

MASTERCARD INTERNATIONAL INC.

Petitioner

V.

LEON STAMBLER


Patent Owner

CBM2015-00044

U.S. Patent No. 5,793,302

Oral Hearing

March 18, 2016

 US005793302A	
United States Patent [19] Stambler	[11] Patent Number: 5,793,302 [45] Date of Patent: *Aug. 11, 1998

[54] **METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION**

[76] **Inventor:** Leon Stambler, 7803 Boulder La., Parkland, Fla. 35067

[*] **Notice:** The term of this patent shall not extend beyond the expiration date of Pat. No. 5,267,314.

[21] **Appl. No.:** 747,174

[22] **Filed:** Nov. 12, 1996

Related U.S. Application Data

[60] Continuation of Ser. No. 446,369, May 22, 1995, which is a division of Ser. No. 122,071, Sep. 14, 1993, Pat. No. 5,524,073, which is a division of Ser. No. 977,385, Nov. 17, 1992, Pat. No. 5,267,314.

[51] **Int. Cl.:** H04Q 1/00

[52] **U.S. Cl.:** 340/825.34; 380/43; 380/45

[58] **Field of Search:** 340/825.31, 825.34; 380/43, 44, 45

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,699,690	9/1971	Nisman	
3,611,293	10/1971	Constable	
3,657,521	4/1972	Constable	
3,892,948	7/1975	Constable	
3,938,091	2/1976	Azula et al.	
4,004,089	1/1977	Richard et al.	
4,016,405	4/1977	McCane et al.	
4,186,871	2/1980	Anderson et al.	
4,198,619	4/1980	Azula	
4,200,770	4/1980	Hellman et al.	380/44
4,208,575	6/1980	Hall et al.	
4,208,739	6/1980	La	
4,223,403	9/1980	Konheim et al.	
4,234,932	11/1980	Gorgans	
4,264,782	4/1981	Konheim	
4,264,808	4/1981	Owens et al.	
4,268,715	5/1981	Azula	
4,281,215	7/1981	Azula	

(List continued on next page.)

OTHER PUBLICATIONS

Shipley C., "I threw away my checkbook", PC-Computing, vol. 3, No. 11, pp. 112, 114-115, 118-120, Nov. 1990.

Ida J., "Electronic Presentment Due for N.Y. Test", American Banker, vol. 157, No. 143, p. 3, Jul. 27, 1992.

Torrez A., "Banking Industry Looks at Changing Check Guarantees", The Business Journal-Phoenix & The Valley of the Sun, vol. 9, No. 29, pp. 13-14, May 29, 1989.

Sullivan D., "Bank Technology Trick or Treat?", Bankers Monthly, vol. 109, No. 11, pp. 10, 12-14, 18, 20, Nov. 1992.

Seidenberg, "Bell Companies Now Testing Smart Card Offering Increased Feature Functionality", Card News, vol. 5, No. 10, pp. 5-6, May 21, 1990.

"General Magnaplate Corporation Issues Three-Month Report to Stockholders", PR Newswire, 1 page, Nov. 11, 1992.

Byles T., "More Companies Are Paying Bills Electronically", Journal of Commerce, p. 2B, May 5, 1988.

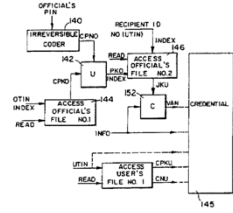
Carraker J.D., "Strides in Electronic Checking Transforming Payment System", vol. 68, No. 3, pp. 18-19, 22, 24, 26, 28, 30, Mar. 1992.

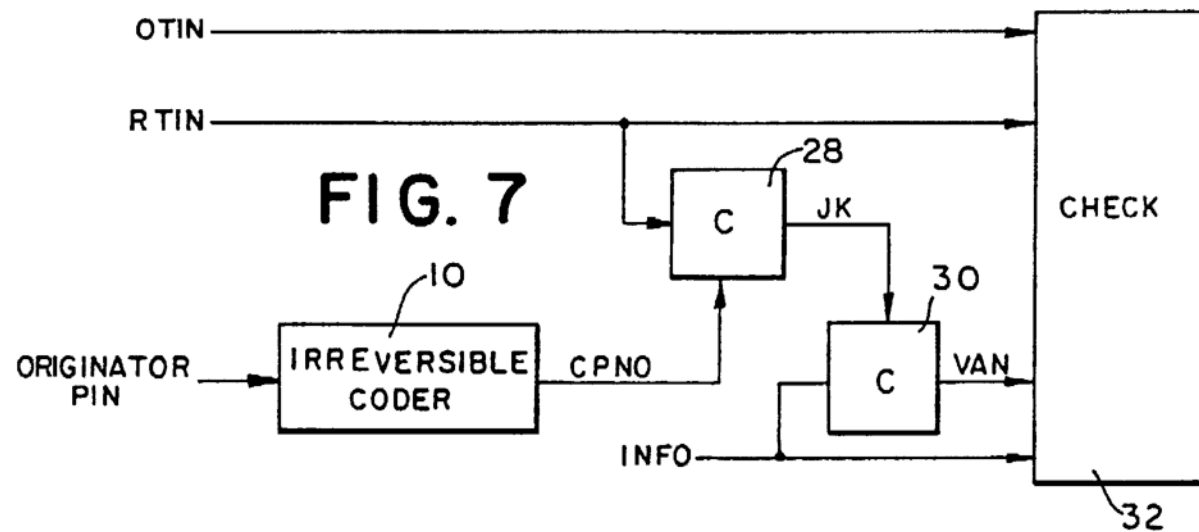
Primary Examiner—Brian Zimmerman
Attorney Agent, or Firm—Panitch Schwartze Jacobs & Nadel, P.C.

[57] **ABSTRACT**

A transaction system wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to decode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

91 Claims, 15 Drawing Sheets





5,793,302

4

rating a
embodi-
ing user
erates a
transaction
5
rating a
ordance
n, with
FIG. 10
10
ing the
ing the

three phases of operation. In the first phase, illustrated in FIG. 6, a user of the system must enroll in order to be recognized by the system. Each user enrolls at his or her bank, or at another convenient location, such as a place of employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

FIG. 14,
a check
15
a check
if a cre-
20
tem for
a secret
alternate

While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of FIG. 6 with the typical transaction information, including the user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be permitted to select an arbitrary number for RN.

30
35
40
45
50

The signal produced by mixer 16 is then transmitted to the bank's computer, where it is applied to a sorter 18. It is assumed that this transmission preferably occurs over a secure line, such as one protected by a tandem coder and uncoder which can utilize a joint terminal-bank key. The sorter recovers the original CPN and RN, saving RN in the user's file at block 22. It should be noted that in saving RN, the user's file is accessed by using his TIN as an index. The received CPN is applied as the data input to a coder 20, which receives RN as its key input, producing a revisable owner code (ROC) which is saved in the user's file in the same manner as RN. Various additional information is saved in the user's file, such as his personal account number (PAN), name, phone number (PHN), account balance, and other relevant information. The user's TIN, PAN or PHN can be used as an index to access the user's file. CPN represents coded authentication information since it is a coded form of the PIN, and since it is used in other parts of the system to authenticate the user and the transaction. The system preferably maintains RN as a secret number (although in the present embodiment the user file is not secret since it is accessed using a non-secret index) and ROC is maintained as a non-secret number. As explained in detail below, CPN is derivable from ROC and RN.

FIG. 7 illustrates how the originator generates a check in accordance with the present invention. This process preferably takes place at the originator's terminal or computer. It is assumed that the originator would be generating a check in the usual manner and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms, such as the recipient's name and TIN (RTIN), and the originator's personal account number and bank identification number. Preferably, the terminal includes a check reader and printer which can read necessary information from the originator's check form and print information on the form, although this could also be done manually by the originator. The originator and the recipient can be the same person, for example, where a person is cashing a personal check originated by the person. In the case of multi-party checks, the check is

"...originator's terminal
or computer..."

The data input to coder 28 is the recipient's TIN (RTIN), which has been read from the check, or accessed from the computer memory, or entered by the originator.

5,793,302

5

originated by a present party (i.e., the originator) in favor of an absent party (recipient).

The originator enters his or her PIN at a terminal or computer. Through irreversible coder 10, the originator's PIN is converted to a coded PIN (CPNO), which is applied as the key input to coder 28. The data input to coder 28 is the recipient's TIN (RTIN), which has been read from the check, or accessed from the computer memory, or entered by the originator. The data output of coder 28 is a joint key (JK), which is applied as the key input to a coder 30. Generally, the JK is generated using information associated with at least one of the parties involved in the transaction (in this case, the originator and recipient). As will be shown more fully below, the joint key (or code) is used to protect and authenticate the originator and recipient. The data input to the coder 30 is the information (INFO) to be authenticated (that is, information relevant to the transaction, such as check number, amount, etc.).

The data output of the coder 30 is a variable authentication number (VAN), which codes the information to be authenticated, based upon information related to the recipient and information related to the originator. Note that the

a coder 44, number (i.e., the data input random number which is applied to the mixer in RNK in a code may readily coded authentication representational system to a

The mixer block 41 is transmitted remote bar use of an RNK, not a sorter 62). The check hold on the che authenticat

At the re in a coder 4

5,793,302

4

rating a
embody-
ing user
verifies a
ntication

FIG. 14,
a check
includ-
a check

of a cre-
g to an

tem for
a secret
ternate

cks uti-
ponents
commu-
art will
ware
locks in

ustrated
known
DBS). A
input, at
more
uch are
it could
e of the
added to
res the
data and

outs and
... D₀).
a inputs
e binary
entional
ve plural
will be
h as one
digits or
ker or a
de word
me divid-
ed signal

al block
k trans-
8A and
63
cessing
involves

three phases of operation. In the first phase, illustrated in FIG. 6, a user of the system must enroll in order to be recognized by the system. Each user enrolls at his or her bank, or at another convenient location, such as a place of employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of FIG. 6 with the typical transaction information, including the user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be permitted to select an arbitrary number for RN.

The signal produced by mixer 16 is then transmitted to the bank's computer, where it is applied to a sorter 18. It is assumed that this transmission preferably occurs over a secure line, such as one protected by a tandem coder and uncoder which can utilize a joint terminal-bank key. The sorter recovers the original CPN and RN, saving RN in the user's file at block 22. It should be noted that in saving RN, the user's file is accessed by using his TIN as an index. The received CPN is applied as the data input to a coder 20, which receives RN as its key input, producing a reversible owner code (ROC) which is saved in the user's file in the same manner as RN. Various additional information is saved in the user's file, such as his personal account number (PAN), name, phone number (PHN), account balance, and other relevant information. The user's TIN, PAN or PHN can be used as an index to access the user's file. CPN represents coded authentication information since it is a coded form of the PIN, and since it is used in other parts of the system to authenticate the user and the transaction. The system preferably maintains RN as a secret number (although in the present embodiment the user file is not secret since it is accessed using a non-secret index) and ROC is maintained as a non-secret number. As explained in detail below, CPN is derivable from ROC and RN.

FIG. 7 illustrates how the originator generates a check in accordance with the present invention. This process preferably takes place at the originator's terminal or computer. It is assumed that the originator would be generating a check in the usual manner and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms, such as the recipient's name and TIN (RTIN), and the originator's personal account number and bank identification number. Preferably, the terminal includes a check reader and printer which can read necessary information from the originator's check form and print information on the form, although this could also be done manually by the originator. The originator and the recipient can be the same person, for example, where a person is cashing a personal check originated by the person. In the case of multi-party checks, the check is

“...and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms, such as the recipient's name and TIN (RTIN), and the originator's personal account number and identification number.”

“...FIG.7 illustrating how an originator generates a check...”

5,793,302

3

FIGS. 6–8 are functional block diagrams illustrating a check transaction system in accordance with a first embodiment of the present invention, with FIG. 6 illustrating user enrollment, FIG. 7 illustrating how an originator generates a check, and FIGS. 8A and 8B illustrating the authentication process when the check is presented to be cashed;

FIGS. 9–12 are functional block diagrams illustrating a credential issuing and authentication system in accordance with a second embodiment of the present invention, with FIG. 9 illustrating the enrollment of an official, FIG. 10 illustrating the enrollment of a user, FIG. 11 illustrating the issuance of the credential, and FIG. 12 illustrating the authentication of an issued credential;

FIGS. 13A–13E, when arranged as illustrated in FIG. 14, collectively represent a functional block diagram of a check transaction system similar to that of FIGS. 6–8, but including the basic processing necessary to clear and pay a check electronically;

FIGS. 15A–15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention; and

FIG. 16 is a functional block diagram of a system for authenticating a party and for authorizing access to a secret file associated with the party according to an alternate embodiment of the present invention.

4

three phases of operation. In the first phase, illustrated in FIG. 6, a user of the system must enroll in order to be recognized by the system. Each user enrolls at his or her bank, or at another convenient location, such as a place of employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of FIG. 6 with the typical transaction information, including the user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be

“...and FIGS. 8A and 8B illustrating the authentication process when the check is presented to be cashed;

5,793,302

3

FIGS. 6–8 are functional block diagrams illustrating a check transaction system in accordance with a first embodiment of the present invention, with FIG. 6 illustrating user enrollment, FIG. 7 illustrating how an originator generates a check, and FIGS. 8A and 8B illustrating the authentication process when the check is presented to be cashed;

FIGS. 9–12 are functional block diagrams illustrating a credential issuing and authentication system in accordance with a second embodiment of the present invention, with FIG. 9 illustrating the enrollment of an official, FIG. 10 illustrating the enrollment of a user, FIG. 11 illustrating the issuance of the credential, and FIG. 12 illustrating the authentication of an issued credential;

FIGS. 13A–13E, when arranged as illustrated in FIG. 14, collectively represent a functional block diagram of a check transaction system similar to that of FIGS. 6–8, but including the basic processing necessary to clear and pay a check electronically;

FIGS. 15A–15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention; and

FIG. 16 is a functional block diagram of a system for authenticating a party and for authorizing access to a secret file associated with the party according to an alternate embodiment of the present invention.

4

three phases of operation. In the first phase, illustrated in FIG. 6, a user of the system must enroll in order to be recognized by the system. Each user enrolls at his or her bank, or at another convenient location, such as a place of employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of FIG. 6 with the typical transaction information, including the user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be

“...method for authenticating the transfer of funds...”

5,793,302

33

a credential by a trusted party, the credential information including information associated with the at least one party, and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1.

48. The method of claim 41 wherein the first party and the second party are the same party.

49. The method of claim 48 wherein the second storage means comprises a credential.

50. The method of claim 41 wherein the first storage means comprises a credential, and the second storage means comprises a credential.

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

57.
an ac
associ
being

5 rece
in
p
s
a

10 gen
u
in
fo
a

15 dete
fu
tran

to
p
th

gen

“You mentioned earlier that you’re well familiar with claim 51, yes?”

A. Yes...”

“So can I communicate with you today by talking about four steps, receiving, generating, determining and transferring?”

A. Please.

Q. Okay. So in what we’ve just seen at figure 8B, would you agree that the originator bank in the described embodiment performed all four of those steps?”

Page 18

1 Q. And then let's go now to claim 51.

2 You mentioned earlier that you're well

3 familiar with claim 51, yes?

4 A. Yes. What claim? It does not mean it would

5 not help me to have it in front of me.

6 Q. It's column 33, it would be tedious to read

7 the whole claim into the record.

8 So can I communicate with you today by

9 talking about four steps, receiving, generating,

10 determining and transferring?

11 A. Please.

12 Q. Okay. So in what we've just seen at figure

13 8B, would you agree that the originator bank in the

14 described embodiment performed all four of those

15 steps?

16 MR. WILLIAMS: Objection to form.

17 THE WITNESS: I need a moment.

18 MR. WILLIAMS: I'll also object as outside

19 the scope, but I'll permit the witness to answer.

20 THE WITNESS: It appears to me that all four

21 of those steps are performed in figure 8B that we've

22 just been looking at in Stambler's embodiment.

23 BY MR. WILLIAMS:

24 Q. So in the '232 patent, in the embodiment we

25 just walked through, all steps of the authentication

“THE WITNESS: 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.”

[illegible]

“Q. So in the '302 patent, in the embodiment we just walked through, all steps of the authentication activity are performed by the originator bank, one entity?

THE WITNESS: If that's his only embodiment, it appears to me that in his embodiment, that is true."

“Is there any disclosure in the detailed description of the '302 patent of those four steps being divided up among more than one entity?”

“THE WITNESS: I have not detected it, but I would need to read -- I think I probably need to read through the whole embodiment to be confident there was no -- ”

Page 19

1 activity are performed by the initiator bank, one
2 entity?

3 MR. WILLIAMS: Objection in fact.
4 THE WITNESS: If there's any only embodiment,
5 it appears to be that in the embodiment, that is true.
6 BY MR. PROSECUTOR:
7 Q. In your understanding and review of the '302
8 patent, did you identify any disclosure of any way
9 that the '302 patent discloses dividing up those steps
10 so that different actors play that role or that
11 different actors perform the same role?

12 MR. WILLIAMS: Objection in fact. Based on a
13 seemed, objection in fact and outside the scope.
14 THE WITNESS: It appears to me that claim 51
15 could be recited that way, but that there is no
16 requirement in claim 51 that the steps be
17 performed by the same entity.
18 BY MR. PROSECUTOR:
19 Q. Okay. The question is a little bit
20 different.
21 Is there any disclosure in the detailed
22 description of the '302 patent of those four steps
23 being divided up among more than one entity?

24 MR. WILLIAMS: Same objection.
25 THE WITNESS: I have not seen -- it appears

Exhibit 2005 Page 19

Page 20

1 to me from what I have read this morning and what has
2 been explained to me that in the portion of the
3 embodiment that we read, all four steps are done by
4 one entity.
5 BY MR. PROSECUTOR:
6 Q. Okay. I appreciate that, but the remaining
7 goes one step further, which is: How you determined
8 any place in the '302 patent where it discloses those
9 four steps being performed by respective different
10 entities?

11 MR. WILLIAMS: Same objection.
12 THE WITNESS: I have not detected it, but I
13 would need to read -- I think I probably need to read
14 through the whole embodiment to be confident that
15 there was no --
16 BY MR. PROSECUTOR:
17 Q. By the way, the taxpayer ID number on "THE
18 DATE in the abbreviation in Figure 10, that's
19 nonsecret information in the context of these
20 embodiments, right?

21 MR. WILLIAMS: Objection to form.
22 THE WITNESS: I don't actually see that it
23 appears in that form.
24 BY MR. PROSECUTOR:
25 Q. All right, please, go to line 11.

Exhibit 2005 Page 20

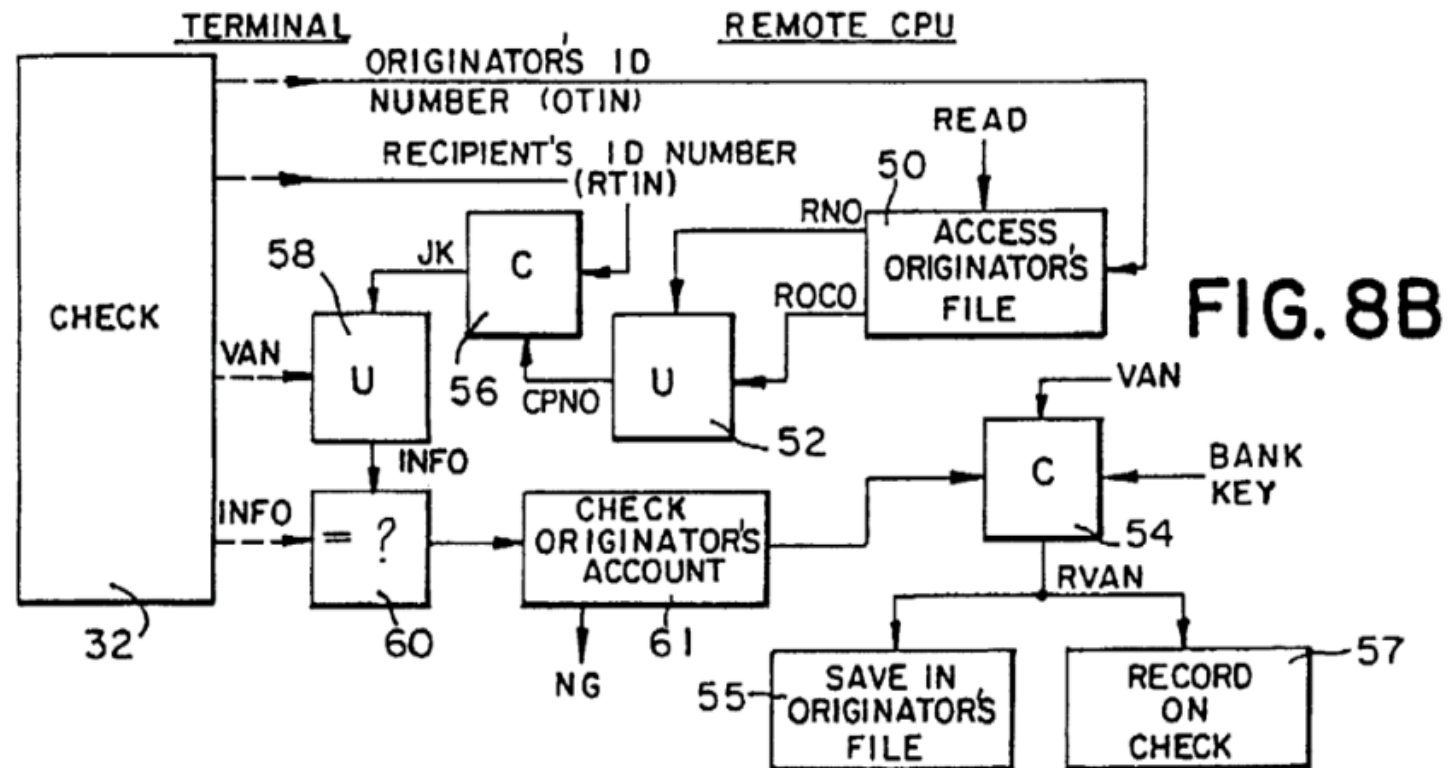
CBM2015-00044
Patent No. 5,793,302

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.

"The VAN shown in Figure 8B is generated at the originator's computer, not at the *originator's bank*."



“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).”

CDM2015-00044
Patent No. 5,793,302

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 5:1-6.

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

CDM2015-00044
Patent No. 5,793,302

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 11. Patent Owner accepts the construction that petitioner offered in CDM2015-00013. *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.

“...must be performed by a single entity. Otherwise, there would be insufficient written description to enable the claim.”

62. After reviewing the specification, I am of the opinion that the limitations of claim 51 must be performed by a single entity. Otherwise, there would be insufficient written description to enable the claim. Said another way, a person of ordinary skill in the art would not have sufficient written description in the specification to enable implementing claim 51 such that multiple entities divide up the performance of the comprising steps. To stray from the specification in this fashion would require undue experimentation and with little predictability of success.

63. As stated previously, claim 51 sets forth a method comprising four steps: receiving funds transfer information, generating a VAN, authenticating the funds transfer information using the VAN and credential information, and transferring the funds if the transfer information is determined to be authentic.

64. The sole support for this claim 51 in the specification is the funds transfer embodiment I previously discussed. In that embodiment, all four steps are performed by the originator's bank. The bank first receives the funds, generates a VAN, compares the VAN against the VAN on the funds transfer information, and transfers the funds if the comparison fails.

65. Such an embodiment is easy to understand and straightforward for a person of ordinary skill in the art to implement. Each step is a clear precursor for the next.

Exhibit 2004 Page 21

66. If multiple entities perform these steps, there is information deficient about how to implement the claim. For example, if one entity receives the funds transfer information, and another entity then determines the VAN, the claims and the specification do not describe how the funds transfer information gets from the first entity to the second. Or, if one party performed those first two steps, but another party determined if the VAN was authentic, the patent says nothing about how the VAN is transmitted *and* how it would be transmitted *securely*. Because the VAN is an authentication number, it would have to be transmitted securely (without significant vulnerability from attacks) from the party generating the VAN to a party determining if the VAN is authentic.

“If multiple entities perform these steps, there is information deficient about how to implement the claim.”

67. Cryptographic protocols, including authentication protocols, are notoriously difficult to get correct. For example, the Needham-Schroeder protocol, published in 1978, was found to have a weakness (vulnerable to a “replay attack”) in 1981. It should be noted that this protocol was developed by two people with Ph.D.’s and a wide number of years of experience. In other words, two individuals that were *far above* one of *ordinary* skill in the art. For a person of ordinary skill in the art to know how to alter claim 51 to be performed by multiple parties, this hypothetical individual would have to create a workable cryptographic protocol to keep the authentication secure. This is particularly so when no measures are

“Cryptographic protocols, including authentication protocols, are notoriously difficult to get correct.”

Exhibit 2004 Page 22

Page 70

1 S. NIELSON

2 So in that hypothetical, do you still

3 think that there's a lack of written description

4 in the specification to enable that?

5 MR. GREENSPOON: Object to the form.

6 THE WITNESS: So if we have steps 1

7 and 2 done by a different entity than steps

8 3 and 4, I think I've already identified one

9 of my concerns with it, which is that I

10 don't think that reads correctly.

11 But if you're going to have -- so

12 where you have the -- So I don't think there

13 is written description to describe how you

14 split that up between those two entities.

15 BY MR. WILLIAMS:

16 Q. All right. Do you have the patent?

17 A. Yes, I've got it.

18 Q. Let's just start with the basics. So

19 how is the check being presented in this

20 embodiment? Like physically where is the check

21 showing up to begin this process?

22 A. So the word "check" isn't in Claim 51,

23 but you're just referring to the embodiment that

24 I --

25 Q. So the embodiment that's described

TSG Reporting - Worldwide 877-702-9580
MasterCard, Exh. 1023, p. 70

“So in that hypothetical, do you still think that there’s a lack of written description in the specification to enable that?

THE WITNESS: So if we have steps 1 and 2 done by a different entity than steps 3 and 4, I think I’ve already identified one of my concerns with is, which is that I don’t think that reads correctly.

But it you’re going to have -- so where you have the -- So I don’t think there is written description to describe how you split that up between those two entities.”

originated by a present party (i.e., the originator) in favor of an absent party (recipient).

The originator enters his or her PIN at a terminal or computer. Through irreversible code **28**, the originator's PIN is converted into a coded PIN (CPNO), which is applied as the key input to code **28**. The data input to code **28** is the recipient's TIN (RTIN), which has been read from the check, or accessed from the computer memory, or entered by the originator. The data output of code **28** is a joint key (JK) which is applied as the key input to a code **30** (JK). Generally, the JK is generated using information associated with at least one of the parties involved in the transaction (in this case, the originator and recipient). As will be shown more fully below, the joint key (or code) is used to protect and authenticate the originator and recipient. The data input to the code **30** is the information (INFO) to be authenticated (that is, information relevant to the transaction, such as check number, amount, etc.).

The data output of the coder 30 is a variable authentication number (VAN), which codes the information to be authenticated, based upon information related to the recipient and information related to the originator. Note that the VAN is alternatively generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the JK. The VAN and at least a portion of the information relevant to the transaction are written or imprinted upon the check 32, thereby becoming a permanent part of it. Alternatively, the check may represent an electronic transfer of funds or some other electronic transaction. In this case, the VAN and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction.

It is contemplated that in creating the VAN, all information would not necessarily be coded in the same manner. For example, the amount of the check might be considered important enough so as to be recoverable completely, and it would be coded into the VAN in a manner that would permit complete recovery. Other information, such as the date and check control number might be considered less important and would be coded into the VAN in such a manner as to permit detection of changes (e.g., error detection coding), but without complete recovery of the original information.

As noted above, other predetermined information which is known jointly by the originator and recipient, and which does not appear on the check, can also be used to derive the VAN. For example, when a check is drawn to multiple recipients, e.g., husband and wife, each recipient's TIN (which does not appear on the check) may be used to derive the joint code and VAN. This makes it more difficult to fraudulently generate the VAN since the predetermined information not appearing on the check would not be generally known.

FIGS. 8A and 8B illustrate the authentication process at a terminal when the recipient presents the originator's check to be cashed. The terminal communicates via a network of the banks involved in the transaction. Preferably, the terminal includes a device which can read information directly from the check 32. Alternatively, the terminal operator can manually key information into the terminal, based upon information appearing on the face of the check 32. At block 40, the recipient inserts his or her PIN, and at block 41, identifies his bank and enters his TIN (RTIN) and all information required by the terminal to initiate the transaction. An irreversible code 42 processes the PIN to produce the coded PIN, CPNR, which is applied as the key input to

a coder 44. A random number generator produces a random number (i.e., an arbitrary number) RNKX which is applied as the data input to coder 44. Coder 44 then produces a coded random number (i.e., a coded arbitrary number), CRNX, which is applied to mixer 40 along with RNKX. The output of the mixer is, therefore, a signal which contains CRNX and RNKX is a converted form, so that neither number nor CPNR may readily be discerned from the signal. CRNX represents coded authentication information because it is a coded representation of CPNR, and because it is used by the system to authenticate the recipient and the transaction.

The mixer signal, along with the information entered in block 41 and the information read from the check are transmitted to the computer at the recipient's bank (i.e., remote bank CUF) over preferably an unsecured line (the use of an unsecured line is possible because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62). The system first authenticates the identity of the check holder at the recipient's bank. Next, the information on the check, as well as the originator and recipient, are authenticated at the originator's bank.

At the recipient's bank, the output of mixer 48 is received in a sorter 62, which separates CRNK and RSN, with CRNK being applied to a comparison block 64 and RSN being applied to a comparison block 66. The output of comparison block 64 is applied to a control block 68, which generates the recipient's RTN. RTN, his bank's computer is able to secret his file at block 64 and to extract his ROC (a non-secret number) and RSN (a secret number). ROCK and JNN (secret inputs, respectively) to an undoer 70, which generates the recipient's CPNR. CPNR, which is applied as the key input to coder 64. Coder 66, therefore, reproduces the recipient's coded random number, CRNK (in the same manner as coder 64). The output of coder 66 is applied to a comparison block 68. It should be appreciated that the CPNR output of undoer 70 is the true CPNR derived from the bank's records. Accordingly, the CRNK produced by coder 64 in the transaction is compared to the CPNR produced by coder 66. If the authentication of the recipient has failed and it is presumed that recipient is not the party presenting the check, the transaction is therefore aborted. On the other hand, if the

recipient's identity is authenticated, the transaction can proceed. The recipient's bank then communicates with the originator's bank, conveying all the information about the transaction and requesting authorization to pay (block T1).

As shown in FIG. 6B, at the originator's bank, using OTN (or the originator's PAN) as an index, the originator's ROCO and random number, RNO, are extracted from the originator's file at block 50. ROCO is applied as the data input to an uncoder 52, and RNO is applied as the key input to uncoder 52. Uncoder 52 therefore reverses the operation performed by coder 20 (FIG. 6) when the originator enrolled, producing the originator's CPN, CPNO. CPNO is then applied as the key input to a coder 56, which receives the recipient's TIN, KTIN, as the data input.

In accordance with the embodiment just described, it is contemplated that security considerations may warrant revising the ROC from time to time independent of any transaction. Toward this end, CPN could be reconstituted from the current ROC and RN as in block 52. Next, a new RN is used with CPN to generate a revised ROC, making use of a coder in the same manner as coder 28 of FIG. 6. The user's new RN and ROC are stored and accessed, and CPN need only be reproduced at the bank where the user maintains an account.

In the same manner as coder 28 of FIG. 7, coder 56 therefore produces the joint key JK. JK is applied as the key

“The recipient’s bank then communicates with the originator’s bank, conveying all the information about the transaction and requesting authorization to pay (block 71).”

5,793,302

7

input to an uncoder 58, which receives the VAN from check 32 as its data input. Uncoder 58 therefore reverses the coding operation performed by coder 30 of FIG. 7. If the information on the check has been unmodified, the coder 58 should therefore reproduce the information INFO from the check which was sought to be authenticated. In block 46, a comparison is made between the output of uncoder 58 and the information appearing on the check. Failure of this comparison is an indication that the check may have been modified after being issued, and the originator's bank notifies the recipient's bank that the check will not be honored.

Alternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can then be compared with the VAN from the check to authenticate the check.

Should the comparison be favorable, this is an indication that the check is authentic and unmodified, and the originator's bank accesses the originator's account (block 61) to determine if the account is in order and has sufficient funds or credit to pay the check. The date of the check is determined to be acceptable. If the check control number does not appear in the originator's file as a previously cashed check, then the current check control number is saved to prevent fraudulent check reuse. The originator's bank generates a redeemer or redemption VAN (RVAN) in order 54, using its bank key and the original VAN. RVAN is saved in the originator's file (block 55) and is recorded on the check (block 57). The originator's account is then debited. The originator's bank then authorizes the recipient's bank to pay the check. On the other hand, if originator's bank finds any irregularity in the check or in the originator's account, it will notify the recipient's bank that the check is dishonored.

The RVAN (and other RVAN's from other transactions) can be accessed from originator's files by banks and other financial institutions involved with processing checks to determine the status of checks. Thus, by creating and storing the RVAN's in the originator's files, fraudulent reuse of checks is avoided.

At block 72 (FIG. 8A), the recipient's bank receives the originator's bank's instructions. It will then notify the recipient if the check has been dishonored. If the check has been honored, the recipient's account may be credited as in a deposit. Alternatively, the recipient can receive payment immediately if he is at an appropriate terminal, such as an automatic teller machine.

Essentially, the check has cleared automatically, on-line, without further check handling or processing.

In a transaction where the user cashes his own personal check, the originator and recipient are one and the same. A VAN is created from a joint code which combines information associated with the user, such as the user's identification number (TIN or PAN) and the user's CPN, which is generated directly from a PIN entered by the user. When the VAN is authenticated, the joint code is derived by combining the user's identification number (TIN or PAN), and the user's true CPN, which is generated from the RVN and RBCD retrieved from the user's file, with the TIN (or PAN) serving as a file index.

As noted above, in FIG. 8A it is possible to use an unsecured link between the mixer 48 and the sorter 62 because CCRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62. However, a security problem still exists in using an unsecured line between the mixer 48 and the sorter 62 because the signal can be recorded and then played back later to attempt to fraudulently authenticate a fraudulent transaction. In an alternate embodiment of the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the recipient's terminal by coding at least a transmission date and time with the CPNR by a coder (not shown). The ADVAN is then mixed with the CCRNX and the RNX by the mixer 48 and sent to the remote bank CPU over the unsecured line to the sorter 62. At the remote bank CPU, the CPNR which is generated by the uncoder 70 is used to uncode the ADVAN to regenerate the transmission date and time. The signal received over the unsecured line is then authenticated by comparing the regenerated transmission date and time to a reception date and time (that is, the date and time at which the signal was received at the remote bank CPU). In this manner, the recipient and transaction are further authenticated.

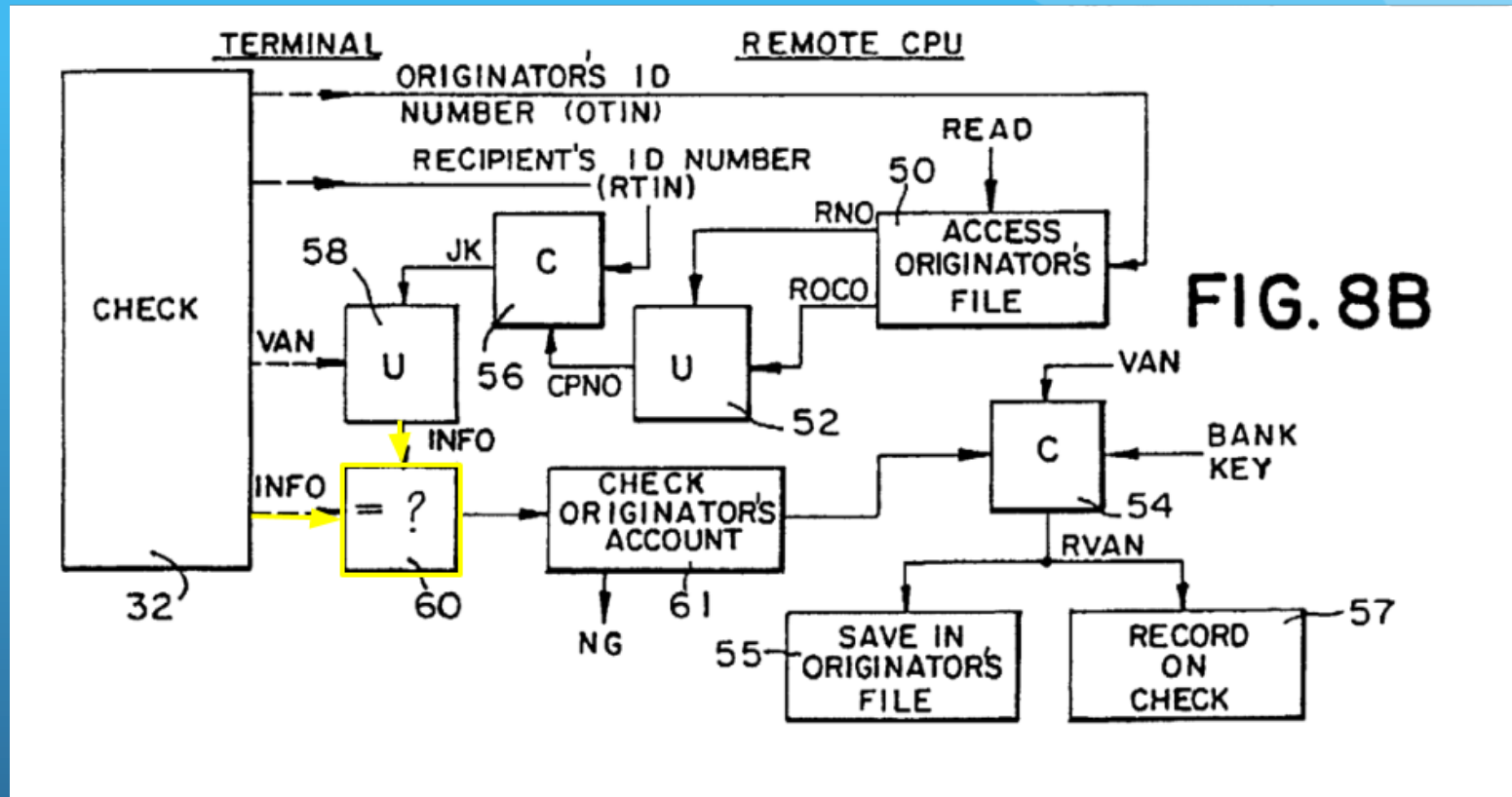
According to another embodiment of the present invention, RNX is generated at both the recipient terminal and the remote bank CPU. To generate the RNX at the remote bank CPU, a random number generator is located at the remote bank CPU, wherein the random number generator at the remote bank CPU is similar to and synchronized with the random number generator 46 located at the recipient's terminal. Instead of transferring the RNX and the CCRNX, only the CCRNX is transferred over the unsecured line from the recipient's terminal to the remote bank CPU. At the remote bank CPU, the CPNR generated by the uncoder 70 is coded by the coder 66 with the RNX generated at the remote bank CPU to generate the CCRNX. The generated CCRNX is then compared by the comparator 64 with the CCRNX transferred from the recipient's terminal to the remote bank CPU to authenticate the recipient and the signal received over the unsecured line. In this manner, the recipient and transaction are further authenticated.

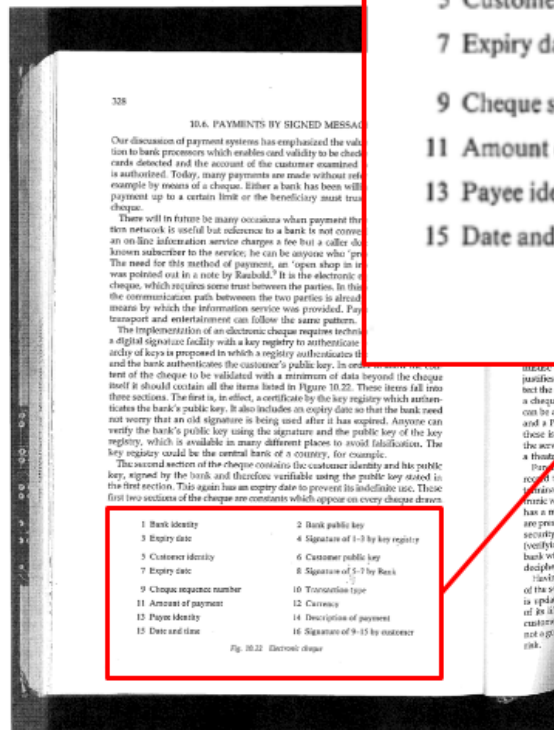
According to another embodiment of the present invention, CCRNX is never generated. Instead, the CPNR generated by the uncoder 42 is sent to the remote bank CPU over a secured line, rather than over an unsecured line. The CPNR generated by the uncoder 70 is then compared by a comparator (not shown) with the CPNR sent from the recipient's terminal to the remote bank CPU to authenticate the recipient. In this alternate embodiment, the random number generator 46, coder 44, mixer 48, sorter 62, and coder 66 are not required, although a secure line is required.

FIGS. 9-12 constitute a functional block diagram illustrating the present invention in a credential issuing and authentication system. The system involves the same three phases of operation as the check transaction system of FIGS. 6, 7, 8A and 8B. However, all users are enrolled by an authorized official who must be enrolled first. Accordingly, there are two enrollment processes which are somewhat different. The first one is enrollment of the official, and the second one is enrollment of a user prior to or at the time of issuing his credentials. It is contemplated that this system 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. This system would also be useful in protecting against unauthorized access to all types of records, as previously indicated.

FIG. 9 illustrates enrollment of the official. This can be accomplished at a terminal or computer which is in communication with a remote computer over a link which is assumed to be secure. The remote computer may, for example, be the central computer at the agency issuing the credentials. At the remote computer, number generator 100 generates a random number which, at block 102, is com-

“Alternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can then be compared with the VAN from the check to authenticate the check.”





- 347 -
MasterCard, Exh. 1004, p. 347

Ex. 1004 – D. W. Davies *et al.*, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer* (1989), Fig. 10.22

“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.”

CRM201540044
Patent No. 5,793,302

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 15, at 36-38. This argument fails for several reasons.

First, Patent Owner never explains the basis for its premise. The “previously issued” credential discussed in the preamble does not appear in the claim until the “Materializing” step. Accordingly, the claim requires only that the credential be issued before the “Materializing” 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 56. Davies thus describes how the token stores a credential (i.e., a previously issued credential) before being presented 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

CRM201540044
Patent No. 5,793,302

about the transaction, to form the electronic check message sent back to the token for signing. Id. at 328-31. Specifically, the “consumer’s response 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 (arrows 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 credential, 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” (i.e., receiving information) “including information for identifying the amount 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. Pages 15, at 34-45. 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.

CBM2015-00044
Patent No. 5,793,302

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.

16

“Therefore, Davies teaches that the certificate containing the 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.”

“As such, the court construes ‘previously issued’ to mean ‘issued before the execution of the steps recited in the claim’ and finds that the ‘previously issued’ limitations are not separate steps in the claimed methods.”

instrument. Therefore, the court rejects Defendants’ plain meaning construction. Rather, the court construes this phrase to mean “joining the VAN to the payment instrument.”

r. “previously issued” / “being previously issued” / “is previously issued”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction
issued before the execution of the steps recited in the claim	issued before the execution of a requirement of the claim
The term is not an additional claim step.	The term is a claim step.

Plaintiff’s proposed construction for “previously issued” was adopted by the *JPMorgan*, *Merrill Lynch*, and *Chase* courts, which held (1) that “previously issued” means “issued before the execution of the steps recited in the claim” and (2) that this term does not give rise to an additional claim step. Having reviewed Defendants’ arguments, the court is not convinced that its previous three constructions were erroneous. As such, the court construes “previously issued” to mean “issued before the execution of the steps recited in the claim” and finds that the “previously issued” limitations are not separate steps in the claimed methods.

s. “the adequacy of the funds in the first party’s account being verified after the instrument is issued”

Plaintiff’s Proposed Construction	Defendants’ Proposed Construction
the adequacy of the funds in the first party’s account being verified after the instrument for transferring funds is issued	after the instrument is issued, determining whether or not the first party has sufficient funds in his/her account to transfer funds
This term is a limitation, but is not an additional claim step.	

The parties’ argument with regard to the phrase “the adequacy of the funds in the first party’s account being verified after the instrument is issued” is whether the phrase recites an additional step in the claimed method. In *JPMorgan*, this court rejected Defendants’ argument

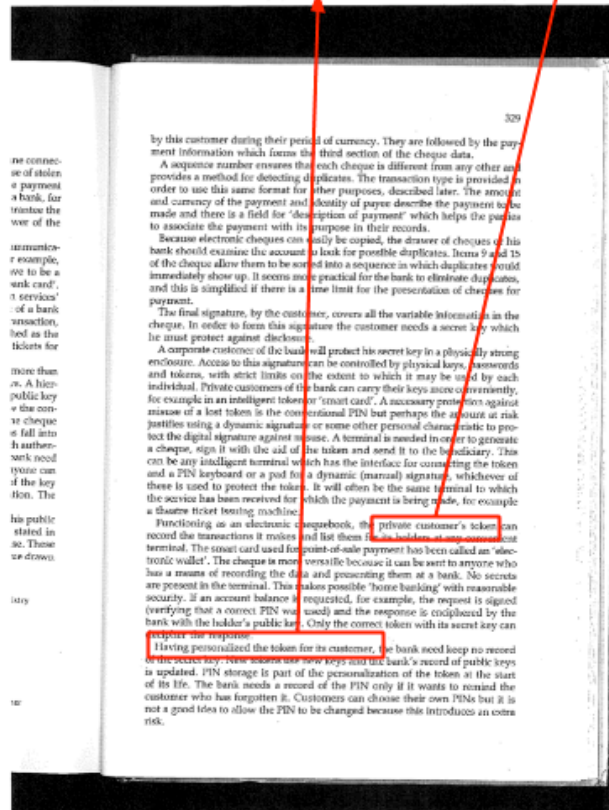
to the method being performed, "a credential being previously issued to at least one of the parties." MasterCard points to the customer's certificate stored in the electronic check as the claimed "credential." There is no disclosure stating that this "credential" is created, much less *issued* to the 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

"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."

“private customer’s token”

“Having personalized the token for its customer...”

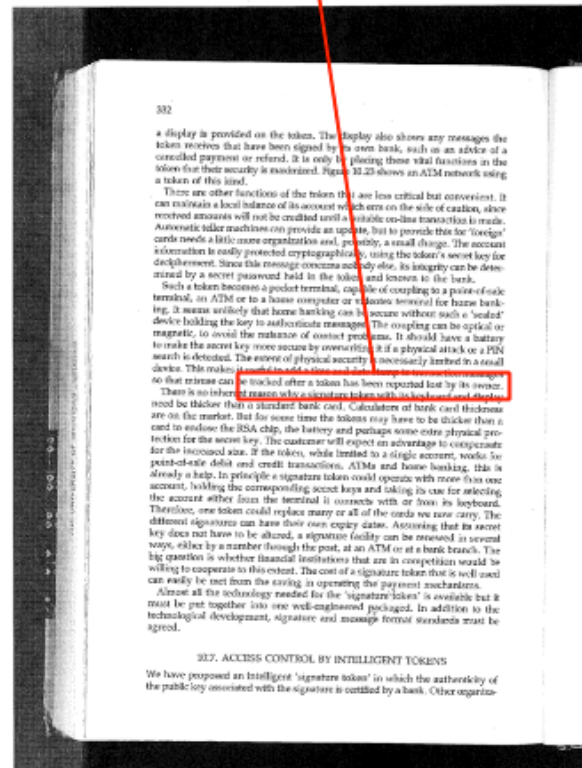


- 348 -

MasterCard, Exh. 1004, p. 348

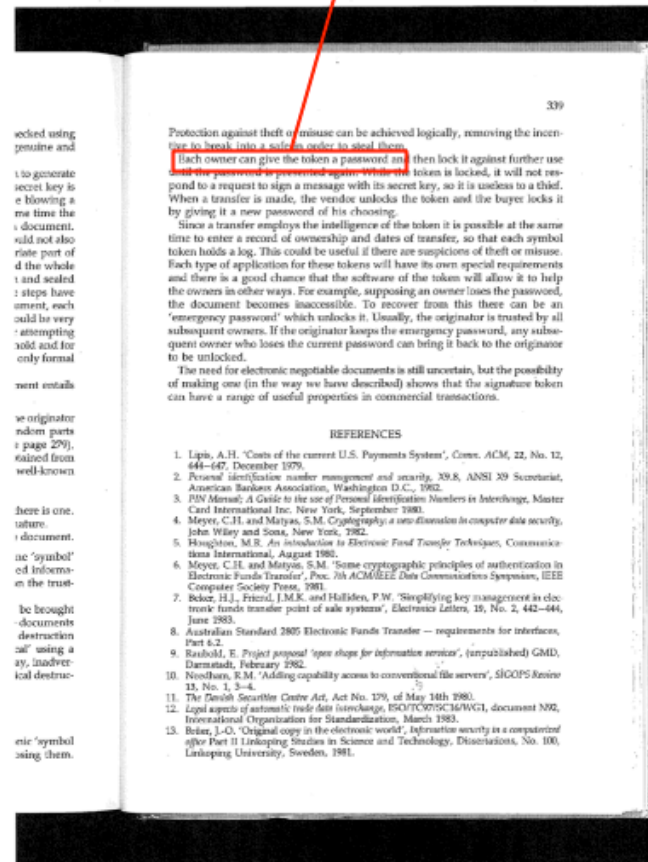
Ex. 1004 – D. W. Davies *et al.*, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer* (1989), p. 329

“...can be tracked [if] lost by its owner...”



- 351 -
MasterCard, Exh. 1004, p. 351

“Each owner can give the token a password...”



Page 73

1 A. I do not remember.

2 Q. Some of the fields are already disclosed to

3 be optional, right, such as description of payment,

4 14?

5 A. I believe that one's optional. I don't know

6 if there's another optional one or not.

7 Transaction type, I don't know what a

8 transaction type is.

9 Q. You don't? On page 331, the end of the first

10 paragraph is actually not a full paragraph but the end

11 of the first paragraph has this sentence "To

12 differentiate these messages and provide for even

13 wider use, the format of figure 10.22 includes the

14 transaction type which denotes a customer check, ATM

15 request, interbank payment, payment advice and so

16 forth."

17 A. Thank you.

18 Q. Does that refresh your --

19 A. That refreshes my memory. It seems like it

20 would need a transaction type.

21 Q. So is it fair, then, to read that field 10,

22 the transaction type, is going to control whether the

23 customer check is to be utilized as a person-to-person

24 check versus an ATM request?

25 A. I think so.

"Q. So is it fair, then, to read that field 10, the transaction type, is going to control whether the customer check is to be utilized as a person-to person check versus an ATM request?

A. I think so."

Page 74

1 Q. So an ATM request could be a code that goes
2 into field 10 that indicates that some of the other
3 fields might be optional for this usage, right?
4 A. Yes.
5 Q. Now, in the workflow of the ATM embodiment,
6 they have a picture, figure 10.23, right?
7 A. Yes.
8 Q. And the very origin of this collection of
9 arrows is this box under the first box which seems --
10 A. The keypad, that's a keypad. That appears to
11 me to be the request comes from a keypad, which is the
12 little box under the ATM.
13 Q. Yes, and the word "request" is next to those
14 as a symbol of some sort of keypad, right.
15 And then that first arrow goes to what looks
16 like a -- resembles a calculator of the era?
17 A. Yes.
18 Q. That's going to be a keypad possibly with the
19 display?
20 A. That's the token.
21 Q. So the words next to that symbology are
22 amount, PIN, pay.
23 So do you take from that that the workflow is
24 somebody somehow electronically connects the token to
25 the ATM machine, makes some sort of request on the ATM

TSG Reporting - Worldwide
(877) 762-9580
EXHIBIT 2005 PAGE 74

“Q. So 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, right?”

A. Yes.”

Page 78

1 person to person example.

2 So the population of usable fields in the

3 format of 10.22 can differ as between a customer check

4 transaction type and ATM transaction type, correct?

5 A. Well, since he specifies that the transaction

6 type field could include ATM request, I think the

7 answer is yes.

8 Q. Electronic checks can be easily copied,

9 right?

10 A. Yes.

11 Q. Okay. So let's go to your opinion on how

12 these two transaction types described in Davies

13 section 10.6 might read on claim 51.

14 A. All right.

15 Q. First of all, what is the so-called

16 credential?

17 A. So as I said to you earlier, the credential

18 is the unpopulated check that will be filled in inside

19 the -- by the actions of the customer and completed

20 inside the token.

21 Q. Who issues that unpopulated check?

22 A. The bank.

23 Q. So the claim language requires that the

24 credential is issued to at least -- well, the

25 credential is issued by a trusted party.

USG Reporting - Wordworks
(877) 535-9580
EXHIBIT 2005 PAGE 78

“Q. So the population of usable fields in the format of 10.22 can differ as between a customer check transaction type and ATM transaction type, correct?”

A. Well, since he specifies that the transaction type field could include ATM request, I think the answer is yes.”

Page 99

1 S. NIELSON

2 It's not entirely clear how changing

3 the transaction type would adjust your format for

4 10.22.

5 Q. Well, 10.22, field 10, that's

6 transaction type?

7 A. Right.

8 Q. So isn't that the field that's being

9 discussed there?

10 A. Right. What I'm saying is, you don't

11 need, say, Item 13 or 14 in 10.22, or at least

12 it's not necessarily going to be the same set.

13 Q. So you say at the bottom of 76 that if

14 the transaction type is an ATM, there would be no

15 need to write payee identity into the check. And

16 that's field 13, right?

17 A. Field 13, yes.

18 Q. So I don't understand, though, why you

19 say that. Someone is going to need to be paid,

20 right?

21 A. Well, if you're doing an ATM

22 withdrawal, then the customer's identity would be

23 the same identity as the payee.

24 Q. Why do you say that?

25 A. Because the money is being withdrawn

TSG Reporting - Worldwide 877-702-9580
MasterCard, Exh. 1023, p. 99

“Q. So you say at the bottom of 76 that if the transaction type is an ATM, there would be no need to write payee identity into the check. And that's field 13, right?”

A. Field 13, yes.”

Page 10

Q. Now, Bank A.

A. Yes.

Q. And there are distinct banks?

A. Yes.

Q. And that Bank A needs to get paid before any money is going to go out of that ATM, right?

A. Yes.

Q. So there has to be some way for it to send money back to know who to pay?

A. Yes.

Q. Wouldn't it be logical as far as identifying from the check field for payment identity?

A. Well, I don't know that that's necessarily true. I guess I'm still thinking about my paper check example. I don't see paper checks or an ATM, but when you write a check to cash or something, that the payee identity is -- I'm not sure. I don't know.

Q. It would be one way to do it though, right, would be to identify bank A in that field?

127

The Witness: (shakes his head) No, that was not what he said.

Page 10

Q. Now, Bank B.

A. Well, the reason why that seems odd to me is that this line to work for your system at your own ATM is well, so also goes into the payment identification? I don't see that that makes sense.

Q. But in the case where you're not at your ATM, what I just said would work, correct?

A. I'm not sure. I don't know.

PR. WILLIAMS: So we can take a break if we need one, otherwise we can keep pushing through here.

(the witness.)

THE WITNESS: Let me just ask you to let me answer, the reason why it's not clear is because lawyer doesn't describe it. You know, there are a lot of different ways we can conjecture about it, but my point was it's not described.

BY MR. WILLIAMS:

Q. He describes the ATM example as involving making a payment to Bank A, though?

A. Yes, he does.

Q. And that is the bank's name -- that's the payer bank?

128

The Witness: (shakes his head) No, that was not what he said.

“Q. Wouldn’t it be logical to put that identity into the check field for payee identity?

A. Well, I don’t know that that’s necessarily true. I guess I’m still thinking about my paper check example. We don’t use paper checks at an ATM, but when you write a check to cash or something, that the payee identity is -- I’m not sure. I don’t know.

Q. It would be one way to do it, though, right, would be to identify Bank A in that field 13?

A. Well, the reason why that seems odd to me is that this has to work for when you're at your own ATMs as well. So what goes into the payee field then? I don't see that that makes sense."

CBM2015-00044
Patent No. 5,793,302

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,

"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."

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

“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.”

Page 109

1 S. NIELSON

2 A. It's the payee.

3 Q. Okay. You're basing that off of the

4 way the claim talks about the first party and the

5 second party, right?

6 A. Let me make sure. Yes, a transfer of

7 funds from an account associated with a first

8 party to an account associated with a second

9 party.

10 Q. Okay. So the Davies check doesn't

11 identify an account of the person being paid?

12 That's your point?

13 A. Yes.

14 Q. I got it. Okay.

15 The payee, however, is identified in

16 the Davies check?

17 A. It has an identity field for the

18 payee, yes.

19 Q. All right. In Paragraph 86, the last

20 sentence says: "Davies never ties together paper

21 checks and key registries."

22 So the electronic check in Davies

23 includes a signature of a key registry, right?

24 A. The electronic check includes a

25 signature by the key registry.

TSU Reporting - Worldwide 877-702-9580
MasterCard, Exh. 1023, p. 109

“Q. Okay. So the Davies check doesn’t identify an account of the person being paid? That’s your point?”

A. Yes.

Q. I got it. Okay.
The payee, however, is identified in the Davies check?

A. It has an identity field for the payee, yes.”

CBM2015-00044
Patent No. 5,793,302

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"¹²). 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

¹² The card issuing bank, which serves as a key registry for its customers, is a trusted party. See Ex. 2005, at 79:1-20.

"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')."

“The customer’s certificate is not used to determine the identity of the entity presenting the check.”

CBM2015-00044
Patent No. 5,793,302

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 signer 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 signer 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. *Id.*, 1004.

“Thus, we are not persuaded that Petitioner demonstrated that it is more likely than not that it would prevail in establishing the unpatentability of claims 51, 53, 55, and 56 as anticipated by Meyer.”

CBM2015-00044
Patent 5,793,362

Meyer textbook in support of its anticipation challenge. *E.g.*, Pet. 35–38, 43–45. Specifically, Petitioner cites (i) a non-cryptographic grocery transaction, (ii) the use of a cryptographic message authentication code (“MAC”), and (iii) the use of digital signatures based on public key algorithms, for different limitations of independent claim 51 (Pet. 19, 22, 35, 38, 42, 45), and in some instances, for the same limitations of claim 51, *e.g.*, a non-secret credential being previously issued by a trusted party to at least one of the parties, and reciting receiving funds transfer information (Pet. 37–41). Patent Owner argues that, “Petitioner mixes unrelated embodiments within Meyer that do not relate to one another, to stitch together what it believes will work as an anticipation contention. In fact, the distinct embodiments are incommensurable.” Prelim. Resp. 52.

We agree with Patent Owner. “For anticipation, it is not enough that the prior art reference discloses multiple, distinct teachings that the ordinary artisan might somehow combine to achieve the claimed invention.” *In re Akroy*, 455 F.2d 586, 587–88 (CCPA 1972); *Net Admonev, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). Petitioner cites to multiple and distinct portions of the Meyer textbook to disclose individual limitations of independent claim 51. None of the cited distinct embodiments — the non-cryptographic grocery transaction, or the cryptographic message authentication code (“MAC”), or the digital signature — is cited for each limitation of claim 51. For example, the non-cryptographic grocery transaction is not cited as disclosing the step of generating a VAN, the MAC generation is not cited as disclosing the step of transfer of funds, and the digital signature is not cited as disclosing the authentication of funds from an account associated with a first party to an account associated with a second party. Pet. 35–37, 41–44. Thus, we are not persuaded that Petitioner has demonstrated that it is more likely than not that it would prevail in establishing the

CBM2015-00044
Patent 5,793,362

unpatentability of claims 51, 53, 55, and 56 as anticipated by Meyer.

A. Proposed Objections Over Davies and Meyer

Petitioner provides explanations of how Davies and Meyer teach or suggest the limitations of the four challenged claims. Pet. 50–66. For claims 51 and 53, Petitioner cites to Davies as in its arguments for proposed anticipation by Davies, and adds citations to Meyer for the generating step of the recited method, along with the sequence of the method whereby at least a portion of the receiving step occurs before the generating step. Pet. 50–65.

For dependent claim 55, Petitioner makes the same assertions for obviousness as in its argument for proposed anticipation by Davies, namely, that Davies teaches or suggests that the VAN is generated by an error detection code (“Davies describes that the signature (“VAN”) on a message M is generated by signing H(M) using the sender’s secret key, where H(M) is obtained by applying a one-way function H to the message”). Pet. 63–64; *see also* Pet. 69 (“Davies ... suggest[s] that the signature, *i.e.*, VAN, is based on a one-way function”). Although as stated above, this argument is insufficient to demonstrate that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as anticipated by Davies, we are persuaded that the combination of Davies and Meyer teach or suggest claim 55’s limitations and that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as obvious over Davies and Meyer.

For dependent claim 56’s limitations, Petitioner cites to Meyer’s disclosure of a second VAN and of sending a “negative response” to the terminal if the requested transaction cannot be honored. Pet. 64–66; Ex. 1002, 597.

Patent Owner argues that because neither Davies nor Meyer anticipate the claims, “their combination cannot render the claims obvious.” Prelim. Resp. 56.

CBM2015-00044
Patent 5,793,302

unpatentability of claims 51, 53, 55, and 56 as anticipated by Meyer.

E. Proposed Obviousness Over Davies and Meyer

Petitioner provides explanations of how Davies and Meyer teach or suggest the limitations of the four challenged claims. Pet. 50–66. For claims 51 and 53, Petitioner cites to Davies as in its arguments for proposed anticipation by Davies, and adds citations to Meyer for the generating step of the recited method, along with the sequence of the method whereby at least a portion of the receiving step occurs before the generating step. Pet. 50–63.

For dependent claim 55, Petitioner makes the same assertions for obviousness as in its argument for proposed anticipation by Davies, namely, that Davies teaches or suggests that the VAN is generated by an error detection code (“Davies describes that the signature (“VAN”) on a message M is generated by signing H(M) using the sender’s secret key, where H(M) is obtained by applying a one-way function H to the message”). Pet. 63–64; see also Pet. 69 (“Davies . . . suggest[s] that the signature, i.e., VAN, is based on a one-way function”). Although as stated above, this argument is insufficient to demonstrate that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as anticipated by Davies, we are persuaded that the combination of Davies and Meyer teach or suggest claim 55’s limitations and that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as obvious over Davies and Meyer.

For dependent claim 56’s limitations, Petitioner cites to Meyer’s disclosure of a second VAN and of sending a “negative response” to the terminal if the requested transaction cannot be honored. Pet. 64–66; *Ex. 1022, 597*.

Parent Owner argues that because neither Davies nor Meyer anticipates the claims, “their combination cannot render the claims obvious.” Prelim. Resp. 56.

“For claims 51 and 53, Petitioner cites to Davies as in its arguments for proposed anticipation by Davies, and adds citations to Meyer for the generating step of the recited method, along with the sequence of the method whereby at least a portion of the receiving step occurs before the generating step. Pet. 50-63.”

Page 38

1 referring to?

2 Q. If you read through all the way to the end of

3 the paragraph 126 --

4 A. Yes, would improve the signing efficiency,

5 yes.

6 Q. The improvement in signing efficiency occurs

7 when you're dealing with a very large message, that's

8 when the one-way hash really improves signing

9 efficiency?

10 A. The efficiencies grow with the size of the

11 message, yes.

12 Q. So there will become a message so small the

13 efficiency doesn't improve and, in fact, it becomes

14 extra overhead for the process?

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

16 Q. So for this rationale of improving signing

17 efficiency, that's not a rationale for applying a

18 one-way hash that would apply to a short message like

19 fund transfer messages?

20 A. I think in that case, your thinking would not

21 be dominated by the improvement in efficiency, speed,

22 cost, yes.

23 Q. So Davies at least teaches no reason to

24 combine error detection codes into a funds transfer

25 cryptographic message because fund transfer messages

TSG Reporting - Worldwide
(877) 702-9580
EXHIBIT 2005 PAGE 38

“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.”