelated” Disclosures of Davies

Patent Owner argues that the Petition “conflate[s] different unrelated disclosures” of Davies. Paper 16, at 28. This is a rehash of the argument made by Patent Owner in its preliminary response, which the Board properly rejected. Paper 10, at 16. The Petition relies on the electronic check disclosure of Davies’ chapter 10 — primarily Section 10.6. Ex. 1004, Davies pp. 328-32. While some

background details regarding the techniques are explained earlier in Davies, those background disclosures are not “unrelated.”

Patent Owner’s primary argument seems to be that the electronic check and ATM embodiments are not related. Paper 16, at 28-29. Davies explicitly ties these concepts together. First, Davies describes how funds can be transferred between accounts using paper check, then explains that the paper checks can be “[c]hanged into a modern form as a message with a digital signature,” which can be “regarded as an ‘electronic cheque.’” Ex. 1004, Davies pp. 285-86. Section 10.6 describes how that electronic check can be implemented by using “a digital signature facility with a key registry to authenticate public keys,” *id.* at 328, along with an intelligent token to protect the customer’s secret key and to perform the digital signature, *id.* at 329. Davies then explains how this electronic check can be utilized to perform a “point-of-sale payment” at a traditional retail merchant, or at an ATM to obtain cash. *See id.* at 330 (the “same intelligent token which provides an electronic cheque between individuals can ... also ‘cash a cheque’ at an ATM with on-line verification.”). Indeed, Davies expressly notes that this technique of using an electronic check to obtain cash from an ATM is what is shown in Fig. 10.23. *Id.* (“Figure 10.23 shows how this [*i.e.* cashing a check at an ATM] works in a shared ATM network.”). Accordingly, Patent Owner’s argument that the petition has mixed unrelated disclosures lacks merit.

B. Claim 51 Is Not Limited to a Single Entity

Patent Owner argues that “Davies does not anticipate because the four method steps are not performed by a single entity.” Paper 16, at 31. As discussed above, however, this is not a requirement of the claims. *See supra* Part II.A.

C. Davies Discloses a Single Entity Performing All Steps of Claim 51

Patent Owner argues under “divided infringement” principles set forth in *Akamai Techs., Inc. v Limelight Networks*, 797 F.3d 1020 (Fed. Cir. 2015) (*en banc*), a single entity can be attributed with acts performed by others if “that entity directs or controls others’ performance.” *Id.* at 1022; Paper 16, at 13-14, 33-34. Petitioner disagrees that the *Akamai* standard applies to anticipation, but even if it did, Davies satisfies it.⁹ The “receiving” steps and “generating” steps are performed, not by the customer, but rather by the token issued by the customer’s bank. *See, e.g.*, Ex. 2005, at 90:25-91:5. Davies confirms this, stating: “[t]he token ... authenticates a message to its ‘master’ which is the card issuer’s computer system.” Ex. 1004, Davies p. 327. Davies also describes additional controls the card issuer can place on the token, *e.g.*, limits on transactions, and notes the token’s “intelligence is used on behalf of the customer *and the card*

⁹ Patent Owner provides no support for its argument that *Akamai* altered the law of anticipation, such that one reference must disclose not only all claim elements, but also those elements being performed by one entity. Paper 16, at 13.

issuer....” Id. at 325, 327 (emphasis supplied). Thus, the customer’s bank in Davies directs the performance of all of the claimed steps. Accordingly, under the *Akamai* standard, Davies discloses all steps being performed by one entity.

D. Davies Discloses the Claim Elements “Receiving Funds Transfer Information” and the “Credential Being Previously Issued”

Contrary to Patent Owner’s assertion, Davies does not disclose that the “customer ‘receives’ funds transfer information from itself.” Paper 16, at 34. Rather, the token, issued by the card issuing bank, receives funds transfer information from a terminal. Ex. 2005, at 90:3-91:5. As Davies explains, the token contains a microprocessor and memory allowing the use of “intelligence” when the token is inserted into the terminal. Ex. 1004, Davies pp. 324-25, 327. The token receives the transaction data for the check from the terminal, and signs that data. *Id.* at 331 (“The ‘cheque’ enters the card from the terminal....”); *id.* at 329 (“A terminal is needed to generate a cheque, sign it with the aid of the token and send it....”). Therefore, the token (more precisely, the microprocessor in the token) receives the electronic check data structure (Fig. 10.22) during a transaction. *Id.* at 330-31 and Fig. 10.23 (“The customer’s request is formed into a message and presented to the token.”). Accordingly, the Patent Owner’s assertion that the customer “receives funds transfer information from itself” is simply based on a misunderstanding of Davies.

Patent Owner also asserts that the “customer identity” information found in

the electronic check cannot be both “received” by the token during the receiving step and be part of a “credential” that is “previously issued” as recited in the preamble of claim 51. Paper 16, at 36-38. This argument fails for several reasons.

First, Patent Owner never explains the basis for its premise. The “previously issued” credential mentioned in the preamble does not appear in the claim until the “determining” step. Accordingly, the claim requires only that the credential be issued before the “determining” step takes place. Patent Owner does not dispute that the determining step in Davies occurs after the credential is issued.

Second, even if the credential must be issued before the “receiving” step, Davies still discloses this. With reference to Fig. 10.22 of Davies, it is undisputed that the information found in items 1-8 of the electronic check (including item 5, “Customer identity”) are stored in the memory of the token. *See* Paper 16, at 36. Davies thus describes how the token stores a certificate (i.e., a previously-issued credential) before being inserted in a terminal for a transaction. Davies also discloses that the funds transfer data, including all of the check data, are received by the token at the time of the transaction. In particular, the terminal reads information from the token (including the constant information in items 1-8 that “appear on every cheque drawn”), as well as any variable information maintained by the token (such as the “cheque sequence number”). Ex. 1004, Davies pp. 328, 330. The terminal assembles this information, with additional variable information

about the transaction, to form the electronic check message sent back to the token for signing. *Id.* at 328-31. Specifically, the “customer’s request is formed into a message and presented to the token,” *id.* at 330; the “‘cheque’ enters the card from the terminal” to be signed by the token, *id.* at 331 and Fig. 10.23 (arrow from terminal to token). Davies further describes that these electronic checks are recorded on the token, functioning as an “electronic chequebook.” *Id.* at 329. Therefore, Davies teaches that the certificate containing the customer’s identity and customer’s public key are read by the terminal to form an electronic check message, which is then presented back to the token (including that customer’s identity) to be signed and stored for later reference. *Id.* at 325-31. Thus, Davies discloses the credential is “previously issued” and “receiving funds transfer information,” including “information for identifying the account of the first party.”

E. Davies Discloses A “Credential”

As discussed previously, Patent Owner’s interpretation of credential is flawed. *See supra* Part II.B. Patent Owner mischaracterizes the disclosure of Davies to argue that Davies does not disclose the “credential” of claim 51. Paper 16, at 38-43. On the contrary, even using Patent Owner’s proffered definition of a credential: “a document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party,” Davies discloses it.

Contrary to Patent Owner's argument, Petitioner does not assert that the electronic check message as a whole is the credential. *See* Paper 16, at 38-40. Rather, Petitioner relies on the "blank check" of Davies (*i.e.*, the non-variable items 1-8 of the electronic check of Fig. 10.22 — of which items 5-8 can also be referred to as the "customer's certificate"). Paper 7, at 26-27; Ex. 2005, at 59:17-60:12. This information is stored on the token by the card issuing bank (*i.e.*, it is "previously issued" by a "trusted party"¹⁰). Ex. 1004, Davies pp. 328-30 ("customers of the bank can carry their keys ... in an intelligent token..."); *id.* at Fig. 10.22. The "credential information" is later included in the electronic check message sent to the card issuing bank for purposes of determining the identity of the party that signed the electronic check (*i.e.*, for the purposes of determining the identity of the customer). *Id.*

The customer's certificate meets the limitations of a "credential." The customer's public key in the certificate is, as its name implies, public. It can be transferred to anyone for the purpose of determining the identity of check signatory. This non-secret credential information is used, along with variable information (items 9-15 in the electronic check), and the customer's signature (item 16) (*i.e.*, a "VAN"), *id.* at 328-29, to "determine whether the at least a

¹⁰ The card issuing bank, which serves as a key registry for its customers, is a trusted party. *See* Ex. 2005, at 79:1-20.

portion of the received funds transfer information is authentic” in the “determining” step. Particularly, as admitted by Patent Owner, the card issuing bank verifies the customer’s signature (item 16) (*i.e.*, “VAN”) using the customer’s public key (item 6) (*i.e.*, the “credential information”). Paper 16, at 40. If the signature is verified, the received funds transfer information is determined to be authentic. In this manner, the “credential” is used to determine the identity of the signor of the electronic check message.

Patent Owner’s argument that “an imposter” could present the customer’s certificate to the bank is irrelevant. Paper 16, at 41. The customer’s certificate is not used to determine the identity of the entity presenting the certificate. Rather, it is used to determine the identity of the customer as the signor of the check, *i.e.*, the party requesting a transfer of funds from his account.

F. Davies Discloses Information Identifying the Account of the Second Party

Patent Owner’s argument that Davies does not disclose “information for identifying the account of the second party” is also without merit. Paper 16, at 44-47. This argument is based on Patent Owner’s assertion that in the Davies ATM disclosure, “no ‘payee’ field is needed or used.” Paper 16, at 26. As an initial matter, Patent Owner’s argument is irrelevant because it fails to address Davies’s disclosure of an electronic check at a non-ATM point of sale, which Patent Owner does not dispute includes an identification of the party being paid. Ex. 1004,

Davies p. 328 and Fig. 10.22, Item 13 (“Payee identity”).

Moreover, Patent Owner is wrong to assert that no payee identity is used in the ATM example of Davies. Nothing in Davies suggests that the structure of the electronic check message would change when cashing a check at an ATM. *Id.* (check “should contain all the items listed in Figure 10.22”); *id.* at 330-31 (“The same intelligent token which provides an electronic cheque between individuals can therefore function for off-line and on-line point of sale payments” and “can also ‘cash a cheque’ at an ATM with on-line verification.”). Petitioner’s expert confirmed that the payee field would be necessary to complete an ATM transaction. Ex. 2005, at 71:16-72:13 (“So I think the paying bank is the second party. The check maker is the first party.”; “Q. ... who is the payee bank? A. The one who owns the ATM.”).

Even Patent Owner’s expert admitted that the ATM example involves a payment to the Bank that owns the ATM, and further admitted that the ATM-owner must be identified during the transaction. Ex. 1023, at 100:7-102:23 (“Q. So there has to be some way for the [ATM] card issuer bank to know who to pay? A. Yes.”). He identified no other mechanism for identifying the ATM-owner, and when pressed whether the “payee field” disclosed in Davies would be the logical place to identify the payee bank, Patent Owner’s expert merely expressed his ignorance on the issue. *Id.* at 101:15-22 (“I’m not sure. I don’t know.”).

Accordingly, the un rebutted evidence shows that Davies utilizes a “Payee identity” in all of its electronic check transactions, including when cashing a check at a third-party ATM, as shown in Fig. 10.23.

IV. ALL OF THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Claim 51 Is Obvious Over Davies or Meyer Individually, and Over Davies and Meyer Combined

Patent Owner’s sole argument that claim 51 is not obvious over Davies and Meyer is that both Davies and Meyer lack the claimed sequencing (“receiving” before “generating”) and that there is no motivation to combine the two references. Paper 16, at 47, 51-52. Patent Owner is mistaken.

As discussed above, Davies anticipates claim 51. It therefore also renders the claim obvious. *Connell v. Sears, Roebuck & Co.*, 722 F.3d 1542, 1548 (Fed. Cir. 1983) (“a disclosure that anticipates ... also renders the claim invalid under § 103”). The Meyer reference is similar to Davies, and also renders the claim obvious. Paper 7, at 19-22, 35-63. Chapter 10 of Meyer discusses EFT based on shared-key cryptography using “check digits” (MAC) appended to the EFT message. *E.g.*, Ex. 1022, Meyer p. 457. The MAC (*i.e.* VAN) is therefore generated after receiving the funds transfer information. Paper 7, at 19-22. The recipient can then check the received MAC to determine the received transaction data was not fraudulently modified or generated. *Id.* Chapter 11 suggests substituting the MAC with “digital signatures” based on a “public-key algorithm.”

Ex. 1022, Meyer pp. 569, 589-90. The cryptographic operations are performed with a token (“intelligent secure card”) that interacts with a terminal. *Id.* at 588-604, Fig. 11-44 and Table 11-16. Thus, contrary to Patent Owner’s argument, Meyer does not involve a person receiving information from himself. Paper 16, at 47. Meyer therefore renders claim 51 unpatentable.

Patent Owner further argues that Davies and Meyer should not be combined because each “operates effectively,” and “accomplishes its objective.” Paper 16, at 52 (citing *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342 (Fed. Cir. 2012); *Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1324 (Fed. Cir. 2013)). Each of these cases is distinguishable. In *Kinetic* (1) there was no evidence explaining why the references would be combined, (2) none of the prior art taught one of the essential claim elements (treating a wound), and (3) the references taught away from the claimed invention. 688 F.3d at 1369. *See Boston Scientific Scimed v. Cordis Corp.*, Appeal No. 2014-008135, 2015 WL 883933, at *7 (P.T.A.B. Feb. 27, 2015) (distinguishing *Kinetic*). *Broadcom* apparently involved a single-reference obviousness argument, based on a reference directed to a “different problem” from the one the patent addressed, and there was no evidence explaining why the reference should be modified. 732 F.3d at 1334. In contrast, Davies and Meyer each relate to the same problem as the ‘302 Patent (authentication of electronic funds transfers), and the Petition provides several unrebutted reasons to

combine these references. Paper 10, at 21; *cf. KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (“Often, it will be necessary for a court to look to interrelated teachings of multiple patents...”). Claim 51 is therefore obvious.

B. Claim 53 Is Anticipated and Obvious

The Petition shows that claim 53 is taught in Davies, Paper 7, at 34-35, and/or is rendered obvious by a combination of Davies and Meyer, Paper 10, at 20-22. Patent Owner provides no argument directed to this specific claim. *Cf.* Paper 16, at 48. Accordingly, claim 53 should be found unpatentable.

C. Claim 55 Is Obvious Over Davies Combined with Meyer and/or Over Davies Combined with Nechvatal

Claim 55 requires that the VAN be generated using an “error detection code.” As explained in the Petition, Davies discloses generation of a VAN via a digital signature algorithm. Paper 7, at 29-32, 34-35. It was well known to persons of ordinary skill in the art that a digital signature is an “error detection code,” as each parties’ expert agrees. Ex. 2005, at 38:23-39:7, 40:5-10 (“Any authentication operation inherently is an error detection code”); Ex. 1023, at 60:15-61:19 (“Q. Would this definition [of error detection code] cover a digital signature? A. Yes.”). Indeed, this is explained in the background section of Davies. Ex. 1004, Davies p. 261 (“the [digital] signature provides error checking”). Meyer also explains that a digital signature can be considered an authentication (or error

detection) code. Ex. 1022, Meyer pp. 589-90 (“the term DGS [digital signature] is used instead of [authentication code]”).

Moreover, Davies teaches that a hash function “**H(M)**” should be used to create the digital signature. Ex. 1004, Davies pp. 260-61.¹¹ Hash functions were also known to be error-detecting codes, as shown in Nechvatal. Ex. 1005, at 32 (“hash functions ... serve as cryptographic checksums (i.e., error-detecting codes)...”).

Patent Owner, however, argues that there is no motivation to modify Davies in view of Nechvatal. Paper 16, at 53. But Petitioner is not proposing a modification of Davies. It relies on Nechvatal only to show that the hash function in Davies is an error detection code. Paper 7, at 69.

Thus, the disclosures of Davies with either Meyer or Nechvatal, and the

¹¹ Patent Owner’s argument that Davies “teaches away” from the use of hash functions, Paper 16, at 53-58, ignores Petitioner’s argument that the digital signature itself (regardless of how generated) is an error detection code. Moreover, Davies expressly teaches use of a hash function to generate a signature. Ex. 1004, Davies pp. 260-61. That is not “teaching away” from using a hash function; it is the opposite. *See In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004) (no teaching away where prior art did not “criticize, discredit, or otherwise discourage the solution”).

knowledge of a person of ordinary skill in the art, renders this claim obvious.

D. Claim 56 Is Unpatentable

1. Claim 56 is Obvious Over Davies In View of Fischer and Piosenka

Other than referring back to its arguments regarding independent claim 51, Patent Owner does not identify any element of this dependent claim missing in the combination of Davies, Fischer and Piosenka. Paper 16, at 58-59. Instead, Patent Owner attacks only the “reason to combine.” *Id.* at 59-62. But, Patent Owner’s attack is meritless, as it ignores the detailed motivation set forth in the Petition. Paper 7, at 69-71. As explained there, Davies discloses sending a customer’s certificate as well as the customer’s signature. *Id.* at 69-70. Fischer expressly suggests validating a customer’s certificate before using the public key in that certificate to verify the digital signature. *Id.* Patent Owner fails to address this express suggestion found in Fischer.

As to Piosenka, Petitioner relies on this reference for its explicit teaching to deny a request if the digital signature cannot be authenticated. *Id.* at 70-71. Patent Owner’s only argument is that this teaching is “already there in Davies.” Paper 16, at 60. If Patent Owner is correct, the claim is obvious over Davies and Fischer alone. *Cf. Mobotix v. E-Watch*, Case No. IPR2013-00334, slip op. at 2 (P.T.A.B. Jan. 10, 2014) (Paper 18) (“Within the instituted ground based on Ely, [et al.], Petitioner is free to prove ... obviousness ... based on Ely alone.”). If Patent

Owner is wrong, it has failed to rebut Petitioner's showing that Piosenka suggests denying a request signed by a digital signature that cannot be authenticated. Either way, the claim is invalid.

2. Claim 56 is Obvious Over Davies In View of Meyer

Patent Owner argues that Meyer's SKc* (which Petitioner maps to the claimed "VAN1") does not secure "non-secret" credential information to the at least one party. Paper 16, at 49-51. Patent Owner apparently believes that the VAN1 itself must be "non-secret." Such a requirement is not found in claim 56. SKc* secures the non-secret credential information (the customer's public key, PKc) to the customer. In particular, SKc* is used to generate the customer's secret key (SKc). Ex. 1022, Meyer p. 596 and Table 11-16. Patent Owner's expert admits that the customer's secret key has a defined mathematical relationship to the customer's public key (PKc). Ex. 1023, at 119:12-120:6. Thus, Meyer teaches that SKc* is used to secure the non-secret credential (PKc) to the customer.

V. CONCLUSION

For the reasons set forth herein and in the Petition, the Board should find claims 51, 53, 55 and 56 to be unpatentable.

Respectfully submitted,

Date: January 15, 2016

/Robert C. Scheinfeld/

Robert C. Scheinfeld

Eliot D. Williams

BAKER BOTTS L.L.P.

Counsel for MASTERCARD

INTERNATIONAL INCORPORATED

CBM2015-00044
Patent No. 5,793,302

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing PETITIONER'S REPLY
TO PATENT OWNER'S RESPONSE was filed and served electronically via e-
mail on January 15, 2016, in its entirety on the following:

Robert P. Greenspoon
Flachsbart & Greenspoon, LLC
333 N. Michigan Ave., Suite 2700
Chicago, IL 60601
Telephone: (312) 551-9500
rpg@fg-law.com

/Robert C. Scheinfeld/

Robert C. Scheinfeld