United States District Court,
E.D. Missouri, Eastern Division.

ADVANCED SOFTWARE DESIGN CORPORATION, et al,
Plaintiffs.
v.
FISERV, INC,
Defendant.

Case No. 4:07CV185 CDP

Dec. 23, 2008.

Background: Owner of patents for apparatus and method for enhancing the security of negotiable instruments brought infringement action. Parties sought claim construction.

Holdings: The District Court, Catherine D. Perry, J., held that:
(1) terms "encrypt in combination with" and "encrypt a combination of" meant performing mathematical operations of an algorithm which combines "selected information" and one or more of the specified "keys" and generates a control code by encrypting the combined "selected information" and "key" or "key information";
(2) terms "encrypted" or "encrypting" meant applying a known cryptographic scheme or algorithm to obtain a control code;
(3) terms "key information," "key," "keys," and "encryption keys," meant 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; and
(4) term "varies for each instantiation" meant variable and generally not common to all checks issued by the same payor, but not necessarily distinct and unique to every check.

Claims construed.

6,549,624, 6,792,110. Construed.

Keith A. Rabenberg, Michael J. Hartley, Sara Weilert Gillette, Senniger Powers, St. Louis, MO, for Plaintiffs.

Anthony S. Baish, William E. Duffin, William H. Levit, Jr., Godfrey and Kahn, S.C., Milwaukee, WI, Brian D. Roche, Michael P. Bregenzer, Michael M. Geoffrey, Raven Moore, Reed Smith LLP, Chicago, IL, John H. Quinn, III, Michael H. Longmeyer, Nicholas B. Clifford, Jr., Armstrong Teasdale, LLP, Martin M. Green, Green and Jacobson, P.C., St. Louis, MO, for Defendant.

MEMORANDUM OPINION

CATHERINE D. PERRY, **District Judge.**

Plaintiffs Advanced Software and Calin Sandru hold two patents, Nos. 6,549,624 and 6,792,110, that cover an "apparatus and method for enhancing the security of negotiable instruments." Plaintiffs claim that defendant Fiserv, Inc. is infringing both patents. The parties dispute numerous claim terms, and have presented arguments on claim construction during a two-day Markman hearing. This order resolves some of the issues relating to some of the claim terms. Disputes over claim terms not addressed in this order will be resolved at a later stage, either through summary judgment motions or rulings on proposed jury instructions.

I. *Legal standards governing claim construction*

[1] [2] [3] Claim construction is a matter of law. Markman v. Westview Instruments, Inc., 517 U.S. 370, 388-89, 116 S.Ct. 1384, 134 L.Ed.2d 577 (1996). In construing a claim, a court looks first to the intrinsic evidence of record, that is, the claim's language, the specification and the prosecution history. Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582(Fed.Cir.1996). Intrinsic evidence is "the most significant source of the legally operative meaning of disputed claim language." Id.

[4] [5] [6] Within the realm of intrinsic evidence, the appropriate starting point in construing patent claims is always the claim language itself. Comark Communications, Inc. v. Harris Corp., 156 F.3d 1182, 1186 (Fed.Cir.1998). The words of a claim are generally given "their ordinary and customary meaning," Vitronics Corp., 90 F.3d at 1582, which is "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." Phillips v. AWH Corp., 415 F.3d 1303, 1313 (Fed.Cir.2005) (citation omitted). A person of ordinary skill in the art reads the claim term "not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." Id.

[7] [8] A patentee may assign a special definition to a word, so long as that definition is clearly stated in the patent specification or prosecution history. Vitronics Corp., 90 F.3d at 1582. To determine whether a patentee has used any terms in a manner inconsistent with their ordinary meaning, a court must review the specification, which is usually "dispositive" and always "highly relevant" to the claim construction analysis. Id. The Federal Circuit has noted that it is "entirely appropriate for a court ... to rely heavily on the written description for guidance as to the meaning of the claims." Phillips, 415 F.3d at 1317. In Phillips, the court cautioned against elevating dictionary definitions above the express or implied definitions of claim terms found in the specification. FN1 Id. at 1320-22.

FN1. The Phillips Court specifically rejected the approach endorsed by the Federal Circuit in Texas Digital Sys. v. Telegenix, Inc., 308 F.3d 1193, 1202 (Fed.Cir.2002). In Texas Digital, the court limited the role of the specification in claim construction to serving as a check on the dictionary meaning of a claim term if the specification requires the court to conclude that fewer than all the dictionary definitions apply, or if the specification contains a specific alternative definition or disavowal. Id. at 1202. In Phillips, the court held that the Texas Digital approach improperly restricted the role of the specification by essentially elevating abstract definitions over the contextual use of the terms. 415 F.3d at 1320-21.

[9] Although claim terms are to be interpreted in light of the specification and with a view to ascertaining

the invention, "it does not follow that limitations from the specification may be read into the claims." Comark, 156 F.3d at 1186 (quoting Sjolund v. Musland, 847 F.2d 1573, 1581 (Fed.Cir.1988)). The Federal Circuit has recognized that there sometimes is a "fine line between reading a claim in light of the specification, and reading a limitation into the claim from the specification." Comark, 156 F.3d at 1186. Where a term is "not so amorphous that one of skill in the art can only reconcile the claim language with the inventor's disclosure by recourse to the specification," reading a limitation from the specification into the terms is inappropriate. Id. at 1187. *See also* E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co., 849 F.2d 1430, 1433 (Fed.Cir.1988) (stating that the specification can supply understanding of unclear terms, but should never trump the clear meaning of the claim terms).

[10] [11] A court may also consider the patent's prosecution history, which contains "the complete record of all the proceedings before the Patent and Trademark Office, including any express representations made by the applicant regarding the scope of the claims." *Id.* Indeed, the prosecution history is "of primary significance in understanding the claims." Markman, 52 F.3d at 980. Although the prosecution history is always relevant to claim construction, it cannot be used to infer the intentional narrowing of a claim term, unless there has been a "clear disavowal" of the claim coverage. Amgen, Inc. v. Hoechst Marion Roussel, Inc., 314 F.3d 1313, 1327 (Fed.Cir.2003). An example of such disavowal is when the applicant amends a claim to overcome a rejection by the Examiner. Id.

[12] [13] Extrinsic evidence, i.e., evidence that is external to the patent and prosecution history, is not to be consulted when the intrinsic evidence is unequivocal. Bell & Howell Document Mgmt. Prods. Co. v. Altek Sys., 132 F.3d 701, 706 (Fed.Cir.1997); Vitronics Corp., 90 F.3d at 1583 ("[W]here the public record unambiguously describes the scope of the patented invention, reliance on any extrinsic evidence is improper."). It is appropriate, however, "for a court to consult trustworthy extrinsic evidence to ensure that the claim construction ... is not inconsistent with clearly expressed, plainly apposite and widely held understandings in the pertinent technical field." Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1308 (Fed.Cir.1999). In the end, "extrinsic evidence may be useful to the court, but it is unlikely to result in a reliable interpretation of patent claim scope unless considered in the context of the intrinsic evidence." Phillips, 415 F.3d at 1319.

II. *The invention*

The invention disclosed in the '624 and '110 patents is an apparatus and method for enhancing the security of checks. The invention works by applying principles of cryptography-a branch of mathematics that deals with encoding and decoding written information. The invention calls for a bar code or other machine-readable item to be printed on the check face to authenticate that the check has not been altered or forged. According to the claim terms, the invention can work in one of two ways.

The first way in which the invention can work involves using what is known in the art as a "public key encryption scheme." In this method, check information, for example the dollar amount, is taken from the check face and encrypted using a known cryptographic algorithm. The encryption process generates a "control code" that is then printed on the check. The control code can only be read and understood by someone with the means to decode it. A check authenticator such as a bank takes the control code, decodes it, and then compares the result to the dollar amount printed on the check. If the two numbers match, the check is validated. If the numbers do not match, the check is invalid and will not be honored.

The second scheme disclosed by the patent does not use a decoding step. Rather, it works by doing the encoding step twice. This scheme is referred to generally as a "private key" encryption scheme. As with a public key scheme, check information is encoded, and a control code is printed on the check. However, the mathematics of this private key scheme are such that the encoding process is not reversible. There is no way to "get back" the original message using the control code, because the control code cannot be decoded. Therefore, in order to authenticate the check, a validator must read the dollar amount off the check face and re-encrypt it to generate a second control code. The second control code is then compared to the first control code. The check is authentic only if the two control codes match.

In both the public key scheme and the private key scheme, the mathematics that drive the algorithms are widely known. There is nothing "secret" or proprietary about how the math converts check information into a control code. The security of both systems rests instead on the use of keys-mathematical figures that are entered into a widely-known algorithm.

In the case of the public key scheme, two keys are used-one for encryption and one for decryption. A particular public key scheme that is known in the art and is discussed in the patent is the RSA FN2 scheme. In RSA, the encryption and decryption keys are two numbers in a specific mathematical relationship. The two numeric keys work as exponents. To encrypt a certain numeric message, the sender would raise that number to a power using the encryption exponent. To decrypt the message, the receiver would take the received code and raise it to a power using the decryption exponent.FN3 RSA works as a cryptographic scheme because the two exponents cannot be easily derived from one another. That is, if a particular person knows the encryption exponent, he or she cannot thereby use that information to figure out the decryption exponent, or vice versa. This system is called a "public key" system because one key can be made public without compromising the secrecy of the remaining key.

FN2. RSA is a public key cryptography scheme proposed in 1977 and named for the mathematicians who proposed it, Rivest, Shamir, and Adleman. D.R. Hankerson, *et al.,* Coding Theory and Cryptography 284 (2d ed. 2000).

FN3. This is an oversimplification of the RSA scheme. In practice the exponentiation occurs over a particular modulus. The security of RSA rests on the theory that factoring a particularly large modulus is believed to be an intractable problem. *See generally* Hankerson, *et al., supra* note 3, at 284-85.

Conversely, in the private key scheme, any key or keys must be kept secret if the scheme is to remain secure. The preferred embodiment disclosed in the specification discusses a private key scheme modeled after an algorithm known in the art as a Cycle Redundancy Check (CRC). In this scheme, the numeric information to be encoded is concatenated (placed end to end) in a string with two private keys and a third key that is derived from the other two. This long string is then divided by a large polynomial. As with normal long division, the result of this dividing step is a quotient and a remainder. The quotient is then discarded, and the remainder becomes the control code.FN4 The keys that are concatenated with the original information are never disclosed to the public. Like the RSA scheme, the CRC is a widely known method for authenticating data. The keys are what makes the scheme unique to a particular user.

FN4. This shows why the private key scheme disclosed in the specification of the patents is irreversible. Where the control code is simply the remainder of a division problem, retrieving the original dividend is not possible unless both the quotient and the remainder are known. For example if a number is divided by 5 and the remainder is 2, the original number could be 12, 17, or infinitely more possibilities.

Taken as a whole, Sandru's patents disclose an invention that uses known public and private key cryptographic schemes to authenticate checks. In prosecuting his patent before the Patent and Trademark Office, Sandru distinguished his invention from prior art disclosed by Thomas Chapman in Patent No. 5,432,506. The Chapman patent is entitled "Counterfeit Document Detection System." Like Sandru's invention, Chapman's invention is designed to authenticate checks. Chapman's patent, however, does not rely on known mathematical algorithms like RSA or CRC. Instead, Chapman discloses an invention that relies on specific tables and formulas to encode check data. For example, Chapman's invention selects certain characters from the face of the check (these characters might be numbers or letters, and might be taken from the payee field, the check amount field, the date field, or elsewhere). Each character is then representedas a one or two digit number, according to a value assigned to that character on a pre-determined table. The numbers are entered into a simple algebraic formula that uses addition, subtraction and multiplication to generate a unique code. That code is analogous to Sandru's "control code" that is then printed on the check.

Sandru and Advanced Software argue that the patents at issue in this case are nothing like the Chapman patent because Chapman's patent does not disclose a "key-based" cryptographic scheme. That is, there is no numeric string that, along with the check data, is plugged into a widely-known mathematical algorithm. It is at least arguable, however, that the entire Chapman scheme is itself a "key"-the table and the formula taken together are a "secret" scheme that make the encryption possible. In any event, Sandru's representations before the PTO and his efforts to distinguish his invention from Chapman's are important elements to consider when interpreting the Sandru patents' claim terms.

III. *Disputed claim terms*

Before the Markman hearing, the parties submitted a joint notice of disputed claim terms that listed 29 separate terms on which the parties had differing interpretations. The parties have since agreed on constructions for five of the 29 terms. Of the remaining 24 terms, 14 were argued at the Markman hearing, and ten were submitted solely on briefs. I will not be resolving all of these disputes in this order. I do not believe that resolution of every disputed term is essential to this case. Moreover, I believe that conflicts over certain terms will be more appropriately resolved in the context of the parties' disputes on the merits of the case. This order sets forth meanings for the eight key terms that go to the heart of the parties' disagreements. The parties may argue for a particular construction of any remaining terms in the context of summary judgment motions or proposed jury instructions at trial.

Claim 1 of the '110 Patent and Claim 1 of the '624 patent each provides context for the eight disputed terms. Claim 1 of the '110 patent 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.

Claim 1 of the '624 patent claims:

1. A process for enhancing the security of a cheque, comprising:

selecting private and public encryption keys associated with one of a cheque payor and cheque validator;

selecting information found on the cheque wherein the selected information varies for each instantiation of the cheque presented by the same payor;

encrypting a combination of the selected information and one of the private and public keys with a practicably secure cryptographic scheme to thereby generate a control code;

printing the selected information and the control code on the cheque; reading the selected information from the cheque;

decrypting the control code using the other of the private and public encryption keys to thereby obtain decrypted information; and

the cheque validator refusing to honour the cheque if the selected information found on the cheque does not match the decrypted information.

The parties have stipulated that any terms appearing in both the '110 and ' 624 patents should be given the same meaning in both patents. The two claims quoted above use different wording and sentence construction, but the parties agree that the claims both disclose the same essential check authenticating scheme.FN5 The terms to be construed in Claim 1 are as follows.

FN5. Although the two patents disclose essentially the same invention, it is important to note some differences between the two claims quoted above. First, the '110 patent speaks of "key information," while the '624 patent uses the term "private and public encryption keys" and "private and public keys." Second, the '110 patent uses the phrase "encrypted in combination with," while the '624 patent refers to "encrypting a combination of." Finally, Claim 1 of the '110 patent discloses both a "public key" encryption scheme in clause (i) and a "private key" encryption scheme in clause (ii). Claim 1 of the '624 patent only discloses a "public key" encryption scheme, although the preferred embodiment discussed in that patent is essentially the same CRC "private key" scheme discussed in the '110 patent.

A. "*Encrypt in combination with" and "Encrypt a combination of*"

[14] The primary dispute between the parties centers around the meaning of these two phrases, which the parties agree should be construed together. The ' 110 patent speaks of "selected information ... encrypted in combination with key information," while the '624 patent uses the phrase "encrypting a combination of the

selected information and one of the private and public keys."

Advanced Software maintains that these phrases simply mean that the check information to be encoded is encrypted using the appropriate key. Since the patents focus only on key-based cryptographic systems that are widely known, the language here directs that the "key" or "key information" is applied to the "selected information."

Fiserv, however, argues that these phrases describe a two-step process for encryption. First, the selected information is combined with the key information. Then, the combination is itself encrypted using the cryptographic algorithm. The key is not merely "used" to encrypt, rather the key is encrypted along with the check information.

Both parties claim support for their respective positions in the patent text and the file history. Advanced Software, for its part, argues that the "combination" language in both patents was necessary because it distinguishes Sandru's invention from the prior art disclosed in the Chapman patent. By using the phrase "encrypted in combination with," Sandru is making clear that the encryption key, like the check information to be encoded, is inserted into the known cryptographic algorithm. The key and the algorithm are separate. This is unlike the situation in Chapman, where the "key" is derived from the check information by using the algorithm. The "combination" here is still a one-step process that simply uses the key and the algorithm to transform the check information into a control code.

Fiserv disputes this construction by pointing out that plaintiffs' arguments here are different from the arguments they raised before the Patent and Trademark Office. *See* Phillips, 415 F.3d at 1317 (quoting Graham v. John Deere Co., 383 U.S. 1, 33, 86 S.Ct. 684, 15 L.Ed.2d 545 (1966)) ("An invention is construed not only in light of the claims, but also with reference to the file wrapper or prosecution history in the Patent Office."). The parent patent to the patents in suit here is Patent No. 6,233,340. It was this '340 Patent that Sandru had to distinguish from the Chapman patent when arguing before the PTO.

The patent examiner initially rejected the claims in Sandru's '340 Patent because of Chapman. The examiner noted that "Chapman does not explicitly teach encrypting the encryption key along with the selected information," however "it is very old and 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." Sandru did not respond to this assertion by correcting the examiner's interpretation of his patent. Sandru did not argue that the difference between his patent and Chapman's patent is that Sandru uses keys and Chapman does not. He did not argue that the "in combination with" language merely claims that the algorithm uses a key.

Instead, Sandru argued that, since the "key" in Chapman was in essence derived from the check information, there would be no value to encrypting the key along with the check information-the process would not result in any added security. Furthermore, argued Sandru, to the extent that the "key" in Chapman is the algorithm itself, it would not be possible to encrypt a combination of the key and the selected information. Fiserv argues that this prosecution history supports its interpretation of the patent. Given the chance to explain the language of his patent, Sandru emphasized the combination step as an integral part of his invention that is separate from the encryption itself. Sandru did not claim that the patent language merely teaches the use of a key to perform encryption. *See* Chimie v. PPG Indus., Inc., 402 F.3d 1371, 1384 (Fed.Cir.2005) ("The purpose of consulting the prosecution history in construing a claim is to exclude any interpretation that was disclaimed during prosecution.").

Moreover, Fiserv argues that the text of the claim terms and the patent specification further supports its interpretation. Although the claim terms in the '110 patent refer both to public key cryptography like RSA and private key systems, the patent specification emphasizes private key systems like the CRC described in the preferred embodiment. In the Summary of the Invention section of the '624 Patent, Sandru describes one step in the encryption process as "encrypting a combination of the selected information and the encryption key." Then, when the control code is later validated, Sandru says that a validator "can read the un-encrypted selected information from the negotiable instrument, re-combine it with the encryption key and re-encrypt the combination according to said scheme." Thus, Sandru emphasizes "re-combining" as its own step separate from "re-encrypt[ing] the combination." When discussing alternative embodiments such as RSA, Sandru continues to state that the invention calls for "encrypting a combination of the selected information and one of the private and public keys." Consequently, argues Fiserv, the patent consistently refers to the method of "combining" and then "encrypting" as a two-step process.

Advanced Software and Sandru counter this argument by claiming that one of ordinary skill in the art would not read such a limitation into the claim terms. Particularly in the case of RSA, say the plaintiffs, encrypting the key along with the selected information would not make any sense. In RSA, there are two keys, and each one performs a specific function (the encryption key and the decryption key). Under Fiserv's construction, the RSA encryption step would result in an encrypted combination of the selected information and the key. When the control code is decrypted, the encryption key would be revealed. The whole point of using RSA-i.e., having one key public and one key private-would be undermined. Moreover, argues Advanced Software, combining the key and the selected information prior to the encryption would make the encryption step technically impossible, because no computer could store such a large number.

Fiserv responds by noting (as the patent examiner in the '340 patent did) that encrypting a message along with its encryption key is still well-known in the art and is not in itself something that would undermine every encryption. Though the patent specification uses concatenation as a type of "combining," there are other ways that key information could be combined with selected information that would not immediately reveal the private key. In any event, Fiserv argues that even if a particular embodiment of the invention might be infeasible or might undermine the integrity of the encryption scheme, this is not a reason to depart from the plain language of the patent. Construing a patent's terms so as to ensure that the patent is useful and workable is not a goal of claim construction.

The root of the parties' disagreement is the extent to which the patent specification informs the meaning of the words used in the patent claims. The specification teaches that the encryption keys are concatenated with (i.e., combined with) the selected information and that the combination is then encrypted to produce a control code. The phrase "in combination with" or "a combination of" makes sense in this context. The specification helps explain and gives an example of what is meant by a "combination." However, claim terms are not to be limited by embodiments set forth in the specification. Comark, 156 F.3d at 1186; *but see* Kyocera Wireless Corp. v. Int'l Trade Comm'n, 545 F.3d 1340, 1346-47 ("The specification is the single best guide to the meaning of a disputed term."). The claim terms here broadly cover both the private key scheme in the preferred embodiment and public key schemes like RSA. The patents do not specify how key information and selected information are to be "combined" when using an RSA scheme or any scheme other than the one outlined in the preferred embodiment.

Considering all of the arguments presented by the parties on this issue, I conclude that Fiserv's construction of these terms is the construction that is more consistent with the terms' ordinary and customary meaning according to the customary understanding of a person of ordinary skill in the art reading the terms in the context of the intrinsic record. Kyocera, 545 F.3d at 1346. The '624 patent, in particular, refers to "a combination of" items. The items that make up the combination are the encryption key and the selected information. The word "combination" as it is used in Claim 1 of the '624 patent is a noun. It is the thing that is encrypted. Therefore, the process described as a whole in Claim 1 necessarily has two steps: one of combining (or creatingthe combination), and one of encrypting the combination. If the patentee had sought to say "encryption using an encryption key" or "encrypting selected information by applying an encryption key," he could have done so. The word "combination" is specifically and repeatedly used in the patents, and that word must provide some added meaning to the claim terms. Merck & Co. v. Teva Pharm. USA, Inc., 395 F.3d 1364, 1372 (Fed.Cir.2005) ("A claim construction that gives meaning to all the terms of the claim is preferred over one that does not do so."). The added meaning here is supplied by the specification, which teaches a two-step process of combination and encryption. *See* E.I. Du Pont de Nemours & Co. v. Phillips Petroleum Co., 849 F.2d 1430, 1433 (Fed.Cir.1988) ("It is entirely proper to use the specification to interpret what the patentee meant by a word or phrase in the claim.").

Advanced Software's argument that this construction makes the invention nonsensical is not persuasive. The specification shows how key information and selected information can be combined through concatenation. But the patent claims are not limited to combining elements in this particular way. "Combining" in this context is not a specific mathematical operation.FN6 Even in situations where a public key system is used, the combination step can take any number of forms, but the patent still speaks of "combining" the elements prior to encryption. The patent claims state that the selected information and the key information are combined, and that the encryption of these two elements together makes up the control code. The extent to which this method of encryption is practical or feasible is not relevant to claim construction. *See* SmithKline Beecham Corp. v. Apotex Corp., 403 F.3d 1331, 1339 (Fed.Cir.2005) ("The scope of patent claims can neither be broadened nor narrowed based on abstract policy considerations regarding the effect of a particular meaning."). The claims must be construed in accordance with their plain meaning to one of ordinary skill in the art.

FN6. During testimony at the Markman hearing, the defendants' expert witness demonstrated how other types of "combination" processes beyond concatenation, such as an "XOR operation," could be used in the RSA context.

Accordingly,

" *Encrypted in combination with* " and " *encrypt a combination of* " means performing mathematical operations of an algorithm which, first, combines "selected information" and one or more of the specified "keys" and second, generates a control code by encrypting the combined "selected information" and "key" or "key information."

B. *Related claim terms*

A number of the remaining disputed claim terms are integral to the main dispute that I have discussed above. These terms are interrelated and dependant upon one another for their meaning. *See* Kyocera, 545 F.3d at 1347 (quoting Hockerson-Halberstadt, Inc. v. Converse Inc., 183 F.3d 1369, 1374 (Fed.Cir.1999)) ("Proper claim construction ... demands interpretation of the entire claim in context, not a single element in isolation."). For reasons that follow from my previous discussion and use of these terms, the following definitions shall apply:

[15] " *Encrypted* " or "*encrypting* " means applying a known cryptographic scheme or algorithm to obtain a control code.

[16] " *Key information,*" " *key,*" " *keys,*" and " *encryption keys* " means a piece of information that is used with a cryptographicalgorithm to encrypt and/or decrypt the selected information, whereas the cryptographic algorithm can be widely distributed without compromising security.

[17] " *Control code* " and " *generate a control code* " means the end product of the encryption process that is then printed on the check.

[18] " *Decrypt,*" " *decrypting* " and " *decrypted* " means the reverse process of "encrypting," applied to a control code and using the proper key.

C. " *Varies for each instantiation* "

[19] The '624 patent refers to "selected information [that] varies for each instantiation of the cheque." Similar language appears in the '110 patent. Fiserv argues that this phrase implies that for each check, the "selected information" to be encrypted must always be different and unique to that check. Advanced Software argues that Fiserv's proposed definition is inconsistent with the ordinary meaning of the word "varies." According to Advanced Software, a quantity that "varies" changes between instances, but it is not always different.

Advanced Software's reading of the term "varies for each instantiation" is more consistent with the plain language of the claim and the context of the patent as a whole. To insist that the "selected information" must be different in every instance would unduly limit the invention in a way the patent does not contemplate. There is no reason why the payee, check amount, or check date would necessarily be unique to every check. These data fields would "vary" from one check to the next, but it is still possible that the same payee might receive multiple checks, or the same amount could be written on multiple checks.

Accordingly,

" *Varies for each instantiation* " means variable and generally not common to all checks issued by the same payor, but not necessarily distinct and unique to every check.

D. *Terms with a plain and ordinary meaning*

[20] "Unless the intrinsic evidence compels a contrary conclusion, the claim language carries the meaning accorded those words in the usage of skilled artisans at the time of invention." SmithKline, 403 F.3d 1331 at 1339. With respect to the terms "print" or "printing," and "match," the parties have failed to demonstrate that these words should be accorded any particular or unique meaning in light of the patents' context. Thus, I find that the following terms have a plain and ordinary meaning as understood by someone in the art at the time of invention:

" *Print*" and " *printing* " have their plain and ordinary meaning.

" *Match* " has its plain and ordinary meaning.

IV. *Conclusion*

For the reasons stated above, the preceding definitions shall apply to the patent claim terms in the '624 and '110 patents. Disputes over remaining claim terms may be raised in the context of summary judgment motions or at trial, through proposed jury instructions.

So ordered.

E.D.Mo.,2008.
Advanced Software Design Corp. v. Fiserv, Inc.

Produced by Sans Paper, LLC.