United States District Court,
C.D. California, Western Division.

KARA TECHNOLOGY, INC,
Plaintiff.
v.
STAMPS.COM, INC,
Defendant.

No. CV 05-1890 CBM(CTx)

Sept. 10, 2007.

Ari J. Jaffess, Eliot D. Williams, Eric J. Faragi, Jennifer Cozeolino, Neil P. Sirota, Noera Ayaz, Robert C. Scheinfeld, Baker Botts LLP, New York, NY, Frederick A. Clark, McKenna Long & Aldridge LLP, Los Angeles, CA, for Plaintiff.

Marjorie A. Witter, Monick Theresa Paul, Fredricka Ung, James Woo Ahn, Tom Crunk, Graves Law Office, Mark N. Hurvitz, Michael T. Purleski, Shelley Marie Cobos, Squire Sanders & Dempsey, Los Angeles, CA, for Defendant.

ORDER RE: PARTIES'CLAIM CONSTRUCTION BRIEFS

CONSUELO B. MARSHALL**, District Judge.**

The matters before the Court, the Honorable Consuelo B. Marshall, Judge, presiding, are the Plaintiff's and Defendant's Claim Construction Briefs.

JURISDICTION

This Court has jurisdiction pursuant to 28 U.S.C. s.s. 1331 and 1338(a) and supplemental jurisdiction over the related state law claims under 28 U.S.C. s. 1367.

FACTUAL AND PROCEDURAL BACKGROUND

A. Kara's Patent Background

This suit involves two patents invented by Kara Technology Incorporated ("KT"), including U.S. Patent No. 6,735,575 ("the '575 Patent") filed on June 2, 1999 and U.S. Patent No. 6,505,179 ("the '179 Patent") filed on June 30, 1999, which is a continuation-in-part FN1 of the ' 575 Patent. Pl. Claim Constr. at 8-9. As a result of the ' 179 Patent being a continuation-in-part of the ' 575 Patent, the patents use many of the same claim terms.

The invention describes a method for a buyer to purchase a good or service in an e-commerce transaction

and receive a verifiable receipt of the transaction from the seller, which can be used at a later time to verify that the transaction actually occurred. Pl. Claim Constr. at 7. For instance, this technology is used for purchasing stamps on-line whereby stamps are printed by the consumer and the post office is able to verify the authenticity.

On October 22, 2005, KT filed a complaint against Stamps.com in the Southern District of New York for patent infringement, misappropriation and misuse of trade secrets, breach of contract, unfair competition, and unjust enrichment. The case was transferred to the Central District of California on March 16, 2005. Each party filed memoranda requesting the Court to construe certain terms within the patents. The Court conducted a *Markman* hearing on May 31, 2007.

LEGAL STANDARD

Claims define the legal scope of the invention and claim construction is a question of law. Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed.Cir.1995). "[T]he definition in the specification controls the meaning of [the term], regardless of any potential conflict with the term's ordinary meaning as reflected in technical dictionaries." 3M Innovative Props. Co. v. Avery Dennison Corp., 350 F.3d 1365, 1374 (Fed.Cir.2003). If there is no clear definition within the specification, the words of a [patent] claim are generally given their ordinary and customary meaning, i.e. "the meaning that the term would have to a person of ordinary skill in the art in question ... as of the [patent's] effective filing date. Phillips v. AWH Corp., 415 F.3d 1303, 1312-13 (Fed.Cir.2005) (en banc); Ventana Medical Systems Inc. v. Biogenex Lab., 473 F.3d 1173, 1180 (Fed.Cir.2006). "In some cases, the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words." Phillips, 415 F.3d at 1314. In construing claims, the Court is not required to analyze sources in any specific sequence or barred from considering any particular source as long as those sources are not used to contradict claim meaning that is unambiguous in light of the intrinsic evidence. Id. at 1324.

The patent specification is central to a determination of "the meaning of a claim term as it is used by the inventor in the context of the entirety of his invention." Comark Comm'ns v. Harris Corp.., 156 F.3d 1182,1187 (Fed.Cir.1998). The patent specification "is always highly relevant to the claim construction analysis. Usually it is dispositive; it is the single best guide to the meaning of a disputed term." Phillips, 415 F.3d at 1315 (quoting Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576,1582 (Fed.Cir.1996). "The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention [in the specification] will be, in the end, the correct construction." *Id*. at 1316 (quoting Renishaw PLC v. Marposs Societa' Per Azioni, 158 F.3d 1243, 1250 (Fed.Cir.1998)). Although a patent claim may at times contain terms that do not appear in the specification, all "terms and phrases used in the claims must find clear support or antecedent basis in the [specification] so that the meaning of the terms in the claims may be ascertainable by reference to the [specification]." Tandon Corp. v. U.S.I.T.C, 831 F.2d 1017, 1024 (Fed.Cir.1987); *see* Lockwood v. Am. Airlines, Inc., 107 F.3d 1565, 1572 (Fed.Cir.1997).

ANALYSIS

The construction of the following terms is undisputed by the parties:

-> Display means "any visual representation of information;"

-> Printer means "any printing device for creating images on paper, or it could be a device for storing

images which can later be displayed to obtain the goods and or services;"

-> Non-secure Printer means "a printer that does not incorporate security functionality;"

-> Providing, under control of said comparing step means "providing, if permitted by a computer that is programmed to prevent the transaction if the unique data has Been previously accepted."

The parties dispute the construction of the following terms:

-> Preestablished data/said media having preestablished thereon data which is unique to said media;

-> A location independent from said printer;

-> Validity/Establishing the validity of a display;

-> Key data;

-> Decode or Decodable;

-> Said Independent Location Operable to Send to Said Printer a Security Indicia, as Part of a Human Readable Display, Said Security Indicia Created in Part by Information Contained in Said Preestablished Media Data/Security indicia;

-> And Whereby Said Security Indicia is Validatable at a Subsequent Time Partially under Control of Data Contained in Said Preestablished [Media or Paper] Data;

-> Said Control data being decodable, in part, under control of key data associated on said particular printable stock with said unique data/Partially under control of key data.

A. The Construction of "Preestablished Data"

The term "preestablished data" refers to paper or media having unique preestablished data on the paper. Plaintiff contends that the term "preestablished data" means "data established beforehand, e.g., before printing of the information to be created." Defendant contends that the term means "paper having data that is unique to that particular sheet of paper and that is affixed onto the paper prior to the user obtaining the paper."

a. Defendant's construction

Defendant points to the specifications within the patents to support its position that preestablished data refers to "paper having data that is unique to that particular sheet of paper." The patent states that "each preprinted form has a unique identification code, ... [which] insures that a copy of the preprinted form is not being used." Pl.Ex. A at 2:9-12; Pl.Ex. B at 2:33-36. The patent states that "some portion of the preprinted data is unique to the exact form selected by the user at that time." Pl.Ex. A at 2:4-6; PL Ex. B at 2:27-30. The patent uses an example that "the printer can be part of a vending machine which, ..., only contains paper having on (or within) it preestablished data unique to that sheet of paper." Pl.Ex. B at 2:67-3:3.

Defendant supports its contention that the data was affixed onto the paper prior to the user obtaining the

paper with the claim language. In Claim 1 of the '575 patent it states that the method of established validity of a display created by a general purpose creation device is comprised of "placing said device media upon which information may be created, said media having preestablished thereon data which is unique to said media." Pl.Ex. A at 7:37-40.

Defendant contends that the patent specifications leave no doubt that the "preestablished data" means pre-printed on the paper. The Abstracts of the patents state that "preprinted forms" are used. Pl.Ex. A; Pl. Ex B. The Summary of the Invention in each of the patents describes the invention as one in which a "system and method is utilized for establishing a commercially available partially preprinted form" where the "form is advantageously preprinted with both human readable data and machine readable data." Pl.Ex. A at 1:42-46, 52-54; Pl.Ex. B at 1:66-2:3, 9-11.

Further, in the section entitled "Brief Description of the Drawing" a figure is described as a "sample preprinted form." Pl.Ex. A at 3:17; Pl.Ex. B at 3:37. The Detailed Description describes a figure that that "can be ticket stock printed with indicia 16 thereon." Pl.Ex. A at 3:33-35; Pl.Ex. B at 3:56-58.

b. Plaintiff's construction

Plaintiff contends the term "preestablished data" means "data established beforehand, e.g., before the printing of the information to be created." Plaintiff argues that its construction recites the plain meaning of the term and that those with ordinary skill in the art in 1999 would not consider "preestablished data" to be limited to "preprinted data." Keromytis Decl. para. 18. Plaintiff contends that the doctrine of claim differentiation suggests that the meaning of preestablished is distinct from the meaning of preprinted because both terms appear in the patent. Plaintiff points to the following language in the patent to support that preestablished data need not be preprinted:

This security image *can be,* for example, any of the above types. Some of the preestablished data *could be* images which are visible or understandable to humans while other parts of the data can be readable only with special systems.

Pl.Ex. B at 5:18-23 (emphasis added). The specifications in the patent state that printers "can be any printing device for creating images on paper, or it could be a device for storing images which can later be displayed to obtain the goods and or services." Pl.Ex. B at 2:26-67; Pl.Ex. A at 2:42-46. Plaintiffs argue that this language suggests that data can be preestablished as images that may be stored and later displayed without being preprinted. Plaintiffs point to the language in the specification allowing an electronic display device to code and subsequently decode the information as support for its contention that preestablished data does not have to be pre-affixed to the sheet of paper. Pl.Ex. B at 7:35-39.

c. Conclusion

The interpretation of "preestablished data" offered by Plaintiff is closest to the plain meaning of the term and most supported by the language inside the patent. The use of the term "preprinted" so often in the patent suggests that the drafter intends for the meaning of "preprinted" to be different from the meaning of "preestablished" even though the patent supports that "preestablished data" may also be "preprinted" on a sheet of paper prior to printing. The language in the specification, however, does not limit "preestablished data" to mean that which is only preprinted onto sheets of paper.

The Court construes "preestablished data" consistent with Plaintiffs' definition as "**data established**

beforehand, e.g., before the printing of the information to be created." It follows that the phrase "said media having preestablished thereon data which is unique to said media" is construed to mean "said media having unique data established thereon beforehand."

B. The Construction of "A Location Independent From"

Plaintiff contends that "a location independent from" said printer means "any place apart from the printer, such as another device." Defendant contends that the term means "communicating at least a portion of the unique, pre-printed data over an external network to a location that is not under the control of the user of the printer." The term is used in several claims of both patents. For example, Claim 1 of the '575 patent states that a method for establishing the validity of a display is comprised of several steps, including "communicating at least a portion of said preestablished data to a location independent from said device."

a. Defendant's construction

Defendant contends that the claim language compels its interpretation because the patent specification uses the term "location" instead of "device," which connotes a material geographic separation between the printer and the place to which the data is communicated. Defendant states that its meaning is reinforced by the modifier "independent," which denotes a location that is not under the control of the person or entity that is using the printer. Further, Defendant states that when using the term "communicate" the patents allegedly refer consistently to communication over an "external network" to a location that is not under the control of the user. *See e.g.,* Pl.Ex. A at 1:59-62 ("In operation, the purchaser enters into an interaction communication with the seller of the service. This may be ..., from the purchaser's PC at his/her home via the Internet to a website maintained by the seller.")

b. Plaintiff's construction

Plaintiff contends that Defendant's construction of the term impermissibly limits the terms meaning. "[C]laim terms take on their ordinary and accustomed meanings unless the patentee demonstrated an intent to deviate from the ordinary and accustomed meaning of a claim term by redefining the term or by characterizing the invention in the intrinsic record using words or expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope." Teleflex, Inc. v. Ficosa North America Corp., 299 F.3d 1313, 1327 (Fed.Cir.2002). Plaintiff contends that there is no language in the patent specifically restricting the meaning of "location" beyond that which would be its ordinary meaning to a person skilled in the art.

c. Conclusion

Defendant's construction adds limitations to the term "a location independent from" that are not suggested from a reading of the patent as a whole. The patent does not suggest that the patentee demonstrated an intent to deviate from the ordinary meaning of the words in the claim. The patentee uses restricting terms when he intends to limit the phrase. For example, Claim 1 of the '575 patent states that the method comprises of steps for "communicating at least a portion of said preestablished data to a location independent from said device." This suggests that the drafter narrows the patent claims and specifications containing the term "a location independent from" with other language such as "communicating" or "preestablished data" when he intends to limit the meaning of the phrase. Accordingly, "location independent from" said printer or device should be construed in accordance with its plain meaning.

The Court construes the term consistent with Plaintiff's meaning as "**any place apart from the printer, such as another device.**"

C. The Construction of "Validity"

The '575 patent states that information "can be communicated to processor so that when printed indicia is presented, processor can utilize its intelligence to determine the *validity* of the printed indicia to further check that copies are not made and that the services are not given to the wrong person ..." Pl.Ex. A at 5:17-24. Plaintiff contends that validity should be construed in the patents to mean "proper use." Defendant suggests that the term should be construed to mean "authentic."

The parties further request the Court to construe the term "establishing the validity of a display."

a. Defendant's construction

Defendant argues that the specifications within the patents support its construction because the purpose of the inventions are to enable a purchaser of goods or services to obtain a printed receipt that acts "as a final verification of authenticity at the point where the actual services are rendered." Pl.Ex. A at 1:36-39; *See* Pl.Ex. A at 2:32-34 ("For verification of authenticity of the boarding pass and/or luggage tags, the original preprinted indicia is read to obtain a decryption key.")

b. Plaintiff's construction

Plaintiff contends that the "validity" of the invention is best established when it is used properly, meaning when there is some indicia on the stamp that determines its authenticity and its protection against replay by the user (i.e. reusing the same stamp without paying). Plaintiff contends that Defendant's construction only encompasses establishing authenticity of the stamp and does not also encompass protecting against replay. Plaintiff argues that the doctrine of claims differentiation prohibits the Defendant's construction because the patent uses the word "authenticity" within the patent and words within a patent should have different claim meanings.

c. Conclusion

The invention allows the printed receipt to act as a "final verification of authenticity," which establishes the validity of a receipt. The parties do not dispute that a "valid" stamp is also authentic. An authentic stamp is genuine and not copied. Plaintiff's definition encompassing protection from replay narrows the term in a way that is not suggested by the patent and goes against the plain meaning of the term.

The Court construes "validity" consistent with Defendant's construction as "**authentic.**" Accordingly, "establishing the validity of a display" is construed to mean "establishing that a display is authentic."

D. The Construction of "Key Data"

Plaintiff contends that "key data" means "information used to assist in authentication." Defendant contends that the term means "[information or data] comprising a key."

a. Defendant's Construction

Defendant states that the plain meaning of the claim language requires the construction it proposes because one skilled in the art would understand key data to refer to a key. McDaniel Decl. para. 27. Defendant argues that a key is manifestly not just any "information used to assist in authentication" as Plaintiff suggests. Defendant's expert states that one skilled in the art would not normally ascribe such a broad meaning to the term because:

a key is a number typically embodied in a data file that is created by a key generation algorithm and that is in turn used to create an authentication indicia or to validate an authentication indicia, and it is the mathematical properties of keys that enable modern authentication systems such as digital signature and hashed message authentication code systems to function.

McDaniel Decl. para. 28. Further, Defendant contends that Plaintiff's definition is impermissible because it reads "key" out of the definition. *See* Oak Technology, Inc. v. International Trade Com'n., 248 F.3d 1316, 1329 (Fed.Cir.2001) ("[to] read an express limitation out of the claims ... will not do because '[c]ourts can neither broaden nor narrow claims to give the patentee something different than what he has set forth") (internal quotes omitted).

b. Plaintiffs construction

Plaintiff contends that a person of ordinary skill in the art would understand the term "key data" in the patents to refer to any information that may be used to assist in the authentication of a document and would not interpret the term to be limited to cryptographic keys. Plaintiff supports its position with specifications in the patent stating that the data may be human readable, contending that because cryptographic information is not normally human readable a key would not be necessary. Keromytis Decl. para. 25; *See e.g.,* Pl.Ex. B at 5:7-22. Plaintiff's expert states that a person of ordinary skill in the art would not interpret the Kara patents to require cryptographic methods to authenticate a document. Keromytis Decl. para. 25.

c. Conclusion

As used within the patent, key data is necessary to validate security indicia contained in preestablished data. *See* Claim 2 of the '575 patent, stating that "[t]he methods of claim 1 wherein created source of ones of said security indicia is validated by *key information* contained in at least a portion of said preestablished data." Plaintiff's construction of key data as information "used to assist in authentication" is not supported by the language in the specifications because it does not encompass the uniqueness of the information contained in the "key data." Whether this data is machine readable only or a code that is visible to the human eye does not change its character as something that contains a unique validation code that is required for authentication.

Accordingly, the Court construes the term in the manner in which Defendant suggests as "**[information or data] comprising a key.**"

E. The Construction of Decoding and Decodable

Plaintiff contends that "decoding" should be construed as "reading" and decodable should be construed as "readable." Defendant states that the Court should construe decoding language to mean "converting a [first or second] indicia that is encoded in an exclusively machine-readable format to a different format" and that decodable should be interpreted to mean "capable of being converted from ciphertext to plaintext by the application of a decryption algorithm."

a. Defendant's construction

Defendant's construction of decoding is derived from the term's meaning in the field of secure systems design, which is to convert encoded text or data in a format that is exclusively machine-readable, to a different format. McDaniel Decl. para. 29. Defendant supports its construction with the term's definition in the *McGraw-Hill Dictionary of Scientific and Technical Terms 5th Ed.*, which is "to translate coded characters into a more understandable form." Further, Defendant cites to patent language that implies or makes clear that a machine reads information on a preprinted item. PL Ex. A at 4:60-5:2, 3:35-40, Fig. 1 & 6:52-56.

Defendant's construction of "decodable" includes the process of decrypting, which requires that the information be capable of being converted from ciphertext,FN2 to plaintext. Defendant's full construction contains a method by which this occurs, which is "by the application of a decryption algorithm under control of a key." Defendant contends that the decryption method mandates this definition and must be done by the machine using a key because of the practical impossibility that a human being may be able to use a key to decrypt anything.

b. Plaintiffs construction

Plaintiff's construction of the terms allow for indicia to be either human readable or machine readable. Plaintiff's cite to the '575 patent language referring to ticket stock stating that:

Indicia portion 16a can be a machine readable portion of the indicia ... and portion 16b is a human readable portion ... for the purposes of this invention the indicia can be entirely human readable, if desired ... the human readable portion could be a different form of the indicia such as bar codes that can be machine readable.

Pl.Ex. A at 3:33-43. Plaintiff's expert states that one of ordinary skill in the art would interpret the terms broadly to mean reading and readable by either a human or a machine. Keromytis Decl. at para. 26. For instance, Plaintiff points out that a human being may decode a human readable serial number by reading it and putting the numbers into a keyboard to enter it into a computer, thereby having human readable data decoded into machine data.

c. Conclusion

Defendant's construction of "decoding" and "decodable" does not comport with the specifications in the patent allowing for human readable data that is part of a code or indicia, which narrows the terms beyond those contemplated by the language in the patent. Plaintiff's construction of the terms encompasses information that is "coded" but that can be read by a machine or by a human which most closely comports with the manner in which the terms are used within the patent as well as the plain meaning of the terms.

Accordingly, the Court construes decoding and decodable consistent with Plaintiff's construction as "**reading**" and "**readable.**"

F. The Construction of the Phrase "Said Independent Location Operable to Send to Said Printer a Security Indicia, as Part of a Human Readable Display, Said Security Indicia Created in Part by Information Contained in Said Preestablished Media Data"FN3

Plaintiff asks the Court to construe this phrase to mean that the "security indicia is created in part using information contained in preestablished data" and that the "independent location is capable of sending to the printer a security indicia, and that the security indicia is part of a human readable display." Defendant asks the Court to construe this language as "said independent location having a computer programmed to create a security indicia under control of a key contained in the preestablished data, and operable to send to the printer a file that contains a graphical representation of the security indicia." To construe this phrase as a whole it is necessary to construe the terms within the phrase.

a. The Construction of Security Indicia

The parties agree that security indicia means a marking that appears on the document printed by the buyer, which is later used to validate the document. Where the parties differ is how the security indicia is created. The main disagreements between the parties are on whether the security indicia must be (1) encrypted, (2) under the control of a key, and (3) sent in a single file.

1. Defendant's construction requires that the security indicia is created under control of a key and that the "information contained in" the pre-printed data is a "key"

To arrive at this construction Defendant maintains that the security indicia is created under control of a key and that the information contained in the pre-printed data is a key.

Defendant contends that the technology of secure systems design supports that security indicia is created using a key. Defendant's expert explains that there were two methods of authentication systems as of 1999 when the patent was issued, and both methods required the use of a key to create the authenticating indicia and to validate a document. One method required creating and attaching a "digital signature" to the document and the other method involved creating a "hashed message authentication code" of the document. All digital signature algorithms use a "key" to create the signature, which is a very large number typically embodied in a data file. In the key system, the person signing the document uses a "private key" that is kept a secret that matches with a distributed "public key," which is used to validate the authenticity of the document. The second method involves using a single key to both create and validate the security indicia through hashing the message (creating a unique fingerprint of the document), encrypting the hash using the key and sending the encrypted message to the recipient who then decrypts the hash.FN4

Accordingly, Defendant contends that the only information that could be said to "create" Kara's security indicia is a key. McDaniel Decl. para.para. 20-21. Defendant's expert states that "it is the use of a person's key that proves that a person created the indicia; without it, the indicia cannot validate the associated document." Id. at para. 20.

Defendant also points to the patent specifications as support for its contention. For example, the patents state that: there is a "second indicia which is machine readable similar to indicia ... and decodable only by utilizing the key which is contained in indicia;" the machine readable data on the pre-printed form "contains *key information* which serves to help decode material ...;" and the seller uses the "unique identification number to establish an encryption code for printing on the form a machine readable security indicia," which will subsequently be used to "verify the authenticity of the information to be printed on the form." Pl.Ex. B at 5:57-60, 2:11-15, 2:36-41. Defendant's contend that the language of the claims and the specifications compel the narrow construction that key information is contained in the pre-printed data. *See* Laitram Corp. v. Morehouse Industries, Inc., 143 F.3d 1456, 1463 (Fed.Cir.1998) (rejecting a broader construction not

supported by the "written description").

2. Plaintiffs construction only requires that the security indicia is created in part using information contained in preestablished data

Plaintiff contends that security indicia is not limited to information that is encrypted using a key because security indicia includes information that is human readable, which by its nature cannot include a key. Plaintiff states that the plain meaning of the phrase does not include or imply that a key must be embedded in the preestablished data. Plaintiff argues that while the specifications of the patents describe certain embodiments in which a key is embedded in the preestabished data, the specification does not limit the claims to these embodiments.

Instead, Plaintiff argues that the specification language only describes embodiments of the invention in which information from the preestablished data is merely *used* to obtain a key. *See e.g.,* Pl.Ex. B at 2:37-39 (the "seller then uses the unique identification number to establish an encryption code for printing on the form a machine readable security indicia"). Plaintiff's expert states that if the information was encrypted, the preestablished data might provide a database key that identified a location in a secure database where a key might be found but not actually have the key within the preestablished data. *See* Keromytis Decl. at para. 23.

Plaintiffs state that the plain meaning of security indicia supports the use of a hologram, and not a key, to establish the validity of a document. Plaintiffs do not offer evidence as to how the patent language supports the use of a hologram.

3. Conclusion

"Security indicia" is part of the method by which the associated document is validated and is integral to the invention's use. The history of secure systems design supports that this invention requires a key. The use of the term "key information" within the patent supports that a "key" is used to validate each document. The patent specifications state that "key information" is preprinted on the form and that the seller uses a "unique identification number to establish an encryption code for printing on the form a machine readable security indicia." Plaintiff's contention that security indicia does not contain a key because it can be human readable is unpersuasive. Codes may be readable to the human eye, but still contain a unique encryption that may not be human understandable. The language in the patent addressing the uniqueness of each preprinted code or indicia supports that the information is "key."

Accordingly, the Court construes "security indicia" to **"be created under control of a key" and that the "information contained in" the pre-printed data be a "key"** consistent with Defendant's definition.

b. Construction of "human readable display"

1. Defendant's construction that the file contains a "graphical representation of the display"

There is no dispute that the claim language on its face recites that the independent location sends the security indicia to the printer, "as part of a human readable display." Defendant contends that in order for the display to be human readable at this stage in the process, it must be comprised of a file that contains a graphical representation of the display, such as a bit map or vector graphics file. McDaniel Decl. at para. 22. Accordingly, Defendant argues that the clause requires that the entire display, including the security indicia

be sent by the independent location to the user in a file containing a graphical representation of the display.

2. Plaintiff's construction only requires that the security indicia is part of a human readable display

Plaintiff contends that there is no support for Defendant's construction within the patent. Plaintiff argues that the plain meaning of the claim and the meaning which is given those of ordinary skill in the art is that "the independent location is capable of sending to the printer a security indicia, and that the security indicia is part of a human readable display."

3. Conclusion

The patent language does not suggest Defendant's narrow construction of the term, nor does the plain meaning of "human readable display" support that there be a graphical representation of the display sent in a single file. If a human readable display can be sent in another way, the language in the patent does not prohibit it.

Accordingly, the Court construes the phrase "as part of a human readable display" consistent with Plaintiff's construction as meaning "**the independent location is capable of sending to the printer a security indicia, and that the security indicia is part of a human readable display.**"

c. The Court's Construction of "Said Independent Location Operable to Send to Said Printer a Security Indicia, as Part of a Human Readable Display, Said Security Indicia Created in Part by Information Contained in Said Preestablished Media Data"

The parties have asked the Court to construe the phrase by suggesting a construction for specific terms within the phrase. The Court finds that after construing the terms in the phrase, it does not construe the full phrase consistent with either Defendant's or Plaintiff's complete construction.

Accordingly, the Court construes the phrase as "**said independent location having a computer programmed to create a security indicia under control of a key contained in the preestablished data that is capable of sending to the printer a security indicia, and that the security indicia is part of a human readable display.**"

G. The Construction of the Term "And Whereby Said Security Indicia is Validatable at a Subsequent Time Partially under Control of Data Contained in Said Preestablished [Media or Paper] Data"

The Court has addressed herein many of the terms contained in this phrase. plaintiff requests the Court to construe this claim to mean that "the security indicia may be, at a subsequent time, established to be valid in part using information contained in the preestablished data." Defendant proposes the construction to mean "and by which it may be established at a subsequent time, under control of the key contained in the preestablished paper data, that the security indicia is authentic."

The Court construes the term "partially under control of data" within this phrase consistent with its construction of security indicia. The "controlling" data is that which contains a "key" containing unique information embedded in the preestablished media, which is used to validate the security indicia.

Based on the Court's conclusions regarding the terms in this phrase, the Court construes the term consistent with Defendant's meaning as "**and by which it may be established at a subsequent time, under control of**

the key contained in the preestablished [media or] paper data, that the security indicia is authentic."

H. The Construction of "Said Control Data being Decodable, in part, Under Control of Key Data Associated on Said Particular Printable Stock with Said Unique Data"

After the *Markman* hearing Defendant requested the Court to construe the phrase "said Control data being decodable, in part, under control of key data associated on said particular printable stock with said unique data," which contains several terms that the Court was asked to construe. Neither party proposed a construction of the phrase.

The Court construes the phrase consistent with its construction of the individual terms within the phrase. Accordingly, the Court construes the phrase as "**said control data being readable, in part under control of data comprising a key, associated on said particular printable stock with said unique data.**"

CONCLUSION

Accordingly, the Court makes the above findings in response to the Parties' Claim Construction Briefs.

IT IS SO ORDERED.

FN1. A continuation-in-part (CIP) application is "an application filed during the lifetime of an earlier nonprovisional application, repeating some substantial portion or all of the earlier nonprovisional application and adding matter not disclosed in the said earlier nonprovisional application." 4A Donald S. Chisum, *Chisum on Patents* s. 13-15 (2005). The CIP can be used for improvements that have developed since the filing of the parent application. *See id* s. 13-16.

FN2. Ciphertext is defined as "text in encrypted form, as opposed to the plain text." *Dictionary.com, Unabridged, (v 1.1)*. Random House, Inc. *http:// dictionary.reference.com/browse/cryptographic* (accessed: May 25,2007).

FN3. The following discussion also encompasses the construction of the terms in the phrase "said independent location operable to create on said media a security indicia, said security indicia created in part by information contained in said preestablished media data."

FN4. Encrypting is the act of converting plaintext into ciphertext and decrypting is the act of converting ciphertext into plaintext. Def. Brief at 10:3-4.

C.D.Cal.,2007.
Kara Technology, Inc. v. Stamps.com, Inc.