United States Court of Appeals for the Federal Circuit

ADVANCED SOFTWARE DESIGN CORPORATION AND CALIN A. SANDRU,
Plaintiffs-Appellants,

v.

FISERV, INC.,
Defendant/Cross Appellant.

2009-1585, 2010-1011

Appeals from the United States District Court for the Eastern District of Missouri in case No. 07-CV-0185, Judge Catherine D. Perry.

Decided: June 2, 2011

KEITH A. RABENBERG, Senniger Powers LLP, of St. Louis, Missouri, argued for plaintiffs-appellants. With him on the brief was MICHAEL J. HARTLEY.

W. THOMAS MCGOUGH, JR., Reed Smith LLP, of Pittsburgh, Pennsylvania, argued for defendant/cross appellant. With him on the brief were BRIAN D. ROCHE, MICHAEL M. GEOFFREY and MICHAEL P. BREGENZER, of Chicago, Illinois.

Before BRYSON, DYK, and PROST, *Circuit Judges*.

BRYSON, *Circuit Judge*.

Advanced Software Design Corporation appeals from a summary judgment of noninfringement in a patent case on appeal from the United States District Court for the Eastern District of Missouri. The court held that check-security products sold by defendant Fiserv, Inc., did not infringe Advanced Software's patent on a method and system for guarding against check fraud and forgery. Advanced Software also seeks review of a separate claim construction ruling by the district court and of the court's denial of its motion to amend its complaint. Fiserv cross-appeals the district court's denial of its motion for summary judgment of invalidity. We reverse in part and vacate in part on infringement, reverse on claim construction, affirm the denial of Advanced Software's motion to amend its complaint, and dismiss the cross-appeal on invalidity.

I

Advanced Software and Fiserv offer competing products for preventing check fraud and forgery. The products generally work by encrypting selected information on a check, such as the name of the payee or the amount of the check, and printing the encrypted information on the check. When someone attempts to cash a protected check, the products validate the check by decrypting the encrypted information and comparing it to the corresponding unencrypted information that has been entered on the check. If the decrypted information does not match the

selected unencrypted information on the check, the check is deemed fraudulent or forged and will not be cashed.

Advanced Software owns exclusive rights to three patents on check-security technology using "key-based" cryptography. Those three patents stem from the same application and have identical written descriptions. The first of the three, U.S. Patent No. 6,233,340 ("the '340 patent"), contains method claims covering the three steps of encrypting, printing, and validating checks, as well as system claims that cover the components used to print and validate checks. The second patent, U.S. Patent No. 6,549,624 ("the '624 patent") also contains three-step method claims, but the claims cover a different type of validating step. The method of the '624 patent conducts validation by decrypting the encrypted information that is printed on the check and comparing the decrypted information to the selected information that is entered on the check. The method of the '340 patent conducts validation by encrypting selected information that is entered on the check and comparing that encrypted information to the encrypted information previously printed on the check. Thus, the '624 patent compares plaintext (unencrypted information) while the '340 patent compares ciphertext (encrypted information). In addition, the claims of the '624 patent are limited to so-called "public key" encryption schemes, i.e., systems that use two encryption keys, one of which can be made public without practically compromising the security of the other. Advanced Software's third patent is U.S. Patent No. 6,792,110 ("the '110 patent"). The scope of the claims of that patent is the subject of this appeal.

Advanced Software contacted Fiserv in 2002 to complain that Fiserv's check-security product, known as "Secure Seal," infringed Advanced Software's patent

rights. After licensing negotiations failed to resolve the dispute, Advanced Software filed this action in January 2007. Although Advanced Software initially asserted all three of its related patents against Fiserv, it learned that Secure Seal did not compare ciphertext to validate checks and therefore could not infringe the '340 patent. Accordingly, it submitted infringement contentions for only the '624 and '110 patents. After a claim construction hearing, the district court construed terms from those two patents. Shortly after the district court issued its claim construction order, Advanced Software learned that Secure Seal did not use a public key encryption scheme and thus could not infringe the '624 patent. Advanced Software therefore moved to dismiss those infringement claims that were based on the '624 patent.

Advanced Software also moved to amend its complaint to add a claim of unfair competition. Advanced Software alleged that Fiserv had made false statements about the superiority of its encryption scheme and that it had discovered the falsity of Fiserv's representations only during discovery. The court denied Advanced Software's motion on the ground that it came too late and that Advanced Software could have discovered the details regarding the encryption scheme used in Secure Seal much earlier in the discovery process.

The parties filed cross-motions for summary judgment on infringement and invalidity of the asserted claims of the '110 patent. The district court granted Fiserv's noninfringement motion, but it denied Fiserv's invalidity motion on the ground that Advanced Software had pointed to genuine issues of material fact on that issue. The district court then dismissed Fiserv's invalidity counterclaim without prejudice and entered a final judgment of noninfringement.

II

The district court issued summary judgment of noninfringement on two grounds. First, it construed the asserted claims of the '110 patent as requiring all three steps (encrypting, printing, and validating) to be practiced by the accused infringer. Because Fiserv did not direct or control the encrypting or printing steps, the court concluded that there could be no direct infringement under this court's decisions in *BMC Resources, Inc. v. Paymentech, L.P.*, 498 F.3d 1373 (Fed. Cir. 2007), and *Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318 (Fed. Cir. 2008). Second, the district court issued summary judgment rejecting Advanced Software's induced infringement claims because, in its view, Advanced Software had no evidence regarding Fiserv's actual knowledge or state of mind. We reverse on the first ground and vacate on the second ground. We also reject Fiserv's alternative grounds for affirming the judgment of noninfringement.

A

The district court construed the asserted claims of the '110 patent to require that the accused infringer practice all of the steps alluded to in the asserted claims, not just the validation step. Claims 1 and 9 are representative of the asserted claims:

> 1. A process of validating a negotiable financial instrument made by a payor, in which selected information found on the financial instrument which varies for each instantiation of the financial instrument made by the same payor is encrypted in combination with key information not found on the financial instrument to generate a control code which is printed on the financial instrument

along with the selected information, the process comprising:

reading the selected information from the financial instrument; and one of

(i) decrypting the control code to thereby obtain decrypted information whereby the cheque validator may refuse to honour the financial instrument if the selected information found on the financial instrument does not match the decrypted information, and

(ii) re-encrypting the selected information as presented on the financial instrument to re-obtain a second control code, whereby the cheque validator may refuse to honour the financial instrument if the second control code does not match the control code printed on the financial instrument.

9. A system for validating the authenticity of selected information found on a negotiable financial instrument, wherein the selected information varies for each instantiation of the financial instrument presented by the same payor, and wherein the selected information is encrypted in combination with key information not found on the financial instrument to generate a control code which is printed on the financial instrument along with the selected information, the system comprising:

> a scanner for reading the selected information and the control code from the financial instrument;
>
> and a data processing device programmed to
>
> (i) decrypt the control code and generate decrypted information for comparison against the selected information found on the financial instrument and for generating a signal in response to the equality thereof, or,
>
> (ii) re-encrypt the selected information as found on the financial instrument to re-obtain a second control code and for generating a signal in response to the quality of the control code found on the financial instrument against the second control code.

The parties agreed that the preamble's encrypting and printing steps limit the claims. They disagreed, however, on whether the steps must be performed by the accused infringer. Advanced Software contended that the encrypting and printing steps merely describe the environment in which the accused infringer must practice the validating limitation. Fiserv argued that the preamble steps must be performed by the accused infringer. The district court adopted Fiserv's construction based on the view that the preamble steps are necessary to define a structurally complete invention. Because Fiserv does not encrypt or print checks, the district court held that Fiserv could not directly infringe.

In that ruling, the district court did not distinguish between using method claim 1 and system claim 9. *Cf. NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1317 (Fed. Cir. 2005). The district court also did not analyze the difference between making and using a claimed system under 35 U.S.C. § 271(a), a distinction addressed by our recent decision in *Centillion Data Systems, LLC v. Qwest Communications International, Inc.*, 631 F.3d 1279 (Fed. Cir. 2011). Because the district court did not address those issues and the parties do not raise them as grounds for decision of this appeal,[1] we do not address the possible consequences of the distinction between those two types of claims for purposes of this case. We consider only whether Fiserv could "use" the claimed inventions by validating checks with Secure Seal or using a system comprising a scanner and a computer running Secure Seal to validate checks.

Our recent decision in *Uniloc USA, Inc. v. Microsoft Corp.*, 632 F.3d 1292 (Fed. Cir. 2011), helps resolve that question. That case involved a claim to a "remote registration station incorporating remote licensee unique ID generating means, said station forming part of a registration system . . . including local licensee unique ID generating means . . . ." *Id.* at 1297 (emphasis removed). Microsoft argued that it did not directly infringe that

[1] Advanced Software addresses the difference between system and method claims when it argues that system claims cannot be construed to contain steps. We need not resolve that question because we construe the preamble steps of system claim 9 to merely define the financial instrument that the claimed system validates. For infringement purposes, the preamble steps need not be performed by the system or the party that uses the system.

claim because it did not "use" a "local licensee unique ID generating means." *Id.* at 1308. Although its customers used such a means, Microsoft contended that there could be no direct infringement under *BMC* and *Muniauction*. This court disagreed, holding that Uniloc's claim, which recited the "remote registration station incorporating remote licensee unique ID generating means," was directed to the actions of a single party. We held that the remainder of the claim, "said station forming part of a registration system . . . including local licensee unique ID generating means," only "define[d] the environment in which that [remote] registration station must function." *Id.* at 1309.

Like the claim in *Uniloc*, the claims at issue in this case contain preambles that define the environment in which an accused infringer must act or describe capabilities that an accused device must have. Representative claim 1 recites a "process for validating a negotiable financial instrument" comprising reading information from the check and decrypting or re-encrypting to validate the check. Fiserv therefore could "use" the method of claim 1 by validating checks even though it does not encrypt and print them. It would infringe the method of claim 1, however, only by validating checks that have been encrypted and printed in accordance with steps described in the preamble.

Similarly, representative claim 9 recites a "system for validating . . . a negotiable financial instrument . . . comprising: a scanner . . . and a data processing device programmed [to validate by decrypting or re-encrypting]." Although a patented system is "used" when a party "controls the system as a whole and obtains benefit from it," *Centillion*, 631 F.3d at 1285, the system of claim 9 does not include an encrypting computer or printer. Fiserv

therefore could infringe simply by controlling the scanner and the decrypting computer.[2]

Fiserv contends that the analysis in *Uniloc* does not apply to this case because the issue in this case is "whether the preambles . . . include steps to be performed, or whether the preambles merely describe the financial instrument on which the claimed process and system operates." Fiserv argues that the preamble steps in the asserted claim do not "merely describe the financial instrument" because the phrases "in which selected information . . . is encrypted [and then] printed" and "wherein the selected information is encrypted [and then] printed" modify the terms "process" and "system," respectively, not the term "financial instrument."

We disagree with Fiserv's framing of the issue. There is no reason why a preamble cannot describe a financial instrument in terms of the steps required to create it, and that is exactly what the preambles of the asserted claims do. Although the terms "in which" and "wherein" set off the limitations on the claim environments less clearly than the language in *Uniloc*, it remains the case that the asserted claims of the '110 patent recite a process or system for validating checks, not for encrypting and printing them.

Citing our decision in *Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 952 (Fed. Cir. 2006), Fiserv contends that in

---

[2] Because Fiserv allegedly uses the claimed system to validate checks that have been encrypted and printed in accordance with the preamble steps, we do not consider whether Fiserv could infringe by using the claimed system for another purpose. *Cf.* 5 Donald S. Chisum, *Chisum on Patents* § 16.02[4][c] (2010).

construing the claims we cannot consider their purpose. Fiserv relies on a statement from that case that "[p]reamble language that merely states the purpose or intended use of an invention is generally not treated as limiting the scope of the claim." Fiserv's argument misinterprets the meaning of that passage from *Bicon*. Although it is true that preamble language that states the purpose of an invention is generally not regarded as setting forth an additional limitation to a claim, in this case we are not construing the preamble's statement of purpose to add a limitation to the claim. Rather, we are looking to the statement of purpose to distinguish between those limitations that describe the environment in which a claim operates from the limitations that must be performed by an accused infringer.

Fiserv also attempts to support its construction by invoking arguments that bear on whether the preamble to a claim is to be treated as a claim limitation. Specifically, Fiserv contends that the preamble steps provide an antecedent basis for terms in the body of the claims, that dependent claims limit the preamble steps, that the specification describes the "invention" as including the preamble steps, and that the prosecution history shows that the examiner understood the preamble steps to be limiting. None of those arguments are relevant here. Advanced Software agrees that the preamble is limiting, but it argues that the preamble simply defines the environment in which an infringing act must be performed or describes the capabilities an infringing system must have. Fiserv offers no reason why the antecedent basis, dependent claims, specification, or prosecution history would affect Advanced Software's theory that the preamble steps limit only the claimed environment, not the claimed method or system.

Finally, Fiserv contends that, early in the litigation, Advanced Software represented that the claims required the performance of all three steps. Fiserv argues that Advanced Software did not adopt its current position until it filed its reply brief on its motion for summary judgment of infringement before the district court. Such a "last-minute change of position," in Fiserv's view, is "persuasive evidence" that Advanced Software's current position is incorrect. However, Advanced Software's original position was describing the scope of the '624 patent and the '110 patent collectively. Because the claims of the '624 patent covered all three steps, we do not consider Advanced Software's general description of the invention in both the '624 and '110 patent to be persuasive evidence as to whether it regarded the preamble steps in the '110 patent claims as doing more than limiting the environment in which the validating step must be performed or describing the capabilities the validating system must have. Notably, Fiserv does not contend that Advanced Software waived the right to assert its current position. Indeed, Fiserv could not make such an argument, because Advanced Software set forth its position in a timely fashion in response to Fiserv's noninfringement arguments.

B

The district court also entered summary judgment of noninfringement on Advanced Software's theory that Fiserv induced its bank customers to infringe by selling Secure Seal to them. Advanced Software raised that theory of infringement in its complaint, but it did not raise inducement as a theory of infringement when it submitted its infringement contentions in response to the district court's scheduling order. The district court ex-

plained its decision to enter summary judgment on that theory in the following way:

> Advanced Software has presented no evidence and has made no effort to build a case showing Fiserv's actual knowledge or state of mind regarding infringement. Advanced Software did not raise induced infringement in its infringement contentions, and makes only a minimal argument on the subject in its supplemental brief. To allow Advanced Software to change course now and proceed to trial on a completely new theory of infringement would be grossly inequitable.

The district court's decision on the inducement issue appears to be based on two grounds: Advanced Software's failure to raise its inducement theory on a timely basis and the absence of evidence as to Fiserv's state of mind. From the district court's comments on the inducement issue, we are unsure whether the court regarded the two grounds it cited for entering summary judgment—untimeliness and an insufficient evidentiary showing—to be independent grounds for its judgment. As to the latter, however, Advanced Software proffered evidence that Fiserv knew of the '110 patent and instructed its bank customers about how to use Secure Seal to validate checks. That evidence is sufficient to create a genuine issue of material fact as to whether Fiserv had the requisite specific intent to induce infringement. *See DSU Med. Corp. v. JMS Co.*, 471 F.3d 1293, 1305-06 (Fed. Cir. 2006) (en banc).

On appeal, Fiserv does not contend that Advanced Software lacked sufficient evidence as to Fiserv's state of mind. Instead, Fiserv argues that Advanced Software had no evidence of direct infringement by Fiserv's cus-

tomers. Advanced Software, however, offered evidence that Fiserv sold its validating software to banks and helped them install it. The district court did not consider whether that evidence would be sufficient circumstantial evidence of direct infringement, *see Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1318-19 (Fed. Cir. 2009), and we elect not to consider the sufficiency of the evidence for the first time on appeal. Accordingly, we vacate the court's summary judgment ruling on the inducement issue to allow the court to consider the sufficiency of Advanced Software's evidence on direct infringement and address whether summary judgment as to inducement is warranted solely based on Advanced Software's failure to raise that issue on a timely basis.

C

Fiserv contends there are four alternative grounds for affirming the judgment of noninfringement. We find none of them persuasive. First, Fiserv contends that checks protected by Secure Seal lack "control codes" because they contain images of vertical and horizontal lines as opposed to binary strings of 1s and 0s. The district court construed "control code" as the "end product of the encryption process that is then printed on the check." Fiserv argues that Secure Seal images are not the end product of the encryption process because the end product of encryption is "actually a binary string of 1s and 0s." We disagree; the end product of the encryption process is encrypted information or ciphertext, however it may be represented. There is no dispute that Secure Seal images represent ciphertext.

Fiserv also contends that the doctrine of claim differentiation requires a distinction between a "control code" in claim 1 and "machine-readable characters correspond-

ing to the control code" in claim 6. It argues that Secure Seal images are "machine-readable characters," and therefore cannot be the "control code" required in claim 1. The problem with that argument is that Fiserv's proposed example of a "control code," a binary string of 1s and 0s, would still be machine readable through optical character recognition. We therefore conclude that, absent better evidence about the meaning of "machine-readable characters" in the '110 patent, the doctrine of claim differentiation does not shed much light on the meaning of "control code."

Second, Fiserv contends that Secure Seal does not use "key information," because its encryption process does not apply "key information" in the encrypting step. The district court construed "key information" as "a piece of information that is used with a cryptographic algorithm to encrypt and/or decrypt the selected information, whereas the cryptographic algorithm can be widely distributed without compromising security." Advanced Software alleges that Secure Seal uses a "permutation key" that satisfies the "key information" limitation. Fiserv responds that the "permutation key" is not used in the alleged encryption process, which is a "bitwise exclusive-OR ('XOR') operation using a pseudorandom binary keystream." We disagree with Fiserv. Although the permutation key in the Secure Seal system is applied to the selected information before the XOR operation, the permutation key is still information that is "used with" the overall cryptographic algorithm. Advanced Software has therefore provided sufficient evidence to create a genuine issue of material fact as to whether the "permutation key" satisfies the "key information" limitation. Moreover, Fiserv's construction would not read on the preferred embodiment, which does not apply key information in the encrypting step. Instead, the preferred em-

bodiment first concatenates the key information and selected information (i.e., places that information end-to-end) and then encrypts the combination by dividing the concatenated information by a specially chosen polynomial known as a "Chebyshov polynomial." Although Fiserv may ultimately be able to resolve its interpretation of the claim with the preferred embodiment of the '110 patent, it has not presented us with any such resolution, and thus we cannot accept that argument as an alternative ground for affirmance.

Third, Fiserv contends that Secure Seal does not satisfy the encryption limitation because Advanced Software has asserted that Secure Seal's "encryption algorithm supposedly must be kept secret." Fiserv argues that Advanced Software's position conflicts with the construction of "key information," stating that "the cryptographic algorithm can be widely distributed without compromising security." There is at least a genuine issue of material fact as to that issue because Fiserv has repeatedly represented that its encryption algorithm can be widely distributed without compromising security. Fiserv does not even take the opposite position in its brief. Instead, it limits itself to repeating Advanced Software's allegation that the Secure Seal algorithm must be kept secret.

Fourth, Fiserv contends that it does not actually validate checks, because Secure Seal does not provide the functionality necessary to refuse to honor a check. The method of validating in claim 1 recites decrypting the ciphertext on the check "whereby the cheque validator may refuse to honour the financial instrument" if the decrypted information does not match the selected information on the check. The system for validating recited in claim 9 refers to "generating a signal in response to the equality" of selected information and decrypted informa-

tion. Fiserv contends that Secure Seal does not allow its users to refuse to honor a financial instrument and does not generate a signal representing the equality of selected information and decrypted information. Based on the testimony of a Fiserv employee about how the Secure Seal system operates when it is installed in a bank, however, we conclude there is at least a genuine issue of material fact as to that question.

III

Prior to entering summary judgment, the district court construed the phrase "encrypted in combination with key information" in the preamble of the asserted claims to require a two-step encryption algorithm in which (1) selected information from the check is mathematically combined with the encryption key, and (2) that combination is encrypted. Although the court's construction did not play a role in the summary judgment of noninfringement, Advanced Software has raised the issue on appeal, arguing that the court improperly read a limitation from the preferred embodiment into the claims. Fiserv contends that the construction is justified by the claim language, the specification, and the prosecution history. Because this issue may become important during the proceedings on remand, we address it now in the interest of judicial economy.

Before the district court's claim construction, Advanced Software submitted infringement contentions based on the '624 patent and the '110 patent. The claims of those patents use different language with respect to the limitation at issue. The '624 patent recites "encrypting a combination of the selected information and [the key]," while the '110 patent recites "selected information . . . encrypted in combination with key information." Fiserv

asserts that Advanced Software stipulated that those limitations should be construed to have the same meaning despite "minor" differences in language. Advanced Software contends that it did not so stipulate, but instead sought a similar broad construction for both patents. As evidence of the purported stipulation, Fiserv points to the joint claim construction chart. That chart, however, supports Advanced Software's contention that it sought the same broad construction for both patents, not that it agreed that the construction should be the same even if the court adopted a narrow construction for the '624 patent. Because the '624 patent has been dismissed from the case, we do not address the proper construction of that patent's language. Instead, we limit our review to the construction of the phrase "selected information . . . encrypted in combination with key information" in the '110 patent.

We disagree with the district court's construction of that phase. Unlike the '340 and '624 patents, which recite "encrypting a combination of the selected information and [the key]," the '110 patent recites "selected information . . . encrypted in combination with key information." On its face, that phrase means that selected information on the check and key information are combined through the encryption process. Fiserv argues that Advanced Software's construction would read the "in combination" language out of the claim. In other words, Fiserv contends there is no meaningful difference between "selected information . . . encrypted in combination with key information" and "selected information . . . encrypted with key information." We disagree. The "in combination" language is necessary to explain that the selected information and key are combined through the encryption process. Otherwise, the claim would appear to mean that the encryption is performed with the key, not with the

encryption algorithm. A key is a necessary input to the claimed encryption algorithm, but it is not the algorithm itself. For example, the RSA encryption algorithm, referred to in the specification of the '110 patent, encrypts information by mathematically combining plaintext and a public key. The keys can change depending on several factors, but the algorithm remains the same.

Fiserv contends that its proposed two-stage construction is required by the specification, but as support for its construction Fiserv repeatedly cites to language discussing particular preferred embodiments. Fiserv asserts that the language it cites refers to the invention as a whole, not just to preferred embodiments, because the language comes from the Summary of the Invention portion of the '110 patent specification. However, each of the portions of the Summary to which Fiserv refers is from a paragraph that discusses a particular embodiment. *See* '110 patent, col. 3, ll. 45-58; col. 4, ll. 12-20. Those portions of the specification are therefore most naturally interpreted as being limited to embodiments of the invention.

We conclude that the specification supports Advanced Software's construction because it contains language describing an encryption algorithm lacking the first combining step:

> To produce the encrypted control code ("ECC"), an encryption algorithm mathematically combines pre-selected information about the cheque, such as the monetary value of the cheque, with one of more encryption keys. The result of the mathematical operation(s) is the ECC.

'110 patent, col. 6, ll. 20-25. Fiserv contends that the quoted language is not helpful because it does not discuss the "encrypted in combination with" limitation. That argument, however, applies with equal force to Fiserv's specification citations because the phrase "encrypted in combination with" does not appear anywhere in the specification. Nonetheless, the quoted language from the specification supports the broader construction because it specifically describes an encryption algorithm that combines selected information and keys without describing an initial combining step.

Fiserv also contends that the prosecution history of the '340 patent supports the district court's two-step construction of the disputed language. Given the difference in the pertinent claim language, the prosecution history of the '340 patent is of little use in construing the pertinent portion of the '110 patent claims. In any event, Fiserv's characterization of the prosecution history of the '340 patent is not persuasive. Fiserv contends that the examiner's characterization of a prior art patent to Chapman shows that the examiner understood the '340 patent to require a two-step encryption process. That characterization follows:

> Chapman does not explicitly teach encrypting the encryption key along with the selected information A to be printed on the check as a first control code. However, Official Notice can herein be taken that it is very old and very well known in the art of cryptography to utilize an encryption algorithm in which the encryption "key" is incorporated into the end result of the algorithm. It is very old and very well known in the art as well, to utilize a (practicably) irreversible encryption algorithm

> which operates on inputted data and a 'key' so as to produce such a result.

Fiserv emphasizes the first sentence of that passage, contending that "encrypting the encryption key along with the selected information" describes the two-step process of first combining the encryption key and selected information and then encrypting the combination. However, we see no reason why that phrase must be interpreted as describing the two-step process. In fact, after describing the limitation that is missing from Chapman, the examiner observed that the limitation was well-known in the field because encryption algorithms existed "in which the encryption 'key' is incorporated into the end result of the algorithm." Advanced Software's proposed construction would still require the key to be incorporated into the end result of the algorithm. It just would not require that the combination occur prior to encryption. We therefore construe "selected information . . . encrypted in combination with key information" to mean that the encryption algorithm combines the selected information and the key information to create the control code.

IV

Advanced Software also appeals the district court's denial of its motion to amend its complaint to add a Lanham Act count for false advertising. Before litigation, Fiserv had allegedly represented to the banking industry that Secure Seal used two distinct encryption algorithms, one of which used public keys. Advanced Software sought Fiserv's source code during discovery, but it did not obtain the complete source code until October 2008. On January 8, 2009, after attorney discussions about the source code, Fiserv changed its representation to declare that Secure Seal used only one encryption algorithm that did not use

changeable public keys. A little more than a month after that change in Fiserv's position, Advanced Software moved to amend the pleadings to assert a Lanham Act claim based on Fiserv's advertisements, which stated that Secure Seal was more secure than other barcode systems (such as Advanced Software's system). The district court denied the motion because the deadline for amendments under the court's initial case management order had passed and, in the court's view, Advanced Software had not provided any "legitimate reason" for the delay.

We review the denial of a motion to amend by applying regional circuit law. *Kalman v. Berlyn Corp.*, 914 F.2d 1473, 1480 (Fed. Cir. 1990). The Eighth Circuit reviews the denial of such a motion for an abuse of discretion. *O'Neil v. Simplicity, Inc.*, 574 F.3d 501, 505 (8th Cir. 2009). "An abuse of discretion occurs where the district court fails to consider an important factor, gives significant weight to an irrelevant or improper factor, or commits a clear error of judgment in weighing those factors." *Gen. Motors Corp. v. Harry Brown's, LLC*, 563 F.3d 312, 316 (8th Cir. 2009).

The parties disagree about which standard the district court should have applied in evaluating the motion. Advanced Software contends that the motion to amend should have been evaluated under the liberal standard of Federal Rule of Civil Procedure 15(a)(2). Fiserv contends that Rule 15(a)(2) does not govern because the motion to amend was filed after the deadline set by the district court. Accordingly, Fiserv argues that the more stringent "good cause" standard of Rule 16(b) applies to this case. *See Sherman v. Winco Fireworks, Inc.*, 532 F.3d 709, 716 (8th Cir. 2008).

Advanced Software contends that its motion to amend did not violate the district court's scheduling order because that order was limited to jurisdictional issues involving the Federal Reserve banks that were previously named as defendants in the case.[3] The district court disagreed with that characterization of its scheduling order. The court explained that although the "order related mainly to jurisdictional issues, it also adopted the parties' proposal for a deadline for amendment of pleadings apart from the jurisdictional dispute." That interpretation of the order is not inconsistent with the language of the order; some of the scheduling directives in the order were explicitly limited to jurisdictional issues, while other directives (including the directive setting forth the deadline for amendment of pleadings) lacked an explicit limitation. Because the district court's interpretation of its own orders is reviewable only for abuse of discretion, *In re Dial Bus. Forms, Inc.*, 341 F.3d 738, 744 (8th Cir. 2003), we adopt the district court's interpretation and therefore conclude that the good cause standard of Rule 16(b) governs the district court's denial of Advanced Software's motion to amend.

Under the good cause standard, the threshold inquiry is whether the movant has been diligent. *See Sherman*, 532 F.3d at 717. The district court found that Advanced Software unduly delayed seeking to amend because it "had ample time to conduct discovery and to have [its] experts analyze defendant's product." Advanced Software contends that it was not aware that Secure Seal lacked public key encryption until Fiserv's attorney so admitted on January 8, 2009. At that point, Advanced Software

[3] The district court dismissed the Federal Reserve banks under 28 U.S.C. § 1498(a).

had had access to the source code for only about four months. Nonetheless, Advanced Software does not explain what occurred during that four-month period that the district court focused on. We therefore cannot conclude that district court abused its discretion by failing to consider an important factor, or that the court committed a clear error of judgment in determining that Advanced Software had not shown good cause for that four-month delay. Accordingly, we affirm the district court's denial of Advanced Software's motion to amend.

V

Fiserv has filed a cross-appeal challenging the district court's denial of its summary judgment motion on obviousness and anticipation (but not the court's order of dismissal of its invalidity counterclaim without prejudice). We lack jurisdiction over the cross-appeal because "[t]he final judgment rule prohibits a party from appealing a district court's denial of a motion for summary judgment." *Lermer Germany GmbH v. Lermer Corp.*, 94 F.3d 1575, 1576 (Fed. Cir. 1996). The Supreme Court has explained that appellate courts lack jurisdiction over the denial of a motion for a summary judgment based on disputed issues of fact because such a denial "does not settle or even tentatively decide anything about the merits of the claim." *Switz. Cheese Ass'n, Inc. v. E. Horne's Mkt., Inc.*, 385 U.S. 23, 25 (1966). Because there has been no final determination on the merits of Fiserv's invalidity counterclaim, we have no jurisdiction to address that claim.

Each party shall bear its own costs for this appeal.

AFFIRMED IN PART, REVERSED IN PART, VACATED IN PART, DISMISSED IN PART AND REMANDED