

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

LEON STAMBLER,)
)
 Plaintiff,)
)
 v.) Civil Action No. 01-0065-SLR
)
 RSA SECURITY, INC., and)
 VERISIGN, INC.)
)
 Defendants.)

Douglas E. Whitney, Esquire and Jack C. Schechter, Esquire of Morris, Nichols, Arsht & Tunnell, Wilmington, Delaware. Counsel for the Plaintiff.

Frederick L. Cottrell, III, Esquire of Richards Layton & Finger, P.A., Wilmington, Delaware. Counsel for Defendant RSA Security Inc. William F. Lee, Esquire, David B. Bassett, Esquire, Donald R. Steinberg, Esquire and Mark D. Selwyn of Hale and Dorr, Boston Massachusetts. Of Counsel.

Steven J. Balick, Esquire and John G. Day, Esquire of Ashby & Geddes, Wilmington, Delaware. Counsel for Defendant Verisign Inc. Thomas W. Winland, Esquire and Vincent P. Kovalick, Esquire of Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, Washington, District of Columbia. Of Counsel.

MEMORANDUM OPINION

Dated: November 14, 2003
Wilmington, Delaware

ROBINSON, Chief Judge

I. INTRODUCTION

On February 2, 2001, plaintiff Leon Stambler filed this action against defendants RSA Security Inc. ("RSA") and VeriSign, Inc. ("VeriSign") for using without a license his patented methods for securing communications.

The plaintiff's patents, each entitled "Method for Securing Information Relevant to a Transaction," generally relate to a method of authenticating a transaction, document or party to the transaction using known encryption techniques. (D.I. 293, 294, 295) The patented methods enable parties to a transaction to assure the identity of an absent party and the accuracy of information involved in the transaction. (Id.) The patented methods thus provide for secure transactions and prevent fraud. (Id.)

Per this court's February 20, 2003 order, the issues of infringement and validity were separately tried. A jury trial was held from February 24 through March 7, 2003 on the issue of patent infringement. The jury found that plaintiff had failed to prove that defendants had induced the infringement of claim 34 of U.S. Patent No. 5,793,302 (the "'302 patent") and claims 1, 16, and 35 of U.S. Patent No. 5,974,148 (the "'148 patent").

At the close of evidence, plaintiff moved for judgment as a matter of law on the issue of inducement of infringement of claim

34 of the '302 patent.

On April 21, 2003, the court entered judgment in favor of plaintiff on the validity of claim 34 of the '302 patent and claim 27 of the '541 patent, and for defendants on the issue of infringement. Currently before the court are plaintiff's post-trial motions for judgment as a matter of law with respect to defendants' inducement of infringement of claim 34 of the '302 patent. (D.I.460) In the alternative, plaintiff moves the court for a new trial. For the reasons stated below, the court will deny plaintiff's motions.

II. BACKGROUND

A. The '302 Patent

The '302 patent issued on August 11, 1998. The named inventor is Leon Stambler. The patent discloses a system for authenticating a transaction, document, or record through the generation of a joint code based upon information associated with at least one of the parties. Claim 34 of the '302 patent is dependent upon claim 33. Claim 33 states the following:

A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a non-secret variable authentication number (VAN) and other non-secret credential information, the method comprising:

previously generating a first error detection code (EDC1) by using at least a portion the other non-secret credential information;

previously coding the first error detection code (EDC1) with first information associated with the second party to derive a variable authentication number (VAN);
previously storing the VAN and the other non-secret credential information in the credential;
retrieving the VAN and the other non-secret credential information stored in the credential;
deriving a second error detection code (EDC2) by using at least a portion of the retrieved other non-secret credential information;
retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties;
uncoding the VAN using the second information associated with the second party to derive a third error detection code (EDC3);
and authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3).

(Col 30. 11.35-65) Claim 34 states that it is a "method of claim 33 wherein the first information associated with the second party comprises a public key, and the second information associated with the second party comprises a non-secret key." (Col. 30, 11.66-67, col.31, 11.1-2)

B. The SSL 3.0 Protocol

Secure Sockets Layer version 3.0 ("SSL 3.0") is widely considered to be the standard method for conducting secured communications via the Internet. (D.I. 443 at 353) The SSL 3.0

protocol addresses two security issues pertaining to Internet communications. First, the protocol insures that parties communicating over the Internet are certain of each other's identity. (D.I. 446 at 1044) Second, the protocol insures that communications between the parties can not be intercepted and deciphered by an unauthorized party.¹ (Id.) SSL 3.0 uses what defendants refer to as the "handshake protocol." (Id.) This protocol may be characterized as having six steps.

In step one, a computer user (the "user") initiates a connection with a website, during which a randomly generated number is sent by the user to the website. (PTX. 323 at 4; D.I. 446 at 1045)

In step two, the website responds by sending a second randomly generated number and the website's digital certificate. (D.I. 446 at 1045) The digital certificate contains information identifying the website (i.e., the website's name, web address), the website's public key,² and a digital signature. (Id. at

¹ To use an analogy, in the absence of a secured communications protocol such as SSL, Internet communications are similar to the "party line" style of telephone communications, as any person could "listen in" on the communications between individuals.

²SSL utilizes a two key asymmetric encryption method, consisting of a public key and a private key. The certificate authority provides to a website both a unique public key and a unique private key. The public key can be widely distributed to users, and permits them to encrypt communications with the website. However, only the website, using its own unique private key, may decrypt communications encrypted with a public key.

1046)

The digital signature is created by a certificate authority through a two-step process that creates a signature unique to each website. First, the website's identifying information and the website's public key are encrypted through a method called error detection coding or "hashing."³ Next the resulting hash code is subjected to asymmetric encryption through application of the certificate authority's private key. (D.I. 444 at 407; D.I. 446 at 1046-47)

In step three, the user applies the certificate authority's public key, which is embedded in the user's browser or software, to decrypt the website's digital signature. By comparing the decrypted digital signature with the other contents of the digital certificate, the user verifies that the digital certificate is authentic.⁴ (D.I. 444 at 409-12; D.I. 447 at

(D.I. 323 at 3)

³Hashing involves applying a mathematical algorithm to a message to be transmitted. (D.I. 443 at 366) The algorithm creates a unique number, known as a hash code, which cannot be decrypted into the original message. This hash code is then transmitted along with the original message to the recipient. The purpose of this hash code is to permit the recipient to determine whether the message it has received has been altered. (Id.) The recipient is able to make this determination, as it can apply the algorithm to the message that it received, and compare it to the hash code accompanying the message.

⁴The user, through applying the certificate authority's public key, obtains the hash code corresponding to the information contained in the digital certificate.

1187-89) At the completion of this step, the user knows that the certificate and corresponding website public key are authentic. The user does not yet know that it has received the certificate from an authentic source.⁵

In step four, the user sends the website a third randomly generated number, which the user has encrypted with the website's public key. (D.I. 446 at 1052)

In step five, the website and the user, using the three randomly generated numbers, independently create a unique set of four keys, known as "session keys." (Id. at 1052) As these session keys are generated based upon the same three random numbers, one of which can only be known by the user and the website, the session keys provide for a unique and secure communication session.

Finally in step six, the website sends the user a message, known as the "finished message," which is encrypted using the session keys, and authenticates the website's identity to the user. (Id. at 1055)

III. STANDARDS OF REVIEW

A. Motion for Judgment as a Matter of Law

To prevail on a renewed motion for judgment as a matter of

⁵In this regard, an analogy can be made to a more common credential such as a driver's license. It is possible to determine that a driver's license is authentic, without also determining that the person carrying that license is a valid possessor thereof.

law following a jury trial, the moving party “‘must show that the jury’s findings, presumed or express, are not supported by substantial evidence or, if they were, that the legal conclusions implied [by] the jury’s verdict cannot in law be supported by those findings.’” Pannu v. Iolab Corp., 155 F.3d 1344, 1348 (Fed. Cir. 1998) (quoting Perkin-Elmer Corp. v. Computervision Corp., 732 F.2d 888, 893 (Fed. Cir. 1984)). “‘Substantial’ evidence is such relevant evidence from the record taken as a whole as might be acceptable by a reasonable mind as adequate to support the finding under review.” Perkin-Elmer Corp., 732 F.2d at 893. In assessing the sufficiency of the evidence, the court must give the non-moving party, “as [the] verdict winner, the benefit of all logical inferences that could be drawn from the evidence presented, resolve all conflicts in the evidence in his favor, and in general, view the record in the light most favorable to him.” Williamson v. Consol. Rail Corp., 926 F.2d 1344, 1348 (3d Cir. 1991); Perkin-Elmer Corp., 732 F.2d at 893. The court may not determine the credibility of the witnesses nor “substitute its choice for that of the jury between conflicting elements of the evidence.” Perkin-Elmer Corp., 732 F.2d at 893. In sum, the court must determine whether the evidence reasonably supports the jury’s verdict. See Dawn Equip. Co. v. Ky. Farms Inc., 140 F.3d 1009, 1014 (Fed. Cir. 1998).

B. Motion for a New Trial

Federal Rule of Civil Procedure 59(a) provides, in pertinent part:

A new trial may be granted to all or any of the parties and on all or part of the issues in an action in which there has been a trial by jury, for any of the reasons for which new trials have heretofore been granted in actions at law in the courts of the United States.

Fed. R. Civ. P. 59(a). The decision to grant or deny a new trial is within the sound discretion of the trial court and, unlike the standard for determining judgment as a matter of law, the court need not view the evidence in the light most favorable to the verdict winner. See Allied Chem. Corp. v. Darflon, Inc., 449 U.S. 33, 36 (1980); Olefins Trading, Inc. v. Han Yang Chem. Corp., 9 F.3d 282 (3d Cir. 1993); LifeScan Inc. v. Home Diagnostics, Inc., 103 F. Supp. 2d 345, 350 (D. Del. 2000), aff'd per curiam, Nos. 00-1485, 00-1486, 2001 WL 345439 (Fed. Cir. Apr. 6, 2001) (citations omitted). Among the most common reasons for granting a new trial are: (1) the jury's verdict is against the clear weight of the evidence, and a new trial must be granted to prevent a miscarriage of justice; (2) newly-discovered evidence exists that would likely alter the outcome of the trial; (3) improper conduct by an attorney or the court unfairly influenced the verdict; or (4) the jury's verdict was facially inconsistent. See Zarow-Smith v. N.J. Transit Rail Operations, 953 F. Supp.

581, 584 (D.N.J. 1997) (citations omitted). The court must proceed cautiously, mindful that it must not substitute its own judgment of the facts and the credibility of the witnesses for those of the jury. The court should grant a new trial on the basis that the verdict was against the weight of the evidence only where a miscarriage of justice would result if the verdict were to stand. See Williamson, 926 F.2d at 1352; EEOC v. Del. Dep't of Health and Soc. Servs., 865 F.2d 1408, 1413 (3d Cir. 1989).

IV. PLAINTIFF'S MOTION FOR JUDGMENT AS A MATTER OF LAW.

A determination of infringement requires a two-step analysis. First, the court must construe the asserted claims so as to ascertain their meaning and scope. Second, the claims as construed are compared to the accused product. See KCJ Corp. v. Kinetic Concepts, Inc., 223 F.3d 1351, 1355 (Fed. Cir. 2000). Claim construction is a question of law while infringement is a question of fact. See id. To establish literal infringement, "every limitation set forth in a claim must be found in an accused product, exactly." Southwall Tech., Inc. v. Cardinal IG Co., 54 F.3d 1570, 1575 (Fed. Cir. 1995).

In order for plaintiff to prove that defendants induced infringement, plaintiff must show that SSL 3.0 literally infringes claim 34. The jury concluded that SSL 3.0 did not literally infringe claim 34 of the '302 patent. In his motion

for judgment as a matter of law for infringement of the '302 patent, plaintiff contends that under this court's claim construction and on the basis of the expert testimony from both sides, all of the limitations of claim 34 are present and no reasonable jury could conclude otherwise.

Defendants respond that the jury did hear evidence with respect to each limitation from which it could conclude that SSL 3.0 did not literally infringe the '302 patent.

Both sides agree that there are only three limitations of claim 34 in dispute. First, whether SSL 3.0 protocol has a "credential" within the meaning of claim 34. (Col. 30, 11.35-41) Second, whether an element of the SSL 3.0's protocol involves "retrieving second information associated with the second party stored in a storage means associated with at least one of the parties." (Col. 30, 11.56-58) Finally, whether an element of the SSL 3.0's protocol involves "authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3)." (Col. 30, 11.62-65)

A. "Credential"

The court construed a "credential" to mean "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party." (D.I. 373 at 6)

Plaintiff contends that the digital certificate employed in the SSL 3.0 protocol is a credential within the meaning of claim 34. Defendants argue that the digital certificate is not a credential because it does not, in the absence of additional steps, authenticate the identity of the sender of the certificate; it only establishes the authenticity of the certificate. (D.I. 448 at 1414-15) Plaintiff contends that defendants' argument conflicts with this court's claim construction as it reads in an additional limitation that the credential must **by itself** establish the identity of a party. (D.I. 461 at 25)

As the meaning of "to establish" was not specifically defined in either the patent itself or the court's claim construction, the jury was to apply an ordinary definition to the term. Hewlett-Packard Co. v. Mustek Systems, Inc. 340 F.3d 1314, 1321 (Fed. Cir. 2003) ("The verdict must be tested by the charge actually given and by giving the ordinary meaning of the language of the jury instruction."). The dictionary defines "establish" to mean: "1. to bring into being on firm or permanent basis; found; ... 3. to cause to be accepted or recognized. 4. to show to be valid or true." Random House Col. Dictionary 452 (revised ed. 1980). The court finds that a reasonable jury could have concluded that the digital certificate is not a credential within the meaning of claim 34, because they could reasonably conclude that the identity of the website is not established in SSL 3.0 at

the time the credential is presented or transferred.

B. "Storage Means Associated with One of the Parties"

Claim 34 requires "retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties," where the "second party" is the certificate authority and the "second information associated with the second party" is the public key. (Col. 30, 11.56-58, 66-67; col. 31, 11.1-2) Defendants dispute that the public key in SSL 3.0, which both parties agree is the "second information associated with the second party," is "stored in a storage means associated with at least one of the parties." The court defined "storage means" as being a "place for storing information, which can be a computer file." (D.I. 373 at 7) The issue between the parties is whether the file on the user's hard drive where the certificate authority's public key is stored is a storage means associated with the certificate authority.

Plaintiff's expert testified that the certificate authority's public key is stored on the user's hard drive and that this location is "associated" with the certificate authority because it is the only thing that resides in that particular location of the user's hard drive. (D.I. 444 at 446) Defendants' expert testified that the user's hard drive where the certificate authority's public key is stored is not associated with either party because there is an absence of control by the

certificate authority over the storage means. (D.I. 447 at 1186-87)

The court finds that defendants' argument to the jury is not in conflict with the claim construction. As the defendants argue, claim 34 requires two associations. First, it requires that there be "second information associated with the second party," meaning the certificate authority's public key; second, there must be a "storage means associated with at least one of the parties." Under plaintiff's broad interpretation, any location where the public key is located is a storage means associated with at least one of the parties. (D.I. 461 at 7). This, however, would make the second clause of this limitation in claim 34 redundant. See Texas Instruments Inc. v. U.S. Intern. Trade Com'n, 988 F.2d 1165, 1171 (Fed. Cir. 1993) ("[T]o construe the claims in the manner suggested ... would read an express limitation out of the claims. This, we will not do because '[c]ourts can neither broaden nor narrow claims to give the patentee something different than what he has set forth.'" (quoting Autogiro Co. of Am. v. United States, 384 F.2d 391, 396, (Ct. Cl. 1967))). The jury, therefore, reasonably could have concluded that to be a "storage means associated with one of the parties," there must be some connection between one of the parties and the storage means, more than the mere presence of the public key.

C. "Authenticating the First Party"

Claim 34 requires "authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3)." The court construed this limitation to mean "verifying the identity of the first party and at least a portion of the non-secret information stored in the credential if EDC2 and EDC3 correspond." (D.I. 373 at 9-10; D.I. 448 at 1463)

The experts agreed that the SSL 3.0 protocol verifies the non-secret information stored in the digital certificate by comparing EDC2 and EDC3. (D.I. 444 at 447-48; D.I. 447 at 1188-89, 1226) The experts also agree that the identity of the website is not verified by virtue of the comparison of EDC2 to EDC3 in SSL 3.0. (D.I. 444 at 414, 590 447-448; D.I. 447 at 1267-68, 1272, 1365) Nonetheless, plaintiff argues that since comparing the EDC2 to the EDC3 is a necessary step to authenticate the website's identity, that the SSL 3.0 protocol infringes. In doing so, plaintiff relies principally on two arguments. First, that defendants have impermissibly read additional limitations into claim 34. Second, that as claim 34 utilizes the "comprising" transitional phrasing, the presence of additional steps does not preclude a finding of infringement.

As the construction of patent claims is a question of law,

it is impermissible for a party in an action for infringement to attempt to avoid liability by arguing the existence of additional claim limitations beyond those construed by the court. See Texas Instruments Inc., 988 F.2d at 1171. In Moba, the Federal Circuit held that a patent on its face, and under the construction given by the district court, did not provide that certain steps in the patented method be sequentially performed. Since the defendants principally relied upon this sequential construction of the claim in their argument to the jury, the court found that no reasonable jury could not have found infringement. Moba, 325 F.3d at 1313-14.

In the present case, defendants did not argue to the jury that an additional limitation should be read into the "authenticating the first party" limitation; instead, they argued that this limitation was simply not met under SSL 3.0. In this case, the jury heard substantial evidence that authentication of the first party did not occur when the EDC2 corresponded to the EDC3. The jury heard substantial evidence that authentication in fact occurred when the "finished message" is sent by the website using the unique session keys. (D.I. 444 at 589; D.I. 486 at 1055)

The use of open style claim construction does not relieve the patent holder from the obligation to show that each limitation of the asserted claim is present in an element of the

alleged infringing product. In the present case, a reasonable jury could conclude that the correspondence between EDC2 and EDC3 does not authenticate the identity of the website.

Having concluded that there was substantial evidence whereby a reasonable jury could conclude that SSL 3.0 does not infringe any of the three contested limitations of claim 34 of the '302 patent, the court will deny plaintiff's motion for judgment as a matter of law.

V. PLAINTIFF'S MOTION FOR A NEW TRIAL

Plaintiff offers two justifications for his motion for a new trial. First, that the verdict of noninfringement as to the '302 patent was against the clear weight of the evidence. Second, that misconduct of the defense counsel improperly influenced the jury.

Plaintiff's brief dedicates only one paragraph to its argument that the jury's verdict was against the clear weight of the evidence. (D.I. 461 at 37) Having already concluded that the jury's verdict was supported by substantial evidence, the court does not find that the evidence supporting the plaintiff's case is so clear that to leave the jury's verdict undisturbed would result in a miscarriage of justice.

Similarly, the court finds that the conduct of defendants' attorneys does not rise to the level of demanding a new trial. A motion for a new trial on the basis of attorney misconduct may

only be granted if the movant demonstrates that such "conduct constitutes misconduct, and not merely aggressive advocacy, and that the misconduct is prejudicial in the sense of affecting a substantial right in the context of the entire trial record." Lucent Techs., Inc. v. Newbridge Networks Corp., 168 F. Supp. 2d 181, 260-61 (D. Del. 2001). In evaluating that misconduct, the court must determine whether the conduct was so prejudicial that it was reasonably probable that the verdict was influenced by the conduct and that a miscarriage of justice would result if the verdict were left undisturbed. See Fineman v. Armstrong World Indus., 980 F.2d 171, 206-07 (3d Cir. 1992). Further, a party may not seek a new trial on the basis of objections not raised in the original trial. See Motorola, Inc. v. Interdigital Tech. Corp., 121 F.3d 1461, 1469 (Fed. Cir. 1997); Caisson Corp. v. Ingersoll-Rand Co., 622 F.2d 672, 681 (3d Cir. 1980); Finch v. Hercules Inc., 941 F. Supp. 1395, 1416 (D. Del. 1996). Consequently, the court will not consider, for purposes of this motion for a new trial, issues not properly preserved by the plaintiff by a contemporaneous objection at trial.

Plaintiff makes numerous contentions with respect to the alleged misconduct of defendants' counsel, including improperly raising issues of patent validity, violating an order of this court, and misstating both the law and claim construction given by this court. Viewing the entire transcripts as a whole, the

conduct of the attorneys in context of the case, and those objections properly preserved by plaintiff's counsel, the court concludes that there was not prejudice to the plaintiff of the quality and quantity that would demand the jury's verdict to be set aside. Consequently, plaintiff's motion for a new trial will be denied.

VI. CONCLUSION

For the reasons stated above, plaintiff's motion for judgment as a matter of law or, in the alternative, for a new trial is denied.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

LEON STAMBLER,)
)
 Plaintiff,)
)
 v.) Civil Action No. 01-0065-SLR
)
 RSA SECURITY, INC., and)
 VERISIGN, INC.)
)
 Defendants.)

O R D E R

At Wilmington this 14th day of November, 2003, consistent with the memorandum opinion issued this same day;

IT IS ORDERED that plaintiff Leon Stambler's motion for judgment as a matter of law, or in the alternative, for a new trial is denied. (D.I. 460)

Sue L. Robinson
United States District Judge