IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LEON STAMBLER,

Plaintiff,

v. CIVIL ACTION NO. 2:08-cv-462

MERRILL LYNCH & CO., INC; et al **JURY TRIAL DEMANDED**

Defendants.

PLAINTIFF'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER

I. INTRODUCTION

This is the second claim construction proceeding before this Court involving the Stambler patents. Presently at issue are five terms that were construed in *Stambler v. JPMorgan Chase & Co., et al.* (the "*JPMorgan* case") and fourteen terms designated by Defendants in this case. Plaintiff has amended several proposed constructions to conform to the Court's constructions in the *JPMorgan* case.

II. OVERVIEW OF THE PATENTS-IN-SUIT

This case involves two patents issued to Leon Stambler – U.S. Patent Nos. 5,793,302 and 5,974,148. The '302 and '148 patents (together the "Stambler patents") are titled "Method for Securing Information Relevant to a Transaction." The Stambler patents share a common specification and claim priority to an application filed on November 17, 1992.

The Stambler patents disclose novel methods to authenticate parties and information involved in transactions. (1:43-54.)[1] Claims 7, 41, 44, 46, 47, 48, and 55 of the '302 patent and claims 28, 34, and 35 of the '148 patent are asserted. [Dkt. No. 329.] With the exception of claim 7, which recites a method for coding information, the asserted claims relate to the transfer of funds and the authentication of information associated with the transfer of funds.

Because the concept of authentication permeates the Stambler patents, a brief introduction to "authentication" is provided. Authentication refers to a plurality of concepts. (See Ex. E at 360-61; Ex. F at 30.) The term authentication can refer to: (i) ensuring that a message has arrived exactly as it was sent, referred to as data integrity; and (ii) ensuring that a message came from the stated source, referred to as data origin authentication. (Ex. E at 360, 363, 365; Ex. F at 30, 140-41.) Authentication can also refer to verifying the identity of an individual, which is sometimes referred to as entity authentication. (Ex. E at 361, 367; Ex. F at 385.)

[1] Column:line, FIG., and Abstract references are to the '302 patent, attached as Exhibit A.

To assist the Court in construing the disputed terms, an overview of the funds transfer embodiments illustrated by FIGS. 6-8 of the Stambler patents follows. These embodiments demonstrate the enrollment of a payment originator (FIG. 6), the creation of a check (FIG. 7), and the redemption and verification of the check (FIGS. 8A and 8B). Although the embodiments of FIGS. 6-8 are described in the context of creating and authenticating a check, the Stambler patents explain that these embodiments (and the disclosed concepts) apply equally to electronic funds transfers and a "paperless/cashless" transaction system, which completes transactions "entirely electronically." (5:28-30; 24:4-7.)[2]

FIG. 6 illustrates the enrollment of an originator at his/her bank. (4:2-51.) The process involves the originator providing the bank with personal information (e.g., a tax identification number, phone number, etc.), and the bank verifying the originator's identity. (4:3-8.) After verifying the originator's identity, the bank opens an account and creates a file for the originator. (4:8-11.) The originator also selects a secret personal identification number ("PIN"), which is irreversibly coded and transferred to the bank. (Id.) As will be described more fully below, the coded PIN is used by the originator and the originator's bank to generate cryptographic keys that are used to code or uncode funds transfer instructions (e.g., a check).

FIG. 7 illustrates generation of funds transfer instructions by an originator – in this example, the originator creates a check. (4:52-53.) The originator inputs funds transfer instructions into a terminal or computer. (4:53-54.) These instructions include the originator's tax identification number ("TIN"), the recipient's TIN, an amount, and other information that is relevant to the transaction. (4:54-60.) In this embodiment, the originator also inputs his/her PIN, which is irreversibly coded to produce the coded PIN. (5:3-6.)

The originator's terminal (or computer) generates a particular cryptographic key, which Mr.

[2] The patents also describe credential issuing and authentication systems. (See, e.g., 12:35-13:39)

Stambler calls the "joint key" (or "joint code"). The "joint key" is created by coding information relating to the originator and information relating to the payment recipient. (5:3-15.) In the example of FIG. 7, the coded PIN of the originator is coded with the recipient's TIN to produce this joint key. (Id.) The joint key is used by the terminal to code the funds transfer instructions, thereby generating what Mr. Stambler coined "a variable authentication number" or "VAN". (5:9-22.) The VAN is associated with the funds transfer instructions. (5:25-33.) As will be discussed below, the VAN is later used to provide data integrity and data origin authentication.

FIGS. 8A and 8B illustrate redemption of the check created in FIG. 7 through a "network of banks involved in the transaction." (5:55-58.) As illustrated in FIG. 8A, to cash the check the recipient first enters his/her PIN into a bank terminal. (5:62-66.) The PIN is irreversibly coded and then transmitted to the recipient's bank along with information read from the check, including the recipient's TIN. (5:66-6:40.) Using the recipient's TIN, the recipient's bank accesses the recipient's file and uses the recipient's coded PIN to verify the identity of the recipient. (Id.) This is an example of entity authentication. If the incorrect PIN is entered, then "the authentication of the recipient has failed and it is presumed that [the] recipient is not the party presenting the check." (6:38-40.) If the recipient's identity is verified, the recipient's bank transfers the information from the check to the originator's bank. (6:43-45.)

In FIG. 8B, the originator's bank receives the funds transfer instructions and the VAN from the recipient's bank, which is requesting authorization to pay. (6:43-45.) Using the originator's TIN, the bank accesses the originator's file and retrieves information that is used to derive the originator's coded PIN. (6:46-55.) The bank's terminal then generates a joint key by coding the originator's coded PIN (derived by the bank) with the recipient's TIN. (6:66-7:2.)

Having separately generated the "joint key," the originator's bank uncodes the VAN included

with the funds transfer instructions. (7:2-3; FIG. 7, uncoder 58.) The originator's bank then compares the information produced by uncoding the VAN with the received funds transfer instructions. (7:3-11; FIG. 7, comparator 60.) If these values are the same, the funds transfer instructions are accepted as "authentic." (7:16-20.) That is, the funds transfer instructions are presumed to be unaltered (the integrity of the data is authenticated) and to have come from the originator (the origin of the data is authenticated). (Id.) Alternatively, the system authenticating the funds transfer instructions generates a new VAN by coding the funds transfer information with the separately generated joint key. (7:12-15.) This newly generated VAN is compared with the received VAN to authenticate the check. (Id.)

As discussed above, three aspects of authentication are implicated in the systems and methods illustrated by FIGS. 6-8B. Entity authentication is implicated when the check recipient cashes a check in FIG. 8A. The recipient's coded PIN is compared with a coded PIN stored by the bank to verify the recipient's identity. Authentication of data integrity is implicated when the information uncoded from a VAN is compared with received funds transfer information to determine if the information has been changed. And data origin authentication is involved when a VAN is coded or uncoded using the joint key. Because the joint key is created using the originator's coded PIN, a VAN created using the joint key corroborates that the VAN was, in fact, created by the originator.

III. DISPUTED CONSTRUCTIONS[3]

A. "a third party for determining" – '302 Patent, claim 41

Stambler's Construction	Defendants' Construction
a party, other than the first or second parties, that performs the determining step of the claim	a party different from the party or parties performing the other steps of the claim, for determining

Stambler proposes the construction adopted by the Court in the *JPMorgan* case. (Ex. C at

[3] Disputed terms and phrases requiring construction by the Court are highlighted in Exhibit 1. Exhibit 1 also includes those terms that the parties have agreed on.

10.) The construction advocated by Defendants was rejected by the Court. (Id.)

Claim 41 is a method of authenticating the transfer of funds from a "first account associated with a first party" to a "second account associated with a second party." The claim recites "a first party," "a second party," and "a third party," and comprises four steps (highlighted below):

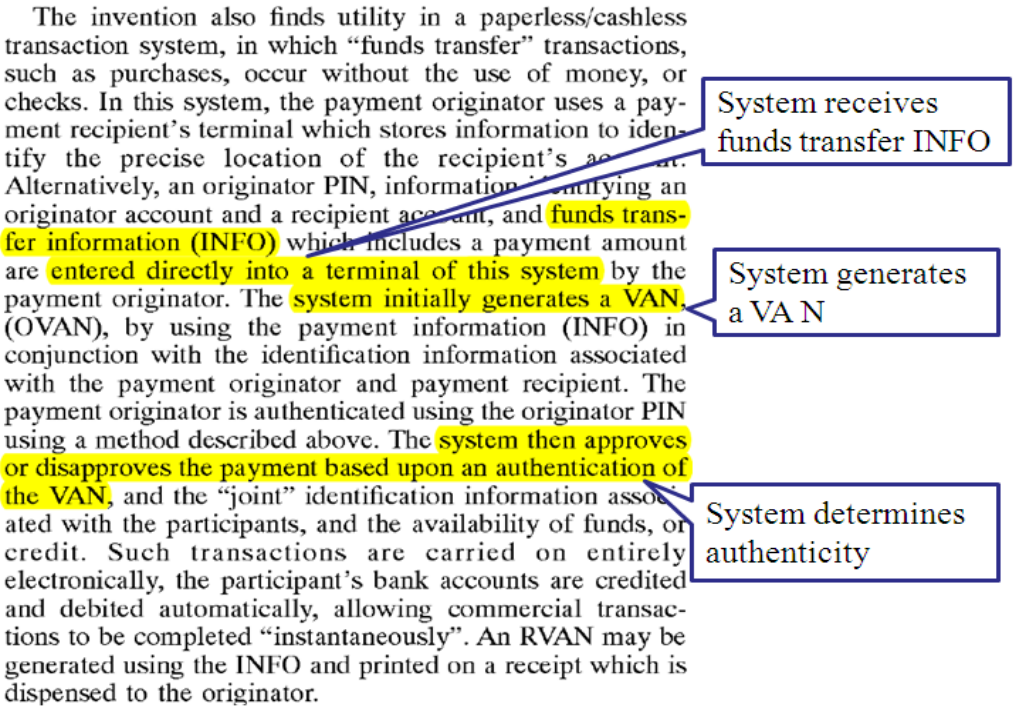
> 41. A method for authenticating the transfer of funds from a first account associated with a first party to a second account associated with a second party . . . the method comprising:
>
> ***receiving*** funds transfer information from the first party, including at least information for identifying the first account of the first party, and information for identifying the second account of the second party…;
>
> ***generating*** a variable authentication number (VAN) using at least a portion of the received funds transfer information;
>
> a third party for ***determining*** whether the at least a portion of the received funds transfer information is authentic by using the VAN; and
>
> ***transferring*** the funds from the first account of the first party to the second account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic. (Ex. A at claim 41.)

The parties agree that the express language of claim 41 requires that the "determining" step be performed by the "third party." But the parties dispute whether claim 41 prohibits the "third party" from performing the "receiving," "generating," and "transferring" steps of the claim. Defendants' proposed construction, which prohibits the "third party" from performing the "receiving," "generating," and "transferring" steps, must be rejected because: (i) it is contradicted by the prosecution history of this specific claim; (ii) it reads out two preferred embodiments; (iii) it runs contrary to the claim language itself; and (iv) it requires a fourth party.

1. The "third party" performs each of the "receiving," "generating," "determining," and "transferring" steps in preferred embodiments.

Defendants' construction is improper because it excludes two preferred embodiments. *See, e.g., Primos, Inc. v. Hunter's Specialities, Inc.*, 451 F.3d 841, 848 (Fed. Cir. 2006) (courts "should not normally interpret a claim to exclude a preferred embodiment"). The prosecution

history expressly cites the "paperless/cashless transaction system" embodiment for support of claim 41 and specifically states that the third party of claim 41 is the disclosed "system." (Ex. G at 54-55.) In the "paperless/cashless" embodiment, the disclosed "system" unquestionably performs each of the "receiving," "generating" and "determining" steps of the claim:



(24:4-29.) Defendants' construction reads out this embodiment because it prohibits the "third party" from performing the "receiving" and "generating" steps of claim 41.

Defendants' construction also excludes the transaction system illustrated in FIGS. 7-8, in which the "third party" performs each of the "receiving," "generating," "determining" and "transferring" steps. In this embodiment, Stambler discloses a system in which an originator (the first party) transfers funds to a recipient (the second party) by way of a check or "an electronic transfer of funds or some other type of electronic transaction." (5:29-31.) When verifying the payment instrument, the originator's bank (the third party) ***receives*** funds transfer information from the recipient's bank. (6:43-45; FIG. 8B.) After receiving this information, the originator's

bank (the third party) uses the funds transfer information to "***generate*** a new VAN":

> 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.

(7:12-15.) After generating the "new VAN," the originator's bank (the third party) then ***determines*** the authenticity of the received funds transfer information by comparing the new VAN with the VAN from the check. (7:12-15.) If the comparison is favorable, the originator's bank (the third party) ***transfers*** funds from the originator's account (the first party's account) to the recipient's account (the second party's account). (7:16-32.) Thus, in this preferred embodiment, the originator's bank (third party) performs each of the "receiving," "generating," "determining," and "transferring" steps of claim 41. Defendants' construction does not read on this embodiment because it precludes the "third party" from performing the "receiving," "generating," and "transferring" steps.

2. The claim language rejects Defendants' construction.

The language of claim 41 requires the "third party" to perform the "determining" step. But the language of claim 41 does not require a particular party to perform the "receiving," "generating," and "transferring" steps. Nor does it preclude a party from performing these steps. It follows that Stambler did not intend to limit performance of the "receiving," "generating," or "transferring" steps to any particular entity. And in light of the above-cited prosecution history and preferred embodiments, it would be improper to adopt Defendants' construction whereby the "third party" cannot perform the "receiving," "generating" and "transferring" steps.

3. The Defendants' construction requires a fourth party.

Under Defendants' construction, the "third party" may perform only the "determining" step of claim 41. In the *JPMorgan* case, the Court found that "[i]f the third party is not permitted to perform any of the other steps, then it becomes clear that some additional party or parties must

perform the receiving and generating steps." (Ex. C at 10.) As a result, the Court correctly determined that Defendants' proposed construction "would require four parties, which is not mandated by the claim language, specification, or prosecution history." (Id.)

B. "variable authentication number (VAN)"

Stambler's Construction	Defendants' Construction
an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both, the number generated by coding information associated with or related to a transaction, document (paper, electronic, or otherwise), or thing with either a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing	a variable number that can be used by a recipient to verify the identity of another who is a party to a transaction and the integrity of information relevant to the transaction, the value generated by coding information relevant to the transaction either with a joint code produced from information associated with the party or directly with information associated with the party

1. Plaintiff's construction is consistent with prior constructions.

In the funds transfer context, a VAN is an encoded variable number used in verifying the integrity and origin of funds transfer instructions (e.g., a check). In the credential issuing and authentication context, a VAN is an encoded variable number used in authenticating a credential, which is presented for purposes of determining identity. Thus, Stambler's proposed construction recognizes that the VAN is "an encoded variable number that can be used in verifying the identity of a party or the integrity of information or both…." This same language was adopted by the Court in the *JPMorgan* case and is consistent with the Delaware court's prior construction.

2. Plaintiff's construction is that given the term by the specification.

All parties' proposed constructions reflect that VAN is a "coined" term with a precise meaning that should be derived from the specification. In Stambler's patents, authentication is achieved through the VAN, which the "Summary of the Invention" describes as a product of coding information with a "joint key" (or "joint code"):

> In accordance with an embodiment of the present invention, when a transaction, document or thing needs to be authenticated, information associated with at least one of the parties involved (e.g., an originator and/or a recipient) is coded 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) or code at the initiation of the transaction.*** (2:9-17.)[4]

And in the embodiment of FIGS. 7-8, Stambler provides an alternate embodiment whereby the VAN is a product of coding funds transfer instructions with information related to one of the parties (without using the "joint key"):

> The data output of coder 28 is a joint key (JK), which is applied as the key input to a coder 30. … 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 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***. (5:9-25.)

All parties' proposed constructions reflect that Stambler's VAN is always created by coding information with either a joint key (or code) or information related to at least one of the involved parties. Accordingly, the Court's construction should reflect that the information to be authenticated is coded "with either a joint key or information associated with or assigned or related to at least one party to the transaction or issuance of the document or thing." (See 2:9-17; 5:9-25; 10:42-45 (assigning a number to a party for use in creating a joint key); 11:15-20 (noting that the VAN / joint key is created using information "***related to***" the parties)).

3. Portions of Defendants' construction must be rejected because they are ambiguous and inconsistent with the specification.

As an initial matter, Defendants' construction should be rejected because it appears to limit the disclosed VAN to use in funds transfers, or "transactions." The patents, however, disclose use of a VAN in other contexts, such as credential issuing and authentication. (11:65-12:2.) The VAN in the credential embodiments can be used, *inter alia*, to verify the integrity of information

[4] The Stambler patents use the terms "joint key" and "joint code" interchangeably. (5:13-15.)

in a credential and to verify the identity of a party. The disclosed credential and the VAN therein are not necessarily used in conjunction with a "transaction," as required by Defendants' construction.

The portion of Defendants' construction that states a VAN is coded "with a joint code produced from information associated with the party or directly with information associated with the party" is also inconsistent with the specification. Specifically, Defendants' construction contradicts the patents' disclosure that a joint key/code is created by coding "information associated with one or more of the parties involved" and that a VAN can be "generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the [joint key]." (2:9-17; 5:22-25.) The specification does not require the VAN to be coded using information related to a particular party (e.g., an originator or a recipient). The patents teach that the VAN may be created using information from either party.

Finally, Defendants' construction injects ambiguity into the claims by including the language "that can be used by a recipient." It is unclear what this language refers to. Is "a recipient" a recipient of an instrument, a party verifying an instrument, the recipient of a credential, or some other party or entity? The Court should reject any construction that leaves such questions open.

C. "secret key of the payor/first party/originator" – '148 Patent, claims 28, 34, and 35

Stambler's Construction	Defendants' Construction
a private key that is created by the payor/first party/originator, or an entity originating an instrument on the payor's/first party's/originator's behalf, by coding information associated with or related to the payor/first party/originator, which is capable of being separately created by a party intended to authenticate the instrument	key that is generated by coding information associated with and known, prior to any coding, only by the payor/first party/originator party for use in any future transactions

The Court rejected Stambler's proposed construction of this claim term in the *JPMorgan* case. Stambler respectfully asks the Court to reconsider its prior construction. Defendants seek a construction that is different than the Court's construction the *JPMorgan* case. (Ex. C at 15.)

The terms "secret key of the payor/first party/originator" appear in claims 28, 34 and 35 of the '148 patent. These claims are "funds transfer" or "payment" methods. (Ex. B at claims 28, 34, and 35.) In each claim, the "secret key" is used to create a VAN. (Id.) For example, claim 34 recites "the VAN being created using at least *a secret key of the first party*." (Id. at claim 34.)

The only cryptographic key that the specification describes using the word "key" and that is used to create the VAN in the funds transfer embodiments is the "joint key," also referred to as a "joint code." (FIGS. 7, 8B, 13D; 5:13-15.) No other "keys" for coding a VAN are disclosed in a funds transfer context. It necessarily follows that the "secret key of the payor/first party/originator" is a specific embodiment of the joint key (or code). The Court should, thus, look to Stambler's disclosure of the joint key to construe the term "secret key of the payor/first party/originator."

1. Stambler's construction is based on the patent's description of "joint key."

Stambler's patents define the joint key (also called "joint code")[5] as a "key" that is created by coding information associated with one or more of the parties, which is capable of being separately created by the party authenticating the instrument. The patents' "Abstract" states:

> 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. … ***During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information***.

The "Summary of the Invention" recites the same definition. (2:9-27.)

The "Detailed Description" also defines the joint key as a key that is created by coding information and that is capable of being separately created by a party intended to authenticate the

[5] (5:13-15) ("the joint key (or code)….")

instrument. Specifically, the joint key of the funds transfer embodiments is created by coding "information associated with ***at least one of the parties involved in the transaction*** (in this case, the originator and recipient)." (5:11-14; FIG. 7; 16:1-6.) An authenticating system later re-creates the joint key in the same manner. (6:66-7:2.) ("In the same manner as coder 28 of FIG. 7, coder 56 therefore produces the joint key JK.")

The specification also explains that creation of the joint key by the payment originator preferably, but not necessarily, takes place at an originator's terminal or computer using information provided by the originator. (4:53-54; FIG. 7.) Consistent with this disclosure, Stambler's construction states that the "secret key" is "created by the payor/first party/originator, or an entity originating an instrument on the payor's/first party's/originator's behalf."

2. <u>The remaining attributes of the "secret key of the payor/first party/originator" are dictated by the claim language.</u>

The specification broadly discloses that the joint key may be created by coding information associated with the payor/first party/originator, the second party/payee/recipient, or both. (5:11-14; FIG. 7.) The claim language "of the payor/first party/originator" specifies that the "secret key" of claims 28, 34, and 35 is created by coding at least information associated with the payor/first party/originator. Accordingly, the proper construction should specify that the "secret key" is created using "information associated with the payor/first party/originator."

Finally, as set forth in claims 28, 34, and 35, the key of the "payor/first party/originator" is "secret." Stambler advocates use of the term "private," which means "designed or intended for one's exclusive use." (See Ex. H at 1442.)

3. <u>Defendants' construction does not read on a preferred embodiment.</u>

The Court should reject Defendants' construction because it is inconsistent with the specification and does not read on at least one preferred embodiment. *See, e.g., Oatey Co. v. IPS*

Corp., 514 F.3d 1271, 1276 (Fed. Cir. 2008) ("We normally do not interpret claims in a way that excludes embodiments disclosed in the specification."). Specifically, the construction includes a limitation that the "secret key" of claims 28, 34, and 35 "is generated by coding information associated with and known, prior to any coding, only by the payor/first party/originator party for use in any future transactions."

In the funds transfer embodiments, the joint key is generated using information known to both the originator and the originator's bank. As illustrated in FIG. 7, the transaction system codes the originator's coded PIN with the check recipient's TIN to produce the joint key. (5:3-10; FIG. 7, element 10, 28.) Defendants' construction, which states the key is created by coding information … known … only by the payor/first party/originator party, must be rejected because the construction ignores the fact that the originator's bank maintains information from which it too can derive the joint key in order to authenticate the instrument.

Moreover, Defendants' construction reads limitations into the claim. The broadly disclosed joint key is created using "information associated with one or more of the parties involved…." (Abstract.) This specific disclosure does not require that the joint key is created using "information associated with and known, prior to any coding, only by the payor…."

D. "credential" – '302 Patent, claims 7, 47, 55

Stambler's Construction	Defendants' Construction
a non-secret document or information obtained from a trusted source that is transferred or presented for purposes of determining the identity of a party	a document or thing obtained from a trusted source that establishes the identity of a party when it is transferred or presented

The parties' dispute centers on how a "credential" is used. Stambler's construction accurately reflects the patents' disclosure of a "credential." This disclosure includes passive instruments such as a driver's license, social security card, and birth certificate. (8:54-58.) These credentials are presented as evidence or proof of identity, and the receiving party or system uses the credential for that purpose. (12:30-34; FIG. 12.) By themselves, credentials such as social

security cards, do not "establish the identity of a party," as required by Defendants' construction. Thus, the term "credential" is a document or information ***used for purposes of*** determining, or confirming, the identity of the party presenting the credential.

Plaintiff asks the Court to reconsider its prior ruling and construe "credential" as "a non-secret document or information.…" In its April 9, 2010 Claim Construction Order, the Court appears to agree that Stambler's "credentials" are not secret. (See Ex. C at 22) ("[A]s used in the patent, a credential is intended to be a document or information presented to another for review. As such, ***it would make sense that the credential cannot be secret***.") (emphasis added). Yet the Court concludes that including the adjective "non-secret" in the construction is unnecessary in light of a limitation found in claim 7 of the '302 Patent, which states that the "credential" includes "non-secret information." (Ex. C at 22.)

However, other claims at issue in this case (specifically, claims 47 and 53 of the '302 Patent) recite a "credential," but ***do not require*** that the "credential" contain "non-secret information." The construction requested by Stambler is ***necessary*** to confirm — as the Court understands — that a "credential cannot be secret." Omitting the term "non-secret" results in an untenable construction because it leaves open the argument that a "credential" could be wholly secret, a concept that runs contrary to the term's explicit use in the Stambler patents.

E. "trusted entity / party" – '302 Patent, claims 7, 47, 53

Stambler's Construction	Defendants' Construction
a party/entity who is trusted or whose integrity is relied on to issue credentials	agency having officially recognized authority to issue credentials

Defendants have asked to construe the terms "trusted party" and "trusted entity." The terms appear in claims 7, 47, and 55, which claim a credential issued by a trusted entity, or party. Stambler's construction is consistent with the meaning given the terms by the patents and the

plain meaning of the terms trusted[6] entity/party.

The Stambler patents broadly disclose systems and methods in which an "official" issues a credential to a "user" after verifying the user's identity. (See, e.g., 11:34-55.) The patents explain that the disclosed systems and methods apply to "all types of credentials," including "all types of identification cards." (8:54-58.) The disclosed concepts are not limited to issuance of particular types of credentials. Mr. Stambler's inventions, thus, find utility not only in the issuance of government identification cards, such as social security cards and passports, but also in the issuance of credentials by non-government entities (for example, employee identification, school identification cards, and other forms of identification).

Stambler's construction of trusted party/entity acknowledges the breadth of the disclosed credential and that the claimed inventions are not restricted to a particular environment. (1:28-32) ("Similarly passports, pay checks, motor vehicle registrations, diplomas, food stamps, wager receipts, medical prescriptions, birth certificates and other official documents are subject to forgery, fraudulent modification.…") A trusted entity is nothing more than a party that is trusted, or relied on, to issue credentials. Nothing in the patents limits the issuance of credentials to an "agency having officially recognized authority to issue credentials," as Defendants suggest.

Comparison of the claimed "trusted party/entity" to claim 11 of the '302 patent confirms Stambler's construction. Claim 11 recites that the party that issues the credential is "an agent, or an agency, or an official of an agency, or an authority, or an administrator, or an entity entrusted with issuing the credential." (Ex. A at claim 11.) In claims 7, 47, and 55, Stambler chose to broadly claim a "trusted entity/party" rather than narrowly claiming an "agency," as recited in claim 11 and proposed by Defendants here. Stambler clearly could have claimed an "agency having officially recognized authority." He did not.

[6] The most common meaning of trusted is "to have or place reliance; depend." (Ex. H at 1920.)

F. "information for identifying the first/second account of the first/second party" – '302 Patent, claim 41

Stambler's Construction	Defendants' Construction
information that is used to identify an account of the first/second party	Information for identifying the first account of the first party: information that is used to identify the first account of the first party from which funds are to be transferred to the second account of the second party Information for identifying the second account of the second party: information that is used to identify the second account of the second party into which funds are to be transferred from the first account of the first party

Stambler proposes the construction that was adopted by the Court in the *JPMorgan* case. (Ex. C at 24.) The parties agree that the disputed language means "information that is used to identify [an account of the first/second party]." The additional language proposed by Defendants – "first account of the first party from which funds are to be transferred to the second account of the second party" and "second account of the second party into which funds are to be transferred from the first account of the first party" – adds nothing to claim 41. In fact, Defendants' proposed language renders meaningless the limitation of claim 41 that recites "transferring funds from the first account of the first party to the second account of the second party."

G. "originator party" / "recipient party" – '148 Patent, claim 35

Stambler's Construction	Defendants' Construction
originator party: plain meaning; alternatively, a party that creates an [instrument for transferring funds]	originator party: party whose funds are being transferred
recipient party: plain meaning; alternatively, the intended recipient of a funds transfer	recipient party: party who receives the funds transfer from the originator party

Defendants have asked for construction of the term "originator party" and "recipient party." Stambler does not believe that either term requires construction. Should the Court elect to construe these terms, the plain language of the claim supports Stambler's construction.

The claim recites that "***an originator party creat[es] an instrument*** for transferring funds." This supports Stambler's alternative construction that the originator is the party that creates the

instrument. The claim further recites that the instrument includes a VAN and "one or more pieces of payment information including an amount, information for identifying the recipient party or the originator party, a date, and a check control or serial number." Notably, the claim does not require that the instrument include information identifying the originator or the originator's account. The claim, thus, contemplates situations where the originator party creates the instrument but is not the party whose funds are being transferred.

The specification also supports Stambler's construction. In describing the embodiment disclosed by Figure 7, the specification states that the "originator generates a check." (4:52.) The patents also describes a multi-party transaction system in which an instrument "is originated by a present party (i.e., the originator) in favor of an absent party (recipient)." (4:67-5:2.)

Additionally, the patents do not limit the originator from creating an instrument that transfers another's funds. In fact, the patents state that that the disclosed inventions are "well suited for generating and processing employee paychecks." (3:66-67.) It is well known that third parties (e.g., ADP) generate paychecks that transfer another party's (e.g., an employer's) funds.

Stambler's construction is also supported by the bill payment embodiment disclosed by the patents. In that embodiment, the party that creates the bill is called the "originator of the bill" and the party that pays the bill is called the "payor." (23:1-11.) This disclosure suggests that Stambler viewed an "originator" as a party or entity that creates something, which is consistent with Stambler's construction in which the "originator party" is a party that creates an instrument.

For these same reasons, Defendants' construction of "recipient" is improper. Specifically, the Defendants' construction requires that the recipient be the "party who receives the funds transfer ***from the originator party***," which is not the case when the originator party transfers another's funds.

H. "first party" / "second party" – '148 Patent, claim 34; '302 Patent, claims 41 and 55

Stambler's Construction	Defendants' Construction
First party: plain meaning; alternatively, claim 34: a party that creates an instrument; claim 41/55: a party identified with a first account Second party: plain meaning; alternatively, claim 34: a party that is intended to receive funds; claims 41/55: a party identified with a second account	First party: party whose funds are being transferred Second party: party who receives the funds transferred from the first party

Defendants have asked to construe the terms "first party" and "second party." Construction is unnecessary because the claims provide the context for determining the role of the first/second party. Moreover, it is improper to construe "first party" or "second party" as having a single meaning because the terms appear in ***numerous*** claims throughout the asserted patents in starkly different contexts. For example, asserted claim 34 of the '148 patent recites "a first party creating an instrument." And asserted claims 41 and 55 of the '302 patent recite an "account associated with a first party." Other claims of the Stambler patents recite "first party" in a context that has nothing to do with transferring funds (e.g., '302 patent, claims 10, 12, 14, 16, 17, 33, 63). Claim 12 recites, for example, "a method for enrolling and issuing a credential to a first party by a second party…." And claim 33 of the '302 patent recites "a method for authenticating a first party by using a credential."

Construction of the terms "first party" and "second party" is unnecessary because the claims define the relationship of the first and second parties to the claimed methods. In claim 34 of the '148 patent, for example, the claim recites that the "first party" creates an instrument for transferring funds. Claim 41 of the '302 patent recites "transferring funds from the first account of the first party to the second account of the second party."

Defendants' proposed constructions should also be rejected because they render meaningless claim limitations. For example, Defendants' proposed constructions for "first party" and "second party" render meaningless the portion of claim 41 of the '302 patent that recites

"transferring funds from the first account of the first party to the second account of the second party."

Further still, Defendants' "one size fits all" construction is inaccurate with respect to many of the asserted claims. For example, Defendants' construction requires that the first party's funds are transferred, yet claim 34 merely recites "a first party creating an instrument for transferring funds to a second party." Nothing in the claims requires that the first party's funds are transferred. As discussed above concerning the term "originator," the specification envisions systems and methods in which a first party creates an instrument for transferring another entity's funds. (See Section II(G).) Regarding claim 41, the claim language merely states that the first party is associated with the first account.

I. "the first/second account information being stored in a first/second storage means" – '302 patent, claim 41

Stambler's Construction	Defendants' Construction
This element is not subject to 35 U.S.C. § 112, ¶ 6. information [associated with] the first/second account being stored in a first/second place for storing information, which can be computer storage Alternatively, if the Court concludes this element is subject to 35 U.S.C. § 112, ¶ 6: Function: storing Structure: documents, files, memory or other computer storage, tables, personal storage media	This term is a means plus function limitation as defined by 35 U.S.C. § 112, ¶ : Function: storing the first/second party's account information. Structure: first/second party's bank's computer

Defendants have asked to construe "the first account information being stored in a first storage means" and "the second account information being stored in a second storage means" and contend that the limitations are means-plus-function limitations governed by 35 U.S.C. § 112, ¶ 6. Notably, neither the defendants nor the court in Delaware suggested that the claimed "first/second storage means" was governed by 35 U.S.C. § 112, ¶ 6. (Ex. D at 7; Ex. I at 79-81.) Likewise, the defendants in the related *JPMorgan* case did not argue that that these limitations

are means-plus-function limitations. Stambler's construction is based on the Delaware court's construction of "first storage means" and "second storage means" – "a first/second place for storing information, which can include a computer file" – and is consistent with the specification and the ordinary meaning of "storage means." (Ex. D at 7.)

1. The disputed phrase is not subject to 35 U.S.C. § 112, ¶ 6.

To construe the disputed claim language, the Court "must decide the subsidiary question of whether the claim element disputed by the parties invokes § 112, ¶ 6." *Rodime PLC v. Seagate Tech., Inc.*, 174 F.3d 1294, 1302 (Fed. Cir. 1999). The Federal Circuit "has consistently held that '[m]eans-plus-function claiming applies only to purely functional limitations that do not provide the structure that performs the recited function.'" *Duratech Indus. Int'l, Inc. v. Bridgeview Mfg., Inc.*, 292 Fed. Appx. 931, 933 (Fed. Cir. 2008). Moreover, when "considering whether a claim term recites sufficient structure to avoid application of § 112, ¶ 6, [the Federal Circuit does] not require[] the claim term to denote a specific structure." *Id.* A claim term avoids § 112, ¶ 6 "if the claim term is used in common parlance or by persons of skill in the pertinent art to designate structure, even if the term covers a broad class of structures …." *Id.*

a. The disputed claim language is not purely functional.

Section 112, ¶ 6 does not apply because the disputed claim language – "the first/second account information being stored in a first/second storage means" – is not purely functional language. *See Rodime*, 174 F.3d at 1302 ("[A] claim element that uses the word 'means' but recites no function corresponding to the means does not invoke § 112, ¶ 6."). Claim 41 does not recite that the claimed "storage means" performs any function.

The disputed claim language should be compared with the claim language in *Motorola, Inc. v. VTech Commc'ns, Inc.*, No. 07-cv-171, 2009 U.S. Dist. LEXIS 59226 (E.D. Tex. July 6,

2009). In *Motorola*, the disputed claim language was "storage means for storing at least one user-programmed call-back number with data defining at least one corresponding user-programmed special audible alert." (Ex. J at claim 1.) The claim at issue in *Motorola* recites classic means-plus-function language. *See Cole v. Kimberly-Clark Corp.*, 102 F.3d 524, 530-31 (Fed. Cir. 1996) (typically, section 112, ¶ 6 is invoked by using the words "means for," followed by a recitation of the function performed). By contrast, claim 41 does not disclose that the "storage means" is "for" performing any function.

b. "storage" had a well-known meaning to those skilled in the art.

The Federal Circuit has refused to apply § 112, ¶ 6 where a claim term has a well-known or well-understood meaning to those skilled in the art. *See Personalized Media Commc'ns LLC v. ITC*, 161 F.3d 696, 704-05 (Fed. Cir. 1998) (finding that "digital detector" could not be construed as means-plus-function limitation; "'detector' is not generic structural term," but rather had "well-known meaning" to those skilled in the art); *Greenberg v. Ethicon Endo-Surgery, Inc.*, 91 F.3d 1580, 1583 (Fed. Cir. 1996) (§ 112, ¶ 6 could not apply to "detent mechanism" simply because claim took its name from function; "detent" had well understood meaning in the art).

By 1992, the term "storage" was well known to those of skill in the art and referred to "any physical device in or on which computer information can be kept." (Ex. K at 330.) Thus, "[u]sed as a noun, 'storage means' identifies a known structure, i.e., a device into which bits of information can be written and later recalled, such as a disk ubiquitously found on a computer system." *Source Search Techs., LLC v. Lending Tree*, LLC, No. 04-4420, 2006 U.S. Dist. LEXIS 79651, at *53-56 (D.N.J. Oct. 16, 2006) (refusing to construe "storage means" as means-plus-function). By 1992, it was well known that various types of physical storage devices could be used to store computer files on a PC or server. In 1992, commonly known and used storage

included various storage media, including hard disks, floppy disks, magneto-optic discs, tape, RAM, ROM, and compact discs, among others. (Ex. K at 72, 149, 168-69, 221, 290, 302, 339.)

2. Defendants' proposed function and structure improperly limit the scope of the claim.

In the event the Court determines that section 112, ¶ 6 governs, construction of the claimed element is a two step process: first, identification of the claimed function; second, to look to the specification and identify the corresponding structure. *Med. Instrumentation & Diagnostics Corp. v. Elekta AB*, 344 F.3d 1205, 1210 (Fed. Cir. 2003). To the extent the Court views this limitation as governed by 35 U.S.C. § 112, ¶ 6, the function is "storing." In means-plus-function claiming, the claimed "means" is modified by language that describes the function performed by the claimed "means" – typically a prepositional phrase beginning with "for." For example, in the *Motorola* case discussed above, the claim language at issue was "storage means for storing at least one user-programmed call-back number …." (Ex. J at claim 1.) In claim 41, the only language that modifies the claimed "means" is "storage." The function performed by the claimed "means" should, therefore, be construed as "storing."

To the extent the Court views this limitation as governed by 35 U.S.C. § 112, ¶ 6, the corresponding structure is "documents, files, memory or other computer storage, tables, personal storage media," each of which the patents disclose as structure for storing information. In the funds transfer embodiments disclosed in connection with Figures 6-8B, for example, account information is stored in a computer file at a bank. (See, e.g., FIG. 6, element 22; FIG. 8A, element 68; FIG. 8B, element 50.) In the funds transfer embodiment of Figures 13A-13E, the patents also disclose tables for storing keys (FIG. 13B, 232) and temporary storage for storing account information (FIB. 13B, 230). And in the paperless/cashless embodiment described at column 24, originator and recipient account information can be stored in a terminal (or

computer) of the recipient or system. (24:7-9.) The patents also disclose storing account information in a credential (Ex. A at claim 50), which can be a document or personal storage media (8:54-60).

Lastly, by construing the corresponding structure as the "first/second party's ***bank's*** computer," Defendants' construction does not read on the "paperless/cashless embodiment" – the very embodiment Stambler cites in the prosecution history as support for this claim. (Ex. G at 54-55.) Specifically, in the "paperless/cashless" embodiment, "a ***payment recipient's terminal*** **…** stores information to identify the precise location of the recipient's account." (24:7-9.) The payment recipient may be the party that is selling a good or service and is certainly not required to be a bank. (24:4-7.) The "paperless/cashless system" embodiment further states that that the funds transfer information may be input "directly into a terminal of this ***system***" which necessarily stores the information prior to "generating a VAN." Nowhere in this embodiment does Stambler describe this "system" as a bank.

J. "error detection code" – '302 Patent, claims 46, 55; '148 Patent, claim 35

Stambler's Construction	Defendants' Construction
the result of applying an algorithm to information in such a manner as to permit detection of changes but without complete recovery of the original information	coded information that is compared by the recipient to detect if there are changes from the information originally encoded into the error detection code

Stambler's construction is that agreed to by the parties in the *JPMorgan* case. (Ex. C at 7.) This construction is substantively identical to the Delaware Court's understanding of the term, which is defined by the patents' specification as the result coding information "in such a manner as to permit detection of changes … but without complete recovery of the original information." (Ex. D at 3; 5:39-44.) Stambler's construction is also consistent with the ordinary meaning of error detection code.[7] Defendants' construction is improper because it imparts unwarranted limitations into the claim that require action by a "recipient" (e.g., "compared by the recipient").

[7] "In codes, a code designed to detect, but not correct, an error in a word or character." (Ex. F at 196.)

K. "coding" – '302 Patent, claims 7, 41

Stambler's Construction	Defendants' Construction
Transforming information by applying a known algorithm	The meaning of "coding" should be supplied within the context of the phrase in which it is used. "Coding" when used in the context of generating a VAN means: "transforming information into a VAN by applying a known algorithm under which the resulting VAN can either be uncoded by reversing the coding operation or compared to a VAN regenerated by applying that same known algorithm to the information." Coding in the context of "creating an error detection code (EDC1) by coding" is a different contextual use of coding.

Stambler's construction is that adopted by the Delaware court and agreed to by the parties in the *JPMorgan* case. (Ex. D at 4; Ex. C at 6.) This construction is based on the patents' broad disclosure of coding. The patents describe coding information using a "coder," which "may be ***any form of such device utilizing a known algorithm***." (3:37-39.) The patents do not limit coding to a particular type or algorithm. Regardless of the context in which the Stambler patents' use the term, "coding" means "transforming information by applying a known algorithm."

Defendants argue that "coding" means different things in different contexts. For example, Defendants argue that "coding," when used in the context of generating a VAN, means "transforming information into a VAN by applying a known algorithm under which the resulting VAN can either be uncoded by reversing the coding operation or compared to a VAN regenerated by applying that same known algorithm to the information." The underlined language describes "coding." The additional limitations describe the result of the claimed coding (a VAN), not "coding." Notwithstanding Stambler's belief that Defendants' characterization of how a VAN is coded is inaccurate, the characteristics of a VAN should not be introduced into the construction of "coding."

The parties' agreed construction of "creating an error detection code by coding" is consistent with Stambler's construction of "coding." It reflects the Delaware court's attempt to harmonize its construction of "coding" with "error detection code." (Ex. D at 3.) The court defined error detection coding as coding in such a manner as to permit detection of changes. (Id.) As a result the court construed "creating an error detection code by coding" as "creating an error detection code by applying an algorithm to information in such a manner as to permit detection of changes but without complete recovery of the original information." (Id.) The underlined language describes "coding." The remaining language describes the result of the coding (an error detection code). (See Ex. F at 196; 3:37-39.)

Finally, it is worth noting that Defendants offer no construction for "coding" as it is used in claim 7 – "coding first information using second information and then coding the result using third information." Stambler's use of the term "coding" in this context is the same as in any other context – "transforming information by applying a known algorithm."

L. "payor" / "payer" – '148 Patent, claim 28

Stambler's Construction	Defendants' Construction
A person or entity who pays, or who is to make a payment. The terms refer to the same party.	Payor: Party paying for or purchasing goods or services Payer: Indefinite

Defendants have asked to construe the terms "payor" and "payer." Stambler's construction for the terms is consistent with the specification[8] and the plain meaning of the terms.[9] Defendants' construction also disregards that a payor/payer may pay for an incurred debt.

The terms appear in claim 28 in the limitation "a payer obtaining a document containing document information, the document information being associated with a debt incurred by the payer or for goods or services to be paid for or purchased by the payor." Stambler's use of the definite article "the" before "payor" indicates that the recited "payor" finds antecedent basis in

[8] The specification describes an embodiment in which a "payor" is a party paying a bill. (23:11-15.)
[9] "Payer, *or* payor. One who pays, or who is to make a payment." (Ex. L at 1129.)

the claimed "payer" and that Stambler intended these terms to refer to the same party.

Defendants' argument that the term "payer" is indefinite should be rejected. Only claims not amenable to construction or insolubly ambiguous are indefinite. *See Bancorp Servs., L.L.C. v. Hartford Life Ins. Co.*, 359 F.3d 1367, 1371 (Fed. Cir. 2004). The parties' agreement in the *JPMorgan* case – that "payor" and "payer" mean the same thing and refer to the same party – is proof that term "payer" is not insolubly ambiguous. (Ex. C at 7.) The only reasonable interpretation of the terms "payor" and "payer" is that the terms mean "a person or entity who pays, or who is to make a payment" and refer to the same party. (Ex. L at 1129.)

M. "previously issued" terms

The term "previously issued" appears in asserted claims 7, 47, and 55 of the '302 patent. Stambler's constructions are based on the Court's construction of "previously issued" in the *JPMorgan* case. There, the Court correctly held that "previously issued" means "issued before the execution of the steps recited in the claim" and that the term does not give rise to an additional claim step. (Ex. C at 24.)

Grammar and syntax can be important in construing claim terms. *See Credle v. Bond*, 25 F.3d 1566, 1571 (Fed. Cir. 1994). The Federal Circuit recognizes that steps of a method claims are most often stated using present participles – verbs ending in "ing." *See id.* at 1572; *Seal-Flex, Inc. v. Athletic Track & Court Const.*, 172 F.3d 836, 849 (Fed. Cir. 1999). Stambler's recitation of method claims is consistent with this accepted practice. And, as is customary in claiming methods, Stambler offsets separate steps using semicolons or the conjunction "and." Moreover, Stambler's claims typically follow the convention of indenting separate claim steps. *See* MPEP § 608.01(i) (7th ed. 1997) ("Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation.") (Ex. N.)

1. "wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity – '302 Patent, claim 7.

Stambler's Construction	Defendants' Construction
This phrase is a limitation but not a step of the claim. wherein a [credential] having non-secret information stored therein is [previously issued] to at least one entity by a [trusted entity]	At least one entity was previously issued a credential having non-secret information by another entity that is considered to be a trusted authority prior to execution of the other steps of the claimed method

Defendants' construction adds no clarity beyond that which will be provided by the Court's construction of "credential," "previously issued," and "trusted entity." Defendants' construction should be rejected to the extent Defendants suggest the disputed limitation is an additional step.

The phrase "wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity" is merely a descriptive phrase that narrows the scope of the claim. As discussed above, Stambler claims the active steps of method claims using present participles. Claim 7 is no different. Stambler recites two active steps: "***coding*** the first information using second information" and "***coding*** the result using third information." The two steps are offset by the conjunction "and."

The phrase "wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity" is a condition that limits the universe of information that is used in the "coding" steps of the claim. After reciting the two "coding" steps, Stambler recites several limitations that limit what information is coded in the coding steps. First, Stambler recites "at least one of the second and third information being associated with at least one entity." Stambler further limits the universe of information that may be used in the coding steps by limiting the "at least one entity," reciting "wherein a credential having non-secret information stored therein is previously issued to at least one entity by a trusted entity." Thus, Stambler's method limits what information is used in the steps of "coding first information

using second information" and "coding the result using third information."

Stambler's construction of the phrase "previously issued" as a condition (and not a step) is also consistent with accepted usage of present and past participles. The present participle, ending in "ing," denotes the verb's action as in progress or incomplete at the time expressed by the sentences principal verb – in this case "coding." (Ex. M at 176.) The past participle denotes the verb's action as complete. (Id.) As does the adverb "previously."

2. '302 Patent, claim 47.

Stambler's Construction	Defendants' Construction
The limitation "at least one party being previously issued a credential by a trusted party" is not a step in the claimed method. The term "previously issued" means "issued before the execution of the steps recited in the claim."	As used in the claims, this means the credential must be issued prior to execution of the other steps of the claim.

Claim 47 depends from claim 41, which recites "receiving," "generating," "determining," and "transferring" steps. Claim 47 limits the method of claim 41 by requiring that at least one party to the funds transfer of claim 41 (e.g., the "first party," "second party," or "third party") was "previously issued a credential." As is customary, the active steps of claim 41 are recited using present participles. These steps are also offsets using semicolons or the conjunction "and."

By contrast, the disputed phrase "at least one party being *previously issued* a credential by a trusted party" is not offset using semicolons and does not use a present participle. For example, the claim does not recite "issuing a credential to at least one party," which would indicate an active step. The claim merely recites "at least one party being ***previously issued*** a credential," indicating that "being ***previously issued*** a credential" is a characteristic of at least one party to the transaction. Defendants' construction, which requires an additional "issuing" step, is a transparent attempt to create a divided infringement issue and must be rejected.

3. "a credential being previously issued to at least one of the parties by a trusted party" – '302 Patent, claim 55.

Stambler's Construction	Defendants' Construction
This phrase is a limitation but not a step of the claim. a [credential] being [previously issued] to at least one of the parties by a [trusted party]	At least one of the first and second parties to the funds transfer must have been issued a credential by another party that is considered to be a trusted party prior to execution of the other steps of the claimed method

Defendants' construction adds no clarity beyond that which will be provided by the Court's construction of "credential," "previously issued," and "trusted entity." Defendants' construction should be rejected to the extent Defendants suggest the disputed limitation is an additional claim step (i.e., "prior to execution of the other steps…").

N. "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN" – '302 Patent, claim 41

Stambler's Construction	Defendants' Construction
using the VAN to determine that the at least a portion of the funds transfer information has not changed and to determine the origin of the at least a portion of the received funds transfer information	[Defendants have indicated that they intend to revise their proposed construction in light of the Court's claim construction order in the *JPMorgan* case. As of filing, Defendants had not yet provided Stambler with their revised proposed construction.]

Stambler's construction harmonizes this claim language with the Court's claim constructions in the *JPMorgan* case. There, the Court held that the VAN in Stambler's funds transfer embodiments can be used to corroborate data integrity and data origin. (See, e.g., Ex. C at 16-19.) It follows that the disputed language "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN" means "using the VAN to determine that the at least a portion of the received funds transfer information has not change and to determine the origin of the at least a portion of the received funds transfer information."

O. "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information" – '302 Patent, claim 55

Stambler's Construction	Defendants' Construction
using the VAN and the credential information to determine that the at least a portion of the funds transfer information has not changed and to determine the origin of the at least a portion of the received funds transfer information	[Defendants have indicated that they intend to revise their proposed construction in light of the Court's claim construction order in the *JPMorgan* case. As of filing, Defendants had not yet provided Stambler with their revised proposed construction.]

In the *JPMorgan* case, the Court held that the VAN in Stambler's funds transfer embodiments can be used to corroborate data integrity and data origin. (See, e.g., Ex. C at 16-19.) It follows that the disputed language "determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information" means "using the VAN to determine that the at least a portion of the received funds transfer information has not change and to determine the origin of the at least a portion of the received funds transfer information."

Dated: May 4, 2010.

Respectfully submitted,

/s/ Brent N. Bumgardner
Texas State Bar No. 00795272
Attorney-in-Charge
Edward R. Nelson, III
Texas State Bar No. 00797142
Christie B. Lindsey
Texas State Bar No. 24041918
Ryan P. Griffin
Texas State Bar No. 24053687
NELSON BUMGARDNER CASTO, P.C.
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107
(817) 377-9111
Fax (817) 377-3485
bbumgardner@nbclaw.net
enelson@nbclaw.net
clindsey@nbclaw.net

rgriffin@nbclaw.net

Eric M. Albritton
Texas State Bar No. 00790215
ALBRITTON LAW FIRM
P.O. Box 2649
Longview, TX 75606
(903) 757-8449
(903) 758-7397 (fax)
ema@emafirm.com

T. John Ward, Jr.
Texas State Bar No. 00794818
WARD & SMITH LAW FIRM
111 W. Tyler Street
Longview, Texas 75601
(903) 757-6400
(903) 757-2323 (fax)
jw@jwfirm.com

Ronald A. Dubner
Texas State Bar No. 06149000
4965 Preston Park, Suite 560
Plano, Texas 75093
(972) 964-6500
(972) 964-6533 (fax)
rondub@gte.com

ATTORNEYS FOR PLAINTIFF LEON STAMBLER

CERTIFICATE OF SERVICE

I hereby certify that on the 4th day of May, 2010, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Eastern District of Texas, Marshall Division, using the electronic case filing system of the court. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

/s/ Brent N. Bumgardner