

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

SECURE AXCESS LLC,

Plaintiff,

vs.

BANK OF AMERICA CORP., ET AL.,

Defendants.

§  
§  
§  
§  
§  
§  
§  
§  
§  
§  
§  
§

CASE NO. 6:10-CV-670

MEMORANDUM OPINION AND ORDER

Before the Court is Defendants’<sup>1</sup> Motion for Summary Judgment of Non-Infringement (Docket No. 564) (“Motion”). For the reasons set forth below, the Motion is **DENIED**.

BACKGROUND

There is only one asserted patent in this lawsuit—U.S. Patent No. 7,631,191 (the “’191 Patent” or the “Patent”). The ‘191 Patent relates to a technology for verifying a webpage is from its true source. Docket No. 461 (“Claim Construction Opinion”) at 2. Because fraudulent webpages often appear authentic, it can be difficult for users to determine whether the page they are viewing is genuine. ‘191 Patent, at 1:25–29. The ‘191 Patent addresses this issue. When a user views a webpage originating from a valid source, an “authenticity stamp” is displayed on the page. *Id.* at 2:39–42. Most of the issues presented in this Motion revolve around the authenticity stamp limitation.

An authenticity stamp is “a visual and/or audio indication that the information (e.g., a web page) being presented has been authenticated and is from a valid source.” Claim

---

<sup>1</sup> This order refers to Bank of America, N.A., Arvest Bank, Bank of the Ozarks, Compass Bank, First National Bank Texas, ING Bank, and FSB d/b/a ING Direct USA collectively as “Defendants.”

Construction Opinion at 13. The parties debate the function of the authenticity stamp. Defendants believe the authenticity stamp plays a passive role in confirming the source of a webpage. In their view, the presence of the stamp is binary. If the stamp is displayed, the source is valid; if the stamp is not displayed, the source is not valid. Thus, Defendants believe the stamp cannot be presented to a user unless the source of the page has already been validated. Defendants argue that because their systems do not confirm the source of a webpage before they display the authenticity stamp, their systems do not infringe.

The Plaintiff Secure Axxess LLC (“Secure”) contends the authenticity stamp plays a more active role in confirming the source of a page. According to Secure, the user ultimately validates the source of a webpage when it sees the authenticity stamp. Secure argues the content of the authenticity stamp allows a user to determine whether a source is valid. Thus, an authenticity stamp can be displayed even if the source is fraudulent because the user will know the authenticity stamp is incorrect.

## **APPLICABLE LAW**

### **Summary Judgment Standard**

Summary judgment shall be rendered when the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law. FED. R. CIV. P. 56(c); *Celotex Corp. v. Catrett*, 477 U.S. 317, 323–25 (1986); *Ragas v. Tenn. Gas Pipeline Co.*, 136 F.3d 455, 458 (5th Cir. 1998). An issue of material fact is genuine if the evidence could lead a reasonable jury to find for the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). In determining whether a genuine issue for trial exists, the

court views all inferences drawn from the factual record in the light most favorable to the nonmoving party. *Id.*; *Matsushita Elec. Indus. Co. v. Zenith Radio*, 475 U.S. 574, 587 (1986).

If the moving party has made an initial showing that there is no evidence to support the nonmoving party's case, the party opposing the motion must assert competent summary judgment evidence of the existence of a genuine fact issue. *Matsushita*, 475 U.S. at 586. Mere conclusory allegations, unsubstantiated assertions, improbable inferences, and unsupported speculation are not competent summary judgment evidence. *See Eason v. Thaler*, 73 F.3d 1322, 1325 (5th Cir. 1996); *Forsyth v. Barr*, 19 F.3d 1527, 1533 (5th Cir. 1994). The party opposing summary judgment is required to identify evidence in the record and articulate the manner in which that evidence supports his claim. *Ragas*, 136 F.3d at 458. "Only disputes over facts that might affect the outcome of the suit under the governing laws will properly preclude the entry of summary judgment." *Anderson*, 477 U.S. at 248. Summary judgment must be granted if the nonmoving party fails to make a showing sufficient to establish the existence of an element essential to its case and on which it will bear the burden of proof at trial. *Celotex*, 477 U.S. at 322–23.

### **Infringement Law**

Infringement analysis is "a two-step process in which we first determine the correct claim scope, and then compare the properly construed claim to the accused device to determine whether all of the claim limitations are present either literally or by a substantial equivalent." *Renishaw PLC v. Marposs Societa' Per Azioni*, 158 F.3d 1243, 1247–48 (Fed. Cir. 1998). Claim construction is an issue of law. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970–71 (Fed. Cir. 1995). A determination of infringement, whether literal or under the doctrine of equivalents is a question of fact. *Biovail Corp. Int'l v. Andrx Pharms., Inc.*, 239 F.3d 1297, 1300

(Fed. Cir. 2001). For literal infringement, “every limitation set forth in a claim must be found in an accused product, exactly.” *Southwall Techs., Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1575 (Fed. Cir. 1995). Any deviation from the literal claim language precludes a literal infringement finding. *Telemac Cellular Corp. v. Topp Telecom, Inc.*, 247 F.3d 1316, 1330 (Fed. Cir. 2001).

## ANALYSIS

### “Authenticity Stamp” Limitation

The parties’ dispute regarding this limitation reflects a fundamental disagreement over the scope of the Patent. In particular, the parties debate the level of human involvement dictated by the Claims. Defendants contend the entire process is automated and involves no human interaction. Motion at 14. Under Defendants’ view, the system authenticates that a web page comes from a valid source, then displays an authenticity stamp. *See id.* at 13 (“Conveyance to the user that the web page has been authenticated as being from its true source is accomplished through the *display* of an authenticity stamp.”) (emphasis added). A human user plays a passive role. If an authenticity stamp is displayed, the page came from a valid source—the user is not required to make a determination about the stamp itself. *See id.* Secure’s view requires the user to play a more active role. Secure believes a page can be authenticated even if the source is fraudulent, so a human user must confirm that the authenticity stamp is correct. Docket No. 574 (“Response”) at 6. Secure refers to this last step as the “validating step.” *See id.* Secure argues the authenticity stamp enables a user to visually confirm the page came from a valid source, so user confirmation is inherent within the Claims. *See id.*

Defendants’ non-infringement position is based on their belief that authentication and validation occur simultaneously. Motion at 9. Defendants first argue they do not infringe because SSL authentication does not confirm a source is valid. *Id.* at 12. Under Secure’s infringement

theory, the “authenticity key” is an image tag. *Id.* at 11. The image tag triggers round-trip SSL authentication, which in turn authenticates the webpage. *Id.* However, SSL alone does not authenticate the source of the page. *Id.* at 12. Thus, using SSL authentication, a system may “authenticate” a malicious source. *Id.* Because SSL does not confirm a source is valid, Defendants do not infringe. *Id.*

Defendants’ second argument is based on timing. Under Secure’s infringement theory, the stamp is always presented to a user, even if a page has not been authenticated. *Id.* at 14. However, the Court’s construction states that the authenticity stamp is presented to a user after authentication has occurred. *Id.* at 13. Thus, Defendants contend Secure’s infringement theory is so broad, any use of a SSL communication channel to transfer data would infringe. *Id.*

Secure counters that authentication and validation are two distinct steps. Response at 6. Secure argues authentication is a machine-level process, while validation requires visual human confirmation. *Id.* In support, Secure points to various portions of Dr. Hugh Smith’s<sup>2</sup> expert report and deposition. Dr. Smith testified “validate” means to confirm the authentication step is correct. *See id.* at 13. In Dr. Smith’s view, once the authentication succeeds, the user must visually confirm the authenticated page is valid. *Id.* at 15. The entire purpose of the stamp is to indicate a source is valid. *Id.* The stamp will only be known to the user and the host computer, so a phishing website would not be able to recreate the image. *Id.* at 11. Thus, a user will be able to confirm a page is valid based on the image displayed in the authenticity stamp. *Id.*

Defendants’ argument can be summarized as follows: (1) authentication and validation occur simultaneously; (2) Secure’s infringement contentions rely on SSL protocol to meet the authentication limitation; (3) SSL protocol does not validate a page’s source; (4) Defendants do not infringe because their SSL authentication does not meet the validation limitation. Their

---

<sup>2</sup> Dr. Smith is Secure’s infringement expert. Motion at 5.

position requires the authentication step to confirm a webpage comes from a trusted source. *See* Motion at 12 (“The SSL session key cannot authenticate that the webpage is from a valid source.”). This implicates the parties’ dispute over the level of human interaction required by the Patent.

The Court’s claim construction opinion requires the authentication step to be performed at the machine level. *See* Claim Construction Opinion at 12 (“The authentication process is accomplished by the user’s device (or plug-in software).”). However, there is no discussion about the validation step. *See id.* at 10–13. This leaves open the possibility a human user can validate a source.<sup>3</sup> *Cf.* ‘191 Patent, at 2:51–53 (“The validation is performed using only information that the true owner of the icon can possess.”). Indeed, the Court’s non-acceptance of Defendants’ proposed construction supports this position. At the *Markman* hearing, Defendants argued “authenticity stamp” meant “a visual and/or audio indication that the *user’s device* has authenticated the source of the formatted data.” *See* Claim Construction Opinion at 10 (emphasis added). The actual construction does not include the “user’s device” requirement. *See id.* at 13. Thus, there is no requirement in the Claim Construction that authentication and validation occur simultaneously.<sup>4</sup>

An authenticity stamp may validate a source after machine-level authentication. One way for an authenticity stamp to validate a source is through the stamp’s content. *See* ‘191 Patent, at 1:63–67 (discussing selection of the authenticity stamp). Defendants contend the only way for a

---

<sup>3</sup> The Abstract of the Patent highlights the user interaction embodied in the Claims. It describes “the present invention” as a system “that allows a *user* to validate that current information (e.g., a web page) originates from the true owner of the icon and is not merely a copy.” ‘191 Patent, Abstract (emphasis added).

<sup>4</sup> Defendants contend Dr. Smith contradicted this statement during his deposition. *See* Motion at 10. When asked what authenticate meant, Dr. Smith responded, “The page needs to be authenticated that it is from a valid source.” *Id.* Defendants argue this statement indicates the authentication step includes validation of the source. However, on several other occasions at his deposition, Dr. Smith highlighted his views on the difference between authentication and validation. *See* Response at 13–14. While Defendants are free to cross-examine Dr. Smith about his conflicting statements, a single inconsistent statement in a deposition is insufficient to establish Dr. Smith’s position at the summary judgment stage.

stamp to validate a source is for the stamp to be displayed. However, the Court’s claim construction opinion never requires the *presence* of an authenticity stamp to confirm the validity of a source. Claim Construction Opinion at 10–13. An authenticity stamp is “a visual and/or audio indication that the information (e.g., a web page) being presented has been authenticated and is from a valid source.” *Id.* at 13. More succinctly, a stamp is an “indication that the information...is from a valid source.” *See id.* All the construction requires is for the stamp to indicate the information comes from a valid source. “Indicate” is a broad word, and there are multiple ways for a stamp to indicate a source is valid. One such way is for the stamp to display an image known to the user. *See* ‘191 Patent, at 2:51–53 (“The validation is performed using only information that the true owner of the icon can possess.”).

The flaw in Defendants’ argument is highlighted by viewing the construction from a process verses outcome perspective. The construction of “authenticity stamp” dictates an outcome—the stamp must indicate a source is valid. Claim Construction Opinion at 13. The construction does not dictate the process of how that outcome is reached. *See id.* All that is required is for the stamp to indicate whether a source is valid. The construction places no restrictions on *how* the stamp must indicate a source is valid. In Defendants’ view, the only way an authenticity stamp can confirm a source’s validity is through the actual presentation of the stamp. However, the Claims do not require an authenticity stamp to confirm a source’s validity in a particular way; they only require the stamp to indicate a source is valid. This indication of validity could be the stamp’s presence, but it does not have to be. An indication of validity could also come from the stamp’s content.

Lastly, Defendants argue Secure’s infringement theory is so broad that “the mere use of an SSL communication channel to transfer data would be sufficient to satisfy the authentication

requirements of the invention recited in the asserted claims of the '191 Patent since every SSL communication requires encoding and decoding.” Motion at 14. This argument misses the point because it ignores validation. One of the “authentication requirements of the invention” is that the authenticity stamp indicates information comes “from a valid source.” *See* Claim Construction Opinion at 13. Secure does not argue SSL protocol alone validates the source of information. *See* Response at 8–10. Rather, under Secure’s view, the authenticity stamp will validate after SSL authentication. *See id.* at 10. Thus, regardless of whether all SSL protocol authenticates, a SSL-based system cannot infringe unless it also validates the source of the information.<sup>5</sup>

### **Disavowal of SSL-based Infringement**

Defendants also argue Secure’s infringement theory attempts to capture claim scope disavowed in the Patent. Motion at 15. Under Secure’s infringement theory, the accused systems implement a secure communication channel using SSL protocol to authenticate a webpage. However, Defendants contend the following sentence in the Patent expressly disavows SSL protocol:

Unlike Secure Sockets Layer (SSL) or other “security session” protocols, the present invention validates aspects of the screen display independent of the communications channel between the user and the web site (however, security session protocols may be used in addition to the present invention).

‘191 Patent, at 2:46–51. Additionally, Defendants cite three other passages they believe indicate “that security tools, including SSL, are used in addition to, and are not part of, the authentication process.” Motion at 18; *see id.* at 19 (“Although the specification reveals that the inventors knew

---

<sup>5</sup> Defendants also argue they do not infringe because the authenticity stamp is presented to a user after authentication has occurred. Motion at 14. This does not require a finding of non-infringement; it limits the instances of infringement. The authenticity stamp is presented to a user after authentication has occurred. Claim Construction Opinion at 12. Under Secure’s infringement theory, a user validates a source after the stamp is presented. Because the authenticity stamp must indicate a valid source, only those connections to a valid source would meet the Claims. An authenticated connection to a phishing site would not meet the Claims because there would be no valid source, as required by the authenticity stamp limitation.

about security protocols, the ‘191 Patent never mentions or provides any hint that a security session protocol would be suitable for authenticating a webpage in accordance with the claimed invention.”). Since the Patent teaches away from using SSL to authenticate the source of a page, Defendants contend Secure cannot rely on SSL protocol to prove infringement. *Id.* at 20.

Secure contends the cited passages are meant to illustrate the importance of the authenticity stamp, not to serve as a disclaimer of SSL protocol. Response at 16. Secure argues SSL protocol is independent of the algorithm used to validate a source. *Id.* at 17. Further, Secure asserts that Defendants originally cited to SSL in their invalidity contentions as meeting the authentication requirements of the Claims. *Id.* at 18.

Secure’s SSL-based infringement contentions are entirely consistent with the cited passages. The inventive step embodied in the Patent is the authenticity stamp, not SSL protocol. *See* ‘191 Patent, at 2:39–40 (describing the stamp as “an additional level of functionality”). A user using SSL protocol can access a malicious webpage that appears genuine, so the authenticity stamp is necessary to confirm the source of the information. *See* ‘191 Patent, at 1:34–38. Because each user knows their stamp, a user is able to determine whether the source is genuine. If the stamp matches the user’s stamp, the source is valid. Conversely, if the stamp is incorrect, the source is malicious. The cited passages address SSL protocol to make this distinction. They do not say SSL protocol cannot be used to meet the Claim limitations; they say SSL protocol *alone* does not meet the Claim limitations. *See id.* at 2:46–51 (noting SSL protocols do not validate the source of information).

## **CONCLUSION**

For the foregoing reasons, Defendants’ Motion for Summary Judgment of Non-Infringement (Docket No. 564) is **DENIED**.

**So ORDERED and SIGNED this 26th day of April, 2013.**

A handwritten signature in black ink, appearing to read 'Leonard Davis', written over a horizontal line.

**LEONARD DAVIS  
UNITED STATES DISTRICT JUDGE**