United States Court of Appeals for the Federal Circuit

06-1182

SAFECLICK, LLC,

Plaintiff-Appellant,

v.

VISA INTERNATIONAL SERVICE ASSOCIATION and
VISA U.S.A., INC.,

Defendants-Appellees.

DECIDED: October 23, 2006

Before BRYSON, Circuit Judge, CLEVENGER, Senior Circuit Judge, and GAJARSA, Circuit Judge.

CLEVENGER, Senior Circuit Judge.

Plaintiff-Appellant Safeclick, LLC ("Safeclick") filed this patent infringement suit against Defendants-Appellees Visa International Service Assoc. and Visa USA, Inc. (collectively, "Visa") on December 30, 2003, in the United States District Court for the Northern District of California. Safeclick alleges that Visa's "Verified by Visa" service infringes claims 6 and 7 of U.S. Patent No. 5,793,028 ("the '028 patent"). On July 19, 2005, Visa filed a motion for summary judgment of noninfringement. The motion was granted on December 21, 2005, and judgment was thereafter entered in Visa's favor. Safeclick appeals that judgment. We affirm.

I

The invention of the '028 patent is an "electronic transaction security system . . . designed to substantially prevent the unauthorized use of transaction identification codes such as credit card numbers for placing transaction requests electronically via any suitable communication link, such as the Internet." '028 patent col.1 ll.43-48. So, for example, when a card-holding consumer ("transactionor") wishes to make a purchase over the Internet from an online merchant ("transactionee"), the invention attempts to ensure that the parties to the transaction are who they purport to be.

In order to make a verified purchase using the invention, the transactionor sends a transaction initiation request from his or her computer to a computer operated by the transactionee. Before proceeding further with the transaction, the transactionee's computer requests verification from a computer operated by an entity such as the bank that issued the credit card ("verifier"). The verifier's computer does this by sending an acknowledgement request to the transactionor's computer. In response, the verifier's computer must receive a private identification code that uniquely identifies the transactionor's computer. If the verifier's computer does not receive the code it expects, the transaction will not be verified.

Because claims 6 and 7 of the '028 patent are substantially similar, only claim 6 is reproduced here (with emphasis on the relevant claim limitation):

> 6. A method comprising the steps of:
>
> transmitting a transaction initiation request requesting the initiation of an electronic transaction to a transactionee computer from a transactionor computer, the transaction initiation request including a public identification code uniquely identifying the transactionor computer, and a public identification code uniquely identifying a transactionee computer;

receiving by the transactionee computer the transaction initiation request;

transmitting a verification request requesting verification of the transaction from the transactionee computer to a verifier computer in response to the transactionee computer receiving the transaction initiation request, the verification request including one of a private identification code and a public identification code uniquely identifying the transactionee computer and the public identification code uniquely identifying the transactionor computer;

receiving the verification request by the verifier computer[;]

transmitting an acknowledgement request requesting acknowledgement of the electronic transaction from the verifier computer to the transactionor computer in response to the verifier computer receiving the verification request;

receiving the acknowledgement request by the transactionor computer;

transmitting an acknowledgement response indicating one of a valid electronic transaction and an invalid electronic transaction from the transactionor computer to the verifier computer in response to the transactionor computer receiving the acknowledgement request, the acknowledgement response including the private identification code uniquely identifying the transactionor computer;

receiving the acknowledgement response by the verifier computer;

transmitting a verification response indicating one of a valid electronic transaction and an invalid electronic transaction from the verifier computer to the transactionee computer in response to the verifier computer receiving the acknowledgement response; and

receiving the verification response by the transactionee computer and executing the electronic transaction in response to the transactionee computer receiving the verification response indicating a valid electronic transaction.

'028 patent col.23 l.60 – col.24 l.41 (emphasis added).

II

More than a decade ago, Visa began development of an internet-transaction protocol known as "3-D Secure" and marketed it under the name "Verified by Visa." Like the invention of the '028 patent, Verified by Visa seeks to reduce fraud by verifying the identity of an online consumer who attempts to make a purchase using a registered Visa credit card. The details of Visa's methodology are largely unimportant to the present case. Suffice it to say, a consumer who attempts to make a purchase using the Verified by Visa system must enter a password into his or her computer and send it to the card-issuing bank's "Access Control Server" ("ACS"). Before that password is sent, however, it goes through a process called "Secure Socket Layer" ("SSL") encryption. The SSL protocol enables the two communicating computers to generate a secret key for use during the communication session. If the transmitted information is not encrypted using this key, then the receiver will be unable to decrypt the information. Consequently, the password sent from the consumer to the ACS must be the correct password, and it must have been encrypted using the appropriate key. Upon its receipt of the encrypted password, the ACS decrypts the password and cross references it with the password on file. If the message containing the password cannot be decrypted—indicating a possibility that it may have been changed accidentally or deliberately in transit—or if the decrypted password does not match the one on file, then the transaction will not be verified.

III

In the proceedings below, the district court construed "private identification code uniquely identifying the transactionor computer" as "a nonpublic code that singularly

identifies the computer used by the transactionor, but not only the transactionor himself or herself." Within thirty days after the issuance of that order, Safeclick was permitted, pursuant to the Northern District of California's Patent Local Rules, to serve Visa with its Final Infringement Contentions (to replace its Preliminary Infringement Contentions, discussed infra) in the form of "[a] chart identifying specifically where each element of each asserted claim is found within each Accused Instrumentality." Patent Local Rules 3-1(c) and 3-6(a). Safeclick took advantage of the opportunity and timely served Visa with a chart in which it is asserted that

> The private identification code uniquely identifying the cardholder computer is the authenticating information entered by the cardholder, which includes the cardholder's password, and, in some case[s], a personal identification statement.

(JA at A02948.)

Visa subsequently filed a motion for summary judgment of noninfringement, arguing that there could be no literal infringement because Safeclick had not adduced any evidence that Verified by Visa meets the "private identification code" limitation as construed by the court. Safeclick answered with a detailed explanation of its theory:

> In Verified by Visa, the cardholder enters a password into his or her computer to verify his or her identity. Before the cardholder sends the password, the cardholder computer and issuing bank computer (Access Control Server, or ACS) share a unique cryptographic key. (Tsudik Decl. ¶¶ 10-11) The cardholder computer uses this unique key to scramble, or encrypt, the typed-in password so that only the verifier computer can read the encrypted password. (Id. ¶ 11) This encrypted password is then sent to the ACS for authentication. (Visa Br. 11-12) The Verified by Visa password is a "private identification code" as defined by the Court. It is undisputedly "nonpublic" because it is not known to the merchant, and thus is not known to all of the parties to the transaction. (Tsudik Decl. ¶¶ 13 [sic, ¶]; Dominguez Dep. 133:18-25[;] Mortara Decl. Ex. 5) And this Verified by Visa password singularly identifies the cardholder computer because the ACS cannot successfully process the encrypted data unless it comes from the cardholder computer. (Tsudik Decl. ¶ 11)

(JA at A03395) (footnote omitted). Visa objected to this theory of infringement under Patent Local Rule 3-6(a) because it was, in Visa's opinion, a theory that had not been set forth in Safeclick's Final Infringement Contentions. Specifically, Visa characterized Safeclick's new theory that the encrypted version of the cardholder's password satisfies the "private identification code" limitation as being materially different than Safeclick's previous theory that the plaintext version of the cardholder's password (i.e., the password "entered by the cardholder") satisfies that limitation. Accordingly, Visa, in its reply, urged the court to preclude Safeclick from proceeding with its new theory. Although the court entertained additional briefing on this issue, at no time did Safeclick seek leave to amend its Final Infringement Contentions. See Patent Local Rule 3-7 (permitting amendment for good cause shown).

The district court considered the summary judgment motion on the papers and concluded that Safeclick had in fact violated the local rules by deviating from its Final Infringement Contentions. In the court's view, Safeclick's old theory of infringement only required the password entered by the cardholder to singularly identify the transactionor computer, whereas Safeclick's new theory of infringement requires both the password entered by the cardholder and the encryption information to singularly identify the transactionor computer. In other words, "it is the entry and the sending of [the password] in the manner that Visa has chosen that identifies the cardholder computer." Safeclick, LLC v. Visa U.S.A., Inc., No. C 03-5865, slip op. at 15 (N.D. Cal. Dec. 21, 2005) (emphasis in original). Thus, the district court refused to consider Safeclick's new theory, and summary judgment was granted in Visa's favor. On appeal, Safeclick urges this court to find that the district court abused its discretion.

IV

The Northern District of California, like every other district court, has its own set of local rules for litigants. However, presumably due to the volume of patent cases brought there, the Northern District also has a special set of Patent Local Rules. Pursuant to those rules, a party claiming patent infringement—generally the plaintiff—must provide the following:

> Not later than 10 days after the Initial Case Management Conference, a party claiming patent infringement must serve on all parties a "Disclosure of Asserted Claims and Preliminary Infringement Contentions." Separately for each opposing party, the "Disclosure of Asserted Claims and Preliminary Infringement Contentions" shall contain the following information:
> . . .
> (c) A chart identifying specifically where each element of each asserted claim is found within each Accused Instrumentality, including for each element that such party contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in the Accused Instrumentality that performs the claimed function;
>
> (d) Whether each element of each asserted claim is claimed to be literally present or present under the doctrine of equivalents in the Accused Instrumentality[.]

Patent Local Rule 3-1.

The plaintiff is not locked into these Preliminary Infringement Contentions. The Patent Local Rules allow for amendment in two ways:

> If a party claiming patent infringement believes in good faith that (1) the Court's Claim Construction Ruling or (2) the documents produced pursuant to Patent L.R. 3-4 so requires, not later than 30 days after service by the Court of its Claim Construction Ruling, that party may serve "Final Infringement Contentions" without leave of court that amend its "Preliminary Infringement Contentions" with respect to the information required by Patent L.R. 3-1(c) and (d).

Patent Local Rule 3-6(a).

> Amendment or modification of the Preliminary or Final Infringement Contentions or the Preliminary or Final Invalidity Contentions, other than as expressly permitted in Patent L.R. 3-6, may be made only by order of the Court, which shall be entered only upon a showing of good cause.

Patent Local Rule 3-7.

Our standard of review for a district court's application of such rules is very deferential. In Genentech, Inc. v. Amgen, Inc., we stated:

> "[U]nlike the liberal policy for amending pleadings, the philosophy behind amending claim charts . . . is decidedly conservative and designed to prevent the 'shifting sands' approach to claim construction." Atmel Corp. v. Info. Storage Devices, Inc., 1998 U.S. Dist. LEXIS 17564, 1998 WL 775115, at *2 (N.D. Cal. Nov. 5, 1998). Furthermore, this court defers to the district court when interpreting and enforcing local rules so as not to frustrate local attempts to manage patent cases according to prescribed guidelines. In reviewing a district court's exercise of discretion, this court determines "whether (1) the decision was clearly unreasonable, arbitrary, or fanciful; (2) the decision was based on an erroneous conclusion of law; (3) the court's findings were clearly erroneous; or (4) the record contains no evidence upon which the court rationally could have based its decision." In re Cambridge Biotech Corp., 186 F.3d 1356, 1369, 51 USPQ2d 1321, 1329 (Fed. Cir. 1999). . . . [Even where] the record shows ample reasons for the district court to permit [a party] to amend its claim chart, our standard of review on this issue does not require reversal in the presence of reasons to permit amendments. Even a determination that the district court's ruling was erroneous does not require reversal. Only if the ruling is found to be clearly erroneous is reversal mandated.

Genentech, 289 F.3d 761, 774 (Fed. Cir. 2002).

Safeclick argues that the district court clearly erred in finding that "Safeclick did not disclose the act of 'sending' the password in its Final Infringement Contentions" because the claim language itself provides for the act of "transmitting" the private identification code, and furthermore, because Safeclick explained in its contentions that "the cardholder enters required authentication information and presses the 'Purchase' or similar button in the browser window to transmit that information." Appellant's Br. at 37-38 (emphasis amended).

Safeclick's argument mischaracterizes the district court's reasoning. The act of transmitting (or sending) the information is not the part of the theory that changed after service of the Final Infringement Contentions, but rather it was the content of what gets transmitted (or sent) that changed. Safeclick explained in its Final Infringement Contentions that information entered by the user (e.g., a password) is transmitted. In subsequent briefing, however, Safeclick went beyond the statement in its final contentions. It explained that the private identification code was not merely the password entered by the user but that password as mathematically transformed for transmission by the SSL features of the user's web browser. This new argument had the advantage of indicating how the merchant's computer could in some sense "identify[]" the consumer's computer as required by the claim. When the password is considered outside its SSL wrapping, the only entity identified is the cardholder, not any particular computer. While it might have been reasonable for the district court to interpret Safeclick's latest infringement contentions as a restatement of its earlier infringement contention with a mere change of "scope and clarity," see Orion IP, LLC v. Staples, Inc., 407 F. Supp. 2d 815 (E.D. Tex. Jan. 9, 2006), it was also reasonable for the district court to interpret Safeclick's latest contentions as impermissibly different than its previous contentions. Consequently, we are unable to conclude that the district court erred by adopting one of two reasonable interpretations. See Genentech, 289 F.3d at 774 ("[Even where] the record shows ample reasons for the district court to permit [a party] to amend its claim chart, our standard of review on this issue does not require reversal in the presence of reasons to permit amendments.").

Safeclick argues in the alternative that even if it did violate the Patent Local Rules, "a case-ending sanction is not appropriate when the opposing party suffers no prejudice." Appellant's Br. at 42. According to Safeclick, the Patent Local Rules at issue here are intended to supplement the disclosures required by Fed. R. Civ. P. 26, and because it is impermissible for local rules to conflict with the Federal Rules of Civil Procedure, the district court should have looked to Rule 37—which is the mechanism by which courts enforce Rule 26—for the proper remedy to Safeclick's infraction. Rule 37 provides in relevant part:

> A party that without substantial justification fails to disclose information required by Rule 26(a) or 26(e)(1), or to amend a prior response to discovery as required by Rule 26(e)(2), is not, unless such failure is harmless, permitted to use as evidence at a trial, at a hearing, or on a motion any witness or information not so disclosed.

Fed. R. Civ. P. 37(c)(1) (emphasis added). Had the district court followed the mandates of this rule, Safeclick contends that it would have been able to show that Visa was not prejudiced by Safeclick's failure to disclose its new theory of infringement. As such, the district court would not have struck Safeclick's theory. Safeclick further argues that the district court was required to provide notice that it was considering striking Safeclick's theory altogether.

The court need not address the Rule 37 issue because Safeclick did not present that argument to the district court. Sage Prods., Inc. v. Devon Indus., Inc., 126 F.3d 1420, 1426 (Fed. Cir. 1997) (explaining that "this court does not 'review' that which was not presented to the district court"); Ecological Rights Found. v. Pac. Lumber Co., 230 F.3d 1141, 1154 (9th Cir. 2000) ("It is to assure two-level consideration that issues usually cannot be raised in appellate courts in the first instance, but instead are waived

(or reviewed only for plain error) if not raised before the district court."). To be sure, Safeclick did point out in its sur-reply brief that "Visa does not even allege that it suffered prejudice in this respect." (JA at A04132.) This single sentence simply does not suffice to show that Safeclick raised Rule 37 before this appeal. At best, that sentence was merely a make-weight argument to support the broader argument that Visa was on notice of Safeclick's theory of infringement. Moreover, although we do not decide here whether Safeclick had a duty to seek leave to amend its Final Infringement Contentions pursuant to Patent Local Rule 3-7, we do note that Safeclick's failure to do so was another foregone opportunity make its Rule 37 argument to the district court.

The Ninth Circuit precedent cited by Safeclick stating that purely legal issues may sometimes be considered for the first time on appeal is of no consequence in this case. See, e.g., In re Am. W. Airlines, Inc., 217 F.2d 1161, 1165 (9th Cir. 2000); Bolker v. C.I.R., 760 F.2d 1039, 1042 (9th Cir. 1985). Assuming arguendo that we would abide by our sister circuit's precedent in this context, the question of whether there must be a showing of prejudice (or, to be more precise, a showing of harmlessness) is a factual issue that is not appropriate for us to resolve on appeal. The plain language of Rule 37 requires the district court to first find that the offending party was "without substantial justification" for its noncompliance with the discovery rules. Although Safeclick certainly attempted to shift the blame by arguing that Visa's discovery responses were inadequate (JA at A04132-33), the district court's written opinion is devoid of any findings with regard to substantial justification. Therefore, it would be inappropriate for us to make findings regarding the question of prejudice

(harmlessness) when that highly factual issue has not been presented to, or addressed by, the district court.

As to Safeclick's further argument that the district court should have provided notice that it was considering striking Safeclick's theory altogether, we disagree. Safeclick was provided with notice. On August 26, 2005, Visa argued in its reply brief that the district court should not consider Safeclick's latest infringement contentions for failure to comply with the local rules. Safeclick was then given an opportunity to file a sur-reply brief, which it did on November 8, 2005. Thus, Safeclick's claim that the district court's action was somehow "out of the blue" is demonstrably false.

V

Accordingly, we hold that the district court did not abuse its discretion by refusing to consider Safeclick's new infringement contention. The judgment of the district court is affirmed.