**IN THE UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF DELAWARE**

| | | |
|---|---|---|
| STRIKEFORCE TECHNOLOGIES, INC., | : | |
| | : | |
| Plaintiff, | : | |
| | : | |
| v. | : | Civ. A. No. 13-490-RGA-MPT |
| | : | |
| PHONEFACTOR, INC., and FIRST MIDWEST BANCORP, INC. | : | |
| | : | |
| | : | |
| Defendants. | : | |

**REPORT AND RECOMMENDATION**

## I. INTRODUCTION

This is a patent suit. On March 28, 2013, StrikeForce Technologies, Inc. ("StrikeForce" or "plaintiff") filed suit against PhoneFactor, Inc. ("PhoneFactor" or "defendant"), FiServ, Inc. ("FiServ"), and First Midwest Bancorp, Inc. ("First Midwest") alleging those entities infringe U.S. Patent No. 7,870,599 ("the '599 patent").[1] On June 11, 2013, StrikeForce filed a "Notice of Dismissal of FiServ, Inc. Without Prejudice."[2] On June 25, 2013, StrikeForce filed an amended complaint removing FiServ as a defendant and adding additional allegations with respect to First Midwest.[3] On July 8, 2014, StrikeForce filed a second amended complaint adding allegations that PhoneFactor and First Midwest also infringe U.S. Patent Nos. 8,484,698 ("the '698

[1] D.I. 1.
[2] D.I. 27.
[3] D.I. 34.

patent") and 8,713,701 ("the '701 patent").[4] On December 4, 2014, StrikeForce and First Midwest filed a "Stipulation and Order of Dismissal" by which all claims between those two parties were dismissed with prejudice.[5]

On November 19, 2014, the court held a *Markman* hearing regarding contested claim terms. This Report and Recommendation sets for the court's suggested constructions of those terms.

## II. BACKGROUND OF THE INVENTION

The patents-in-suit are titled "Multichannel Device Utilizing a Centralized Out-Of-Band Authentication System (COBAS)." The patents are directed to multichannel security systems and methods for authenticating a user seeking to gain access to, for example, Internet websites and VPN networks such as those used for conducting banking, social networking, business activities, and other online services. Such technology is sometimes known as "out-of-band" authentication. When coupled with more traditional processes, they are more commonly known as two factor authentication.[6] The Abstract recites:

> A multichannel security system is disclosed, which system is for granting and denying access to a host computer in response to a demand from an access-seeking individual and computer. The access-seeker has a peripheral device operative within an authentication channel to communicate with the security system. The access-seeker initially presents identification and password data over an access channel which is intercepted and transmitted to the security computer. The security computer then communicates with the access-seeker. A biometric analyzer–a voice or fingerprint recognition device–operates upon

[4] D.I. 68. The patents-in-suit share a common specification. For ease of reference, specification citation herein is to the '599 patent.

[5] D.I. 131.

[6] D.I. 68 at ¶ 12.

> instructions from the authentication program to analyze the monitored parameter of the individual. In the security computer, a comparator matches the biometric sample with stored data, and, upon obtaining a match, provides authentication. The security computer instructs the host computer to grant access and communicates the same to the access-seeker, whereupon access is initiated over the access channel.[7]

## III. LEGAL STANDARD

"The words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art when read in the context of the specification and prosecution history."[8] The Federal Circuit has stated "[t]here are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution."[9]

"To act as its own lexicographer, a patentee must 'clearly set forth a definition of the disputed claim term' other than its plain and ordinary meaning."[10] "It is not enough for a patentee to simply disclose a single embodiment or use a word in the same manner in all embodiments, the patentee must 'clearly express an intent' to redefine the term."[11]

> The standard for disavowal of claim scope is similarly exacting. "Where the specification makes clear that the invention does not include a

---

[7] '599 patent, Abstract.

[8] *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc)); *see also Phillips*, 415 F.3d at 1313 ("We have made clear . . . that the ordinary and customary meaning of a claim term 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." (citing *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004)).

[9] *Thorner*, 669 F.3d at 1365 (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1580 (Fed. Cir. 1996)).

[10] *Id.* (quoting *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002)).

[11] *Id.* (quoting *Helmsderfer v. Bobrick Washroom Equip., Inc.*, 527 F.3d 1379, 1381 (Fed. Cir. 2008)).

> particular feature, that feature is deemed to be outside the reach of the claims of the patent, even though the language of the claims, read without reference to the specification, might be considered broad enough to encompass the feature in question." *SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001). "The patentee may demonstrate intent to deviate from the ordinary and accustomed meaning of a claim term by including in the specification expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope." *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002).[12]

As with its explanation of a patentee acting as its own lexicographer, the Federal Circuit stated "[i]t is likewise not enough that the only embodiments, or all of the embodiments contain a particular limitation."[13] The court concluded: "[w]e do not read limitations from the specification into claims; we do not redefine words. Only the patentee can do that. To constitute disclaimer, there must be a clear and unmistakable disclaimer."[14]

When construing claim terms, a court considers the intrinsic record, i.e., the claim language, the patent specification, and the prosecution history.[15] In particular, the patent specification "'is highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'"[16] In addition to considering the intrinsic record, the Federal Circuit has "also authorized district courts to rely on extrinsic evidence, which 'consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises.'"[17] For instance:

---

[12] *Id.* at 1366.
[13] *Id.*
[14] *Id.* at 1366-67.
[15] *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 977-80 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996).
[16] *Phillips*, 415 F.3d at 1315 (quoting *Vitronics*, 90 F.3d at 1582).
[17] *Id.* at 1317 (quoting *Markman*, 52 F.3d at 980).

> extrinsic evidence in the form of expert testimony can be useful to a court . . . to provide background on the technology at issue, to explain how an invention works, to ensure that the court's understanding of the technical aspects of the patent is consistent with that of a person of skill in the art, or to establish that a particular term in the patent or the prior art has a particular meaning in the pertinent field.[18]

Extrinsic evidence, however, is viewed "as less reliable than the patent and its prosecution history in determining how to read claim terms . . . ."[19]

When construing mean-plus-function terms, additional principles are implicated. "A claim element that contains the word 'means' and recites a function is presumed to be drafted in means-plus-function format under 35 U.S.C. § 112 ¶ 6[, now § 112(f)]."[20] "The presumption is rebutted, however, 'if the claim itself recites sufficient structure to perform the claimed function.'"[21]

To construe a means-plus-function term, courts employ a two-part test. First, the court determines the claimed function.[22] Next, the court "identif[ies] the corresponding structure in the written description of the patent that performs that function."[23] The identified structure "must permit one of ordinary skill in the art to 'know and understand what structure corresponds to the means limitation.'"[24]

When the corresponding structure is a computer, the specification must disclose

---

[18] *Id.* at 1318.
[19] *Id.*
[20] *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1366 (Fed. Cir. 2008).
[21] *Id.* (quoting *Envirco Corp. v. Clestra Cleanroom, Inc.*, 209 F.3d 1360, 1364 (Fed. Cir. 2000)); *see also Sage Prods., Inc. v. Devon Indus., Inc.*, 126 F.3d 1420, 1427-28 (Fed. Cir. 1997) ("[W]here a claim recites a function, but then goes on to elaborate sufficient structure, material, or acts within the claim itself to perform entirely the recited functions, the claim is not in mean-plus-function format.").
[22] *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1332 (Fed. Cir. 2006).
[23] *Id.*
[24] *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1340 (Fed. Cir. 2008) (quoting *Biomedino, LLC v. Waters Techs. Corp.*, 490 F.3d 946, 949-50 (Fed. Cir. 2007)).

an algorithm to perform the claimed function.[25]

> Because general purpose computers can be programmed to perform very different tasks in very different ways, simply disclosing a computer as the structure designated to perform a particular function does not limit the scope of the claim to "the corresponding structure, material, or acts" that perform the function as required by section 112 paragraph 6.[26]

"[A] general purpose computer programmed to carry out a particular algorithm creates a 'new machine' because a general purpose computer 'in effect becomes a special purpose computer once it is programmed to perform particular functions pursuant to instructions from program software.'"[27] "The instructions of the software program in effect 'create a special purpose machine for carrying out the particular algorithm.'"[28] "Thus, in a means-plus-function claim 'in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm.'"[29]

There is an exception to the rule that the specification must disclose an algorithm. Where the claimed "functions can be achieved by *any* general purpose computer *without* special programming . . . it [is] not necessary to disclose more structure than the general purpose processor that performs those functions."[30] The Federal Circuit explained the exception identified in *In re Katz* is a "narrow" one:

---

[25] *Net MoneyIN*, 545 F.3d at 1367 ("[A] means-plus-function claim element for which the only disclosed structure is a general purpose computer is invalid if the specification fails to disclose an algorithm for performing the claimed function.").

[26] *Aristocrat Techs. Austl. Pty Ltd. v. Int'l Game Tech.*, 521 F.3d 1328, 1333 (Fed. Cir. 2008).

[27] *Id.* (quoting *WMS Gaming, Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1348 (Fed. Cir. 1999)).

[28] *Id.* (quoting *WMS Gaming*, 184 F.3d at 1348).

[29] *Id.* (quoting *WMS Gaming*, 184 F.3d at 1349).

[30] *In re Katz Interactive Call Processing Patent Litig.*, 639 F.3d 1303, 1316 (Fed. Cir. 2011) (emphasis added).

> If special programming is required for a general-purpose computer to perform the corresponding claimed function, then the default rule requiring disclosure of an algorithm applies. It is only in the *rare circumstances* where any general-purpose computer without any special programming can perform the function that an algorithm need not be disclosed.[31]

The court in *In re Katz* listed "processing," "receiving," and "storing" as examples of functions that a general-purpose computer may be able to achieve without special programing.[32] This court has determined the function of displaying an icon could likewise be accomplished by a general-purpose computer without special programming.[33]

When disclosure of an algorithm is required, it may be expressed "in any understandable terms including as a mathematical formula, in prose, or as a flow chart, or in any other manner that provides sufficient structure."[34]

Defendant contends several of the disputed terms are invalid as indefinite pursuant to 35 U.S.C. § 112, ¶ 2 which requires the specification to "conclude with one or more claims *particularly pointing out and distinctly claiming* the subject matter which the applicant regards as [the] invention."[35] The Federal Circuit had long held "[o]nly claims 'not amenable to construction' or 'insolubly ambiguous' are indefinite."[36] The Federal Circuit determined:

---

[31] *Ergo Licensing, LLC v. CareFusion 3030, Inc.*, 673 F.3d 1361, 1364-65 (Fed. Cir. 2012) (emphasis added).

[32] *In re Katz*, 639 F.3d at 1316.

[33] *United Video Props., Inc. v. Amazon.com, Inc.*, C.A. No. 11-003-RGA, 2012 WL 2370318, at *11 (D. Del. June 22, 2012).

[34] *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1340 (Fed. Cir. 2008) (internal citation omitted).

[35] 35 U.S.C. § 112, ¶ 2 (emphasis added).

[36] *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1347 (Fed. Cir. 2005), *abrogated by Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120 (2014).

> the definiteness of claim terms depends on whether those terms can be given any reasonable meaning. . . . "If the meaning of the claim term is discernible, even though the task may be formidable and the conclusion may be one over which reasonable persons will disagree, we have held the claim sufficiently clear to avoid invalidity on indefiniteness grounds."[37]

The Supreme Court recently changed the definiteness standard concluding:

> [T]he Federal Circuit's formulation, which tolerates some ambiguous claims but not others, does not satisfy the statute's definiteness requirement. In place of the 'insolubly ambiguous' standard, we hold a patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.[38]

The Court stated the Federal Circuit's "amenable to construction" or "insolubly ambiguous" formulations:

> can breed lower court confusion, for they lack the precision § 112, ¶ 2 demands. It cannot be sufficient that a court can ascribe *some* meaning to a patent's claims; the definiteness inquiry trains on the understanding of a skilled artisan at the time of the patent application, not that of a court viewing matters *post hoc*. To tolerate imprecision just short of that rendering a claim 'insolubly ambiguous' would diminish the definiteness requirement's public-notice function and foster the innovation-discouraging "zone of uncertainty," against which this Court has warned.[39]

The Court explained it "read[s] § 112, ¶ 2 to require that a patent's claims, viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty. The definiteness requirement, so understood, mandates clarity, while recognizing that absolute precision is unattainable."[40]

---

[37] *Id.* (quoting *Exxon Research & Eng'g Co. v. United States*, 265 F.3d 1371, 1375 (Fed. Cir. 2001), *abrogated by Nautilus*, 134 S. Ct. 2120.

[38] *Nautilus*, 134 S. Ct. at 2124.

[39] *Id.* at 2130 (emphasis in original) (internal citation and footnote omitted).

[40] *Id.* at 2129.

Despite the Court's newly enunciated standard for determining indefiniteness, it remains the case that "[t]he party alleging that the specification fails to disclose sufficient corresponding structure must make that showing by clear and convincing evidence."[41] The Federal Circuit has "'noted that typically expert testimony will be necessary in cases involving complex technology.'"[42] Although the *Elcommerce.com* court stated "[w]e do not of course hold that expert testimony will always be needed for every situation," it observed "[w]ithout evidence, ordinarily neither the district court nor this court can decided whether, for a specific function, the description in the specification is adequate from the viewpoint of a person of ordinary skill in the field of the invention."[43]

## IV. CLAIM CONSTRUCTION

The parties have several overarching disputes regarding the claimed inventions that implicate the meaning of a number of disputed claim terms which must be resolved prior to discussion of the individual terms. Defendant argues certain disclosed embodiments are either not claimed and/or were disclaimed during prosecution in distinguishing prior art.

The patent discloses four specific embodiments at Figures 1A, 10, 11, and 13. Figure 1A discloses "a schematic diagram of the of the security system of the present invention as applied to the internet in which an external accessor in a wide area

---

[41] *TecSec, Inc. v. Int'l Bus. Machs. Corp.*, 731 F.3d 1336, 1349 (Fed. Cir. 2013); *see also Datamize*, 417 F.3d at 1348 (noting "the requirement that clear and convincing evidence be shown to invalidate a patent").

[42] *Elcommerce.com, Inc. v. SAP AG*, 745 F.3d 490, 503 (Fed. Cir. 2014) (*vacated on other grounds by* 564 Fed. App'x 599 (Fed. Cir. 2014)) (internal quotation marks omitted) (quoting *Centricut, LLC v. Esab Grp., Inc.*, 390 F.3d 1361, 1370 (Fed. Cir. 2004)).

[43] *Id.* at 506.

network seeks entry into a host system."[44] Figure 10 discloses "a schematic diagram of a second embodiment of the security system of the present invention as applied to the intranet in which an internal accessor in a local area network seeks entry into a restricted portion of the host system."[45] Figure 11 discloses "a schematic diagram of the third embodiment of the security system using as peripheral devices a cellular telephone and a fingerprint module verification device."[46] Figure 13 discloses "a detailed schematic diagram of the fourth embodiment of the security system using as peripheral devices a personal digital assistant (PDA) and the associated fingerprint verification device."[47]

Each of the patents-in-suit incorporate by reference an earlier, now abandoned, application. Plaintiff bases its priority date for the patents-in-suit on the filing date of that abandoned application. Because Figures 11 and 13, and associated descriptions, were not included in the abandoned application, but added later in a continuation-in-part application, defendant argued at the *Markman* hearing that those figures and descriptions should be ignored for purposes of determining the meaning of the disputed claim terms.[48] The court disagrees. The applicable priority date goes to issues of validity with respect to what may be considered prior art. For the issue of claim construction, the court examines the intrinsic record. Because those figures and associated descriptions are part of the intrinsic record, the court rejects defendant's priority date argument as the reason they should be ignored.

---

[44] '599 patent, 4:60-63.
[45] '599 patent, 5:21-24.
[46] '599 patent, 5:25-27.
[47] '599 patent, 5:31-34.
[48] D.I. 123 at 22:19-23:9.

The parties also disagree as to whether a user attempting to access a host computer can have contact with the host computer prior to the user's login verification and authentication by the security computer. According to plaintiff, the claimed invention discloses different embodiments for verifying and authenticating users attempting to access the host computer, using what is called two-factor authentication. Plaintiff states two different forms of user-entered information are required, and two different communication pathways (or "channels") separate the attempt to access from the authentication process.[49] Summarizing the invention, in general terms, the patent states:

> The first step in controlling the incoming access flow is a user authentication provided in response to prompts for a user identification and password. After verification at the security system, the system operating in an out-of-band mode, uses telephone dialup for location authentication and user authentication via a password entered using a telephone keypad.[50]

Defendant maintains the claimed invention isolates a host computer from unauthorized access by intercepting a user's demand to access the host computer by using a separate security computer which performs the login identification verification and user authentication. Defendant argues that only after both steps are completed by the security computer is the user permitted to have any contact with the host computer. Defendant asserts the host computer does not even receive the user's initial demand for access or login identification.[51] Plaintiff disagrees, arguing the claims require

---

[49] D.I. 114 at 1.

[50] '599 patent, 4:10-16.

[51] D.I. 114 at 2; *id.* at 6 ("[Plaintiff's] claims . . . require . . . (i) intercepting a user's login identification and demand to access a host computer, and (ii) preventing the user's contact with the host computer until a separate out-of-band security computer *verifies the login identification and authenticates the user* through an authentication-channel telephone call.") (emphasis added).

preventing the user from gaining access to protected data on (not contacting) the host computer until a separate out-of-band security computer authenticates the user through an authentication channel. Plaintiff contends in all embodiments, the user's computer must, of necessity, initially contact the host computer when trying to access it. After that contact, the host computer sends back a prompt (web) page requesting the user's entry of ID and password. Next, an interception device or control module sends the request for access to the security computer for out-of-band authentication before access is granted to protected data on the host computer. Plaintiff insists the interception device or control module can be on the host computer and that the host computer may perform login identification and password verification, although separate out-of-band authentication of the user must occur before access is granted to protected data on the host computer. According to plaintiff, the separate, out-of-band authentication of the user is the essence of the invention.[52]

The specification indicates the possibility of user contact with the host computer prior to the out-of-band security computer verifying the login identification and authenticating the user via an authentication-channel telephone call, by stating:

> The user requesting access to the host computer from the remote computer is immediately prompted to login at the LOGIN SCREEN PRESENTED BLOCK 152. While the login procedure here comprises the entry of the user identification and password and *is requested by the host computer 34*, such information request is *optionally* a function of the security computer.[53]

---

[52] D.I. 114 at 8.

[53] '599 patent, 9:4-10 (emphasis added). The embodiments of Figures 11 and 13 also shows initial contact with the host computer. The embodiment illustrated in Figure 11 depicts the "user accessing a web application, such as an online banking application, (located on the web server 334[, i.e., host computer]) over the internet 330. The user from a computer 322 accesses the web application over an access channel and enters their USER ID. The web server 334 sends the USER ID to the security system

Plaintiff also points to Figure 10 as an example of initial access to the host computer, and the host computer verifying login information:

> The access network 230 is constructed in such a manner that, when user 224 requests access to *a high security database 232* located at a host computer 234 through computer 222, the request-for-access is diverted by a router 236 internal to the corporate network 238 to out-of-band security network 240. Here the emphasis is upon right-to-know classifications within an organization rather than on avoiding entry by hackers.
>
> Thus, *the accessor is already within the system*, the first level of *verification of login identification and password at the host computer* is the least significant and the authentication of the person seeking access is the most significant. Authentication occurs in the out-of-band security network 240 . . . .[54]

Despite those disclosures, the asserted claims may not cover such instances of initial contact and verification at the host computer.

> Turning to the wide area network of Figure 1A, the specification recites:
>
> The access network 30 is construed in such a manner that, when user 24 requests access to a web page 32 located at host computer or web server 34 through computer 22, the request-for-access is diverted by a router 36 internal to the corporate network 38 to an out-of-band security network 40. Authentication occurs in the out-of-band security network 40 . . . . This is in contradistinction to present authentication processes as the out-of-band security network 40 is isolated from the corporate network 38 and does not depend thereon for validating data.[55]

Thus, the login identification and demand for access is diverted to the security

---

340, also referred to as the centralized out-of-band authentication system (COBAS)." '599 patent, 12:51-57. Similarly, in the embodiment illustrated in Figure 13, "[t]he security system 420 has two distinct and independent channels of operation, namely, the access channel and the authentication channel. The user from a computer 422 accesses the web application over an access channel and enters their USER ID. The web server 334[, i.e., host computer,] sends the USER ID to the security system 440." '599 patent, 12:48-54.

[54] '599 patent, 12:19-32 (emphasis added).

[55] '599 patent, 6:13-23; *see also* '599 patent, 9: 10-12 ("Upon entry of data by user at the ENTRY OF ID AND PASSWORD block 154 the information is passes [sic] to the security computer 40.").

computer.[56] Moreover, the patentee, acting as his own lexicographer told the PTO "[a]n 'out-of-band' operation is defined herein as one conducted *without reference to the host computer or any database in the host network*."[57]

Defendant raises persuasive arguments as to why plaintiff's positions are incorrect. First, in the local area network embodiment of Figure 10, the user is already on the host computer's network and is attempting to access a high security database. The asserted claims are directed to accessing the host computer itself, not "protected data" on the host computer as plaintiff suggests:

> A method for accessing *a host computer* . . . [58]
>
> . . . demand for access to *a host computer* . . .[59]
>
> . . . demand to access *a host computer* . . .[60]
>
> . . . receiving a demand to access *a host computer* . . .[61]
>
> A software method . . . to control access to *a host computer* . . .[62]
>
> . . . demand to access *a host computer* . . .[63]
>
> A security system for accessing *a host computer* . . .[64]

---

[56] At the *Markman* hearing, plaintiff acknowledged this: "[in] the Figure 1 embodiment . . . there's an interception device that routes the user's ID and password to a security computer, and the security computer verifies the first stage login identification." D.I. 123 at 11:3-8.

[57] D.I. 86, Ex. P at SF000657 (emphasis added); *see also* '599 patent, 5:62-66 ("[A]n 'out-of-band' system is defined herein as one having an authentication channel that is separated from the information channel and therefore is nonintrusive as it is carried over separate facilities than those used for actual information transfer."); '599 patent, 1:18-20 ("[A] security network . . . provides user authentication by an out-of-band system that is entirely outside the host computer network being accessed.").

[58] '599 patent, claim 21 (emphasis added).

[59] '599 patent, claim 32 (emphasis added).

[60] '698 patent, claim 1 (emphasis added).

[61] '698 patent, claim 46 (emphasis added).

[62] '698 patent, claim 46 (emphasis added).

[63] '698 patent, claims 53, 54 (emphasis added).

[64] '701 patent, claim 1 (emphasis added).

Plaintiff acknowledges Figure 10 "is different from the Figure 1A embodiment because the accessor . . . is trying to *gain access to protected data* on the host computer *while already on the host computer's network*."[65] The specification specifically distinguishes between "seek[ing] entry into a *host system*"[66] and "seek[ing] entry into a *restricted portion* of the host system."[67] Thus the court determines the relevant asserted claims cover only the Figure 1A embodiment where the user login identification verification and authentication are diverted to the security computer prior to contact with the host computer.[68]

The parties also dispute whether the user's login verification can occur in the access channel. Because the court determined the relevant asserted claims cover only the Figure 1A embodiment, and there is no dispute that in that embodiment such verification occurs in the authentication channel, it follows that verification cannot occur in the access channel.

Finally, the parties disagree over whether the host computer and the security computer must be physically separate, as defendant contends, or the host computer and the security computer may reside on the same hardware, as plaintiff maintains. Plaintiff argues they may reside on the same hardware, while being separated simply through logic or encryption protocols, so long as the security computer's out-of-band authentication occurs through a separate communication channel.[69] As support,

---

[65] D.I. 114 at 10 (emphasis added).
[66] '599 patent, 4:62-63, FIG. 1A (emphasis added).
[67] '599 patent, 5:24, FIG. 10 (emphasis added).
[68] In light of this determination, it is unnecessary to address the parties' arguments as to whether such embodiments were disclaimed during prosecution or the reexamination process.
[69] D.I. 114 at 10.

plaintiff cites Figure 7 and related description. Figure 7 is "a detailed schematic diagram of the software program required for the client/server module of the security system shown in FIG. 3."[70] The court agrees with defendant that the specification's discussion of Figure 7 describes internal protocols used between system modules and does not support the argument that the security computer and the host computer may reside on the same hardware. More importantly, the inventor defined an "out-of-band" system as "one having an authentication channel that is separated from the information channel and therefore is nonintrusive as it is carried over *separate facilities* than those used for actual information transfer."[71] Also, in attempting to overcome an obviousness rejection, the patentee portrayed his patented invention as having a "completely separate authentication channel."[72] Therefore, court again agrees with defendant that the separate devices are in the separate channels.

1. *intercepting* (as a general concept);

   *intercepted* ('599 patent, claims 21, 30, 32);

   *an interception device / a device* ('698 patent, claims 1, 2, 46, 54);

   *an interception device for receiving a login identification originating from an accessor for access to said host computer* ('701 patent, claim 1)

A. **intercepting (as a general concept)**

Plaintiff's proposed construction is: "receiving before access is granted to the host computer."

---

[70] '599 patent, 5:13-15.
[71] '599 patent, 5:62-66 (emphasis added).
[72] D.I. 86, Ex. D at SF000121 ("To add a *completely separate* authentication channel to this 'in-band' system would overly complicate the system . . . .") (emphasis added).

Defendant's proposed construction is: "preventing the host computer from receiving."

The court's determination that the asserted claims cover only the Figure 1A embodiment supports defendant's proposed construction in that the user login information is verified and authenticated before the user can contact the host computer. Intrinsic evidence also supports that construction. Describing Figure 1A, the specification states "the request-for-access [to the host computer] is *diverted* by a router 36 internal to the corporate network 38 to an out-of-band security network 40."[73]

Consequently, the court adopts defendant's proposal and construes "interception" to mean: "preventing the host computer from receiving."

B. **intercepted**

Plaintiff's proposed construction is: "received before access is granted to the host computer."

Defendant's proposed construction is: "prevented from being received by the host computer."

For the reasons stated above, court adopts defendant's proposal and construes "intercepted" to mean: "prevented from being received by the host computer."

C. **an interception device / a device**

Plaintiff's proposed construction is: "a device that receives a request for access before access is granted to the host computer."

---

[73] '599 patent, 6:16-18 (emphasis added). The Abstract similarly recites "[t]he access-seeker initially presents identification and password data over an access channel which is *intercepted and transmitted to the security computer*." '599 patent, Abstract (emphasis added). Plaintiff acknowledges that in the Figure 1A embodiment, "the interception device may divert login identification and demand for access to the security computer." D.I. 114 at 20.

Defendant's proposed construction is: "a device that prevents the host computer from receiving [what the interception device received instead]."

For the reasons stated above, the court adopts defendant's proposal and construes "an interception device / a device" to mean: "a device that prevents the host computer from receiving [what the interception device received instead]."

D. **an interception device for receiving a login identification originating from an accessor for access to said host computer**

Plaintiff argues there is no need to construe this term, disagrees it is a means-plus-function term, and construes "an interception device" as stated above. In the alternative, if the court determines means-plus-function applies, plaintiff states the function, as provided in the claim language, occurs before access is granted to the host computer. It contends the structure includes software, associated hardware, and all equivalents as identified in parties' Amended Joint Claim Construction Chart.[74]

Defendant contends this is a means-plus-function term, with the function: "receiving a login identification originating from an accessor for access to said host computer and preventing the host computer from receiving the login identification." Defendant's proposed structure is: "router 36 (positioned before and separate from the host computer)."

The court determines this is a means-plus-function term. The Federal Circuit "has consistently held that '[m]eans-plus-function claiming applies only to purely functional limitations that do not provide the structure that performs the recited

[74] D.I. 113 at 4-5.

function.'"[75] In considering whether a term receives means-plus-function treatment when that term did not include the word "means," the *Welker* court noted "[t]he generic terms 'mechanism,' 'means,' 'element,' and 'device,' typically do not connote sufficiently definite structure [to avoid means-plus-function treatment]. . . . *The term 'mechanism' standing alone connotes no more structure than the term 'means.'*"[76] Here, the term "device" standing alone connotes no more structure than the term "means." The term recites a function without reciting sufficient structure for performing that function.

**Function**

Defendant's proposed function is "receiving a login identification originating from an accessor for access to said host computer and preventing the host computer from receiving the login identification." Plaintiff agrees with that function excluding "and preventing the host computer from receiving the login identification." For consistency with the court's constructions of the other "intercepting" terms, defendant's proposed function is adopted.

**Structure**

The court also adopts defendant's proposed structure, "router 36 (positioned before and separate from the host computer)."[77] Describing Figure 1A, the specification states "[t]he access network 30 is constructed in such a manner that when user 24

---

[75] *Welker Bearing Co. v. PHD, Inc.*, 550 F.3d 1090, 1095 (Fed. Cir. 2008) (quoting *Phillips v. AWH Corp.*, 415 F.3d 1303, 1311 (Fed. Cir. 2005)).

[76] *Id.* at 1096 (Fed. Cir. 2008) (alterations and emphasis in original) (quoting *Massachusetts Institute of Tech. v. Abacus Software*, 462 F.3d 1344, 1354 (Fed. Cir. 2006)).

[77] The inclusion of the parenthetical is appropriate based on the prior determination that users cannot contact the host computer until after the security computer verified and authenticated the user. In Figure 1A, router 36, although part of corporate network 38, is illustrated as being a separate device, whereas the unclaimed embodiment of Figure 10 does not illustrate router 236, indicating the router could be integral to the host computer in that embodiment.

requests access to a web page 32 located at a host computer or web server 34 through computer 22, the request-for-access is *diverted by a router 36* internal to the corporate network 38 to an out-of-band security network 40."[78]

2. *access channel / first channel* ('599 patent, claims 21, 32; '698 patent, claims 46, 48; '701 patent, claim 1);

*authentication channel / second channel* ('599 patent, claims 21, 28, 32; '698 patent, claims 1, 46, 47, 48, 50, 54; '701 patent, claims 1, 8)

A. **access channel / first channel**

Plaintiff's proposed construction is: "a communication channel separate from the authentication channel."

Defendant's proposed construction is: "an information channel that is separate from and does not share any facilities with the authentication channel."

The parties agree that the access/first channel are separate, however, defendant's proposed construction clarifies that the channels cannot share any facilities to send or receive information or merge into a common network. That construction is consistent with the court's determination that the separate host and security computers are in separate channels and the inventor's definition of an "out-of-band" system as "one having an authentication channel that is separated from the information channel and therefore is nonintrusive as it is carried over *separate facilities* than those used for actual information transfer."[79]

---

[78] '599 patent, 6:13-18 (emphasis added).

[79] '599 patent, 5:62-66 (emphasis added). Plaintiff contends "[t]he specification itself . . . requir[ers] only that the communications of the respective channels be "carried over separate facilities, **frequency channels, or time slots**." D.I. 114 at 26 (emphasis in original) (citing '599 patent, 2:63-64). That statement, however, was made in a discussion of *other patents* the patentee reviewed "in preparing for this application." *See* '599 patent, 2:36-65. When the patentee defined the "out-of-band" system of the patent, he did not include the "frequency channels, or time slots" plaintiff emphasizes in its briefing. The

Therefore, the court adopts defendant's proposal and construes "access channel / first channel" to mean: "an information channel that is separate from and does not share any facilities with the authentication channel."

B. **authentication channel / second channel**[80]

Plaintiff's proposed construction is: "a communication channel separate from the access channel."

Defendant's proposed construction is: "a channel for performing authentication that is separate from and does not share any facilities with the access channel."

For the same reasons for adopting defendant's proposed construction of "access channel / first channel," the court adopts defendant's proposed construction of "authentication channel / second channel": "a channel for performing authentication that is separate from and does not share any facilities with the access channel."

3. *security computer* ('599 patent, claims 21, 32; '698 patent, claims 1, 2, 46, 48, 54; '701 patent, claims 1, 7);

*host computer* ('599 patent, claims 21, 28, 32; '698 patent, claims 1, 46, 48, 54; '701 patent, claims 1, 7)

A. **security computer**

Plaintiff's proposed construction is: "a computer having software for performing the steps leading to the granting or denying of access to a host computer."

---

court also notes that in the Statement of Reasons for Patentability and/or Confirmation, the PTO stated "Woodhill discloses a system that involves accessing a host computer in a first channel and then authenticating in a separate channel, but *both access and authentication merge in the same network* (like the internet) . . . . Woodhill at least does not disclose 'wherein said security computer outputs an instruction to the host computer to either grant access thereto using said access channel or to deny access thereto.'" D.I. 86, Ex. W at SF001026 (emphasis added).

[80] References to "side channel," "out-of-band channel," and "second channel" are synonymous with the "authentication channel." D.I. 113 at 5.

Defendant's proposed construction is: "a computer in the authentication channel that can grant authenticated users access to but is isolated from the host computer."

Defendant's proposed construction is consistent with the court's determination that the security computer and the host computer are physically separate and that the security computer performs user verification and authentication before the user is able to access the host computer. The security computer is located in the authentication channel. The "invention relates to security networks for computer network applications, and more particularly, to a *security network* which provides *user authentication* by an *out-of-band system that is entirely outside the host computer network being accessed*."[81] Therefore, defendant's proposed construction of "security computer" is adopted.

B. **host computer**

Plaintiff's proposed construction is: "a computer which the accessor is attempting to gain access."

Defendant's proposed construction is: "a computer to which the accessor is attempting to gain access, but which no information from an accessor is allowed to enter unless access is granted by the security computer."

The parties agree that a "host computer" is "a computer which the accessor is attempting to gain access." The court determined that the user has no contact with the host computer until his login information has been verified and authenticated. Therefore, defendant's proposed construction of "host computer" is adopted.

---

[81] '599 patent, 1:16-20 (emphasis added).

4. *a multichannel security system / an out-of-band computer security system / a security system* ('599 patent claim 32; '698 patent, claims 1, 46, 48, 54; '701 patent, claim 1)

These terms are each preamble terms. Plaintiff contends they are not limiting and, thus, need no construction. In the alternative, should the court find the preambles limiting, plaintiff's proposed construction for each term is: "a system having an authentication channel separate from an access channel."

Defendant's proposed construction is: "a system that operates without reference to a host computer or any database in a network that includes the host computer."

"In general, a preamble limits the [claimed] invention if it recites essential structure or steps, or if it is 'necessary to give life, meaning, and vitality' to the claim."[82] Plaintiff argues the preambles are not limiting because they only state a use and/or purpose of the claimed invention. Plaintiff maintains the preambles do not recite structural limitations beyond those in the claim elements, and none provide antecedent basis "'necessary to give life, meaning, and vitality'" to the claim elements.[83]

The Federal Circuit, however, has found "clear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the preamble into a claim limitation because such reliance indicates use of the preamble to define, in part, the claimed invention."[84] It is plaintiff's purported reliance on the

---

[82] *Eaton Corp. v. Rockwell Int'l Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003) (alteration in original) (quoting *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002)).

[83] D.I. 114 at 40 (quoting *Pitnety Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999)).

[84] *Catalina Mktg.*, 289 F.3d at 808; *see also, Storage Tech. Corp. v. Cisco Sys.*, 329 F.3d 823,835 (Fed. Cir. 2003) (finding support for the district court's determination that the "forwarding device" of the preambles was limiting, in part, because the applicants relied on the existence of a "forwarding device" in distinguishing their invention over prior art) (citing *Catalina Mktg.*, 289 F.3d at 808).

disputed terms, and the express definition of "out-of-band" system, during prosecution to distinguish prior art on which defendant bases its arguments.

The court agrees with defendant that the disputed preambles are limiting as the patentee acted as his own lexicographer in defining an "out-of-band" operation and relied on that definition in distinguishing prior art. The court has previously determined the security system operates without reference to a host computer or any database in a network that includes the host computer. In response to an office action the applicant stated: "[b]efore proceeding further, the matters of in-band/out-of-band definitions and distinction are addressed. There is a maxim in patent law, which arose long after dictionaries were compiled, that an Applicant is his own lexicographer."[85] In a former office action response, the specification was amended to add the applicant's definition: "[a]n 'out-of-band' operation is defined herein as one conducted without reference to the host computer or any database in the host network."[86] The applicant then relied on the claimed "out-of-band" operation to distinguish U.S. Patent No. 5,153,918 to Tuai, which disclosed a single, "in-band," system. "This Amendment by reference incorporates herein each and every passage of Tuai '918 cited by the Examiner as if set forth at length. In Tuai '918, there is no *inband/out-of-band distinction* as the precess takes place totally in-band."[87] "Not only does Tuai '918 lack the distinct

[85] D.I. 86, Ex. P at SF000711.

[86] *Id.*, Ex. O at SF000657 (underlining in original); *see also* '599 patent, 5:62-66 ("[A]n 'out-of-band' system is defined herein as having an authentication channel that is separated from the information channel and therefore is nonintrusive as it is carried over separate facilities than those used for actual information transfer."); '599 patent, 6:20-23 (In the claimed invention "the out-of-band security network 40 is isolated from the corporate network 38 and *does not depend thereon for validating data*.") (emphasis added).

[87] *Id.*, Ex. O at SF000658-59 (emphasis added).

channels of the Applicant, but *the patent teaches away from out-of-band operation*."[88] "Tuai '918 teaches away from Applicant by stating that the controller 15 is interconnected between the host computer 10 and the modem 12. This defines an in-band system that is *antithetical to Applicant's system which is defined as out-of-band*."[89] "Once again, it is respectfully urged that, while both the reference and the Applicant utilize voice verification techniques, the practices are significantly different from a security perspective and especially so when the *in-band/out-of-band aspect is considered*."[90] In a subsequent office action response, the applicant reiterated, with respect to Tuai "while both the reference and the Applicant utilize voice verification techniques, the practices are significantly different from a security perspective and especially so when the in-band/out-of-band aspect is considered. Thus, when read in context, these are not equivalent."[91]

> During re-examination, in summarizing the pending claims, plaintiff stated:
>
> The Order for *ex parte* reexamination relates to claims 1-34 of U.S. Patent No. 7,870,599 ("the '599 patent"). Claims 1, 11, 18, 21, and 32 and independent claims, each of which is directed to an *"out-of-band" or "multichannel"* computer security system for authenticating a user prior to granting the user access to a host computer.
>
> Briefly, the '599 patent describes an *"out-of-band" network security system* having an authentication channel that is separated from an information (i.e., "access") channel . . . .[92]

In distinguishing U.S. Patent No. 6,016,476 to Maes, plaintiff stressed the out-of-band process of the invention: "[t]hus, in the Maes system, there is no log-on access control

---

[88] *Id.*, Ex. O at SF000659 (emphasis added).
[89] *Id.*, Ex. O at SF000660 (emphasis added).
[90] *Id.*, Ex. O at FSF000664 (emphasis added).
[91] *Id.*, Ex. P at SF0000717-18 (underlining in original).
[92] *Id.*, Ex. U at SF000994 (emphasis added).

to a host computer. Moreover, in Maes, the Universal Card is authenticated with the PDA in the access channel, whereas in the rejected claims, the authentication is via an *out-of-band authentication network* . . . ."[93]

Because the patentee acted as his own lexicographer in defining an "out-of-band" operation and relied on that definition in distinguishing prior art, the court finds these preamble terms limiting, and consistent with the court's construction of other terms, adopts defendant's proposal and construes these terms to mean: "a system that operates without reference to a host computer or any database in a network that includes the host computer."

5. *verifying the login identification* ('698 patent, claim 1)

Plaintiff contends construction of this term is unnecessary and plain and ordinary meaning should be applied. In the alternative, its proposed construction is: "confirming that the information used by an accessor to log in is valid."

Defendant's proposed construction is: "confirming at the security computer that the information used by an accessor to login to the host computer is valid."

The parties agree that the proper construction at least includes "confirming . . . that the information used by an accessor to login . . . is valid." Defendant's proposed construction requires for confirmation to occur at the security computer. The court has already determined that is the case.

In the claimed embodiment of Figure 1A, "when user 24 requests access to a

---

[93] *Id.*, Ex. U at SF001006 (emphasis added). Moreover, in the Statement of Reasons for Patentability and/or Confirmation, the PTO refers to the invention as "generally relat[ing] to security networks for computer network applications, and more particularly, to a security network which provides user authentication by an *out-of-band system that is entirely outside the host computer network being accessed*." *Id.*, Ex. W at SF001025 (emphasis added).

web page 32 located at a host computer or web server 34 through computer 22, the request-for-access is *diverted* by a router 36 internal to the corporate network 38 *to an out-of-band security network 40*."[94] The summary of the invention indicates verification occurs at the security system: "[a]fter verification *at the security system*, the system operating in an out-of-band mode" authenticates the user.[95] Figures 9A through 9E illustrate the "software operation *of the out-of-band security system 40* from the receipt of a request-to-access inquiry to granting-of-access or denial-of-access."[96] The verification portion of that software operation, of the out-of-band security system 40, is then described in column 9 from lines 13 through 46.

The court, therefore, adopts defendant's proposal and construes "verifying the login identification" to mean: "confirming at the security computer that the information used by an accessor to login to the host computer is valid."

6. *subscriber database / a database* ('598 patent, claims 21, 32; '698 patent, claims 46, 48; '701 patent, claim 1)

Plaintiff contends these terms do not require construction and should be given their plain and ordinary meaning. In the alternative, its proposed construction is: "subscriber records / records."

Defendant's proposed construction is: "a database in the authentication channel that maintains subscriber contact information for contacting accessors."

Defendant frames the parties' dispute here as whether the subscriber database resides in the authentication channel and whether the subscriber database maintains at

---

[94] '599 patent, 6:14-18 (emphasis added).
[95] '599 patent, 4:13-16 (emphasis added).
[96] '599 patent, 8:61-63 (emphasis added).

least user-contact information.[97] The court agrees with defendant's proposed construction.

The "out-of-band security network 40 is *isolated from the corporate network* 38 and does not depend thereon for validating data."[98] Again, during prosecution, the applicant stated "[a]n 'out-of-band' operation is defined herein as one conducted *without reference to the host computer or any database in the host network*."[99] The specification describes this out-of-band operation. Figure 2 illustrates "the hardware required by the out-of-band security network for computer network applications of this invention," with the security computer identified as "52."[100] "The computer 52 is adapted to include software programs . . . for receiving the user identification and for validating the corresponding password, and is further adapted to obtain *the user telephone number* from lookup tables within database 54 . . . ."[101] Figures 3 through 8 illustrate the software architecture for that security network.[102] "The security computer 52, FIG. 2, is structured *to include* various software modules, FIG. 3, namely, . . . a *database module 72*."[103] Figure 8 illustrates "SUBSCRIBER DATABASE 126" as part of database module 72. The specification describes Figure 8 as showing "the software program required for the database module 72 *of the out-of-band security system 40* of this invention."[104] The databases of module 72 are "the audit database 124 for the call

---

[97] D.I. 114 at 51.
[98] '599 patent, 6:21-23 (emphasis added).
[99] D.I. 86, Ex. O at SF000657 (emphasis added).
[100] '599 patent, 6:36-38.
[101] '599 patent, 6:42-46 (emphasis added).
[102] '599 patent, 6:54-55.
[103] '599 patent, 6:55-60 (emphasis added).
[104] '599 patent, 8:28-30 (emphasis added).

records; *the subscriber database 126 for subscriber information* . . . ."[105] Therefore, the subscriber database resides within the out-of-band security system which is located in the authentication channel. The subscriber database also must contain some subscriber contact information in order to contact and authenticate the subscriber/user. The specification supports that requirement: "[t]he control module 62 queries the subscriber database 126 and retrieves therefrom *the telephone number associated with the login identification*."[106]

Plaintiff cites claim 32 of the '599 patent as demonstrating the subscriber database does not have to be in the authentication channel as that claim recites "subscriber database" in a separate clause from "security computer": "a subscriber database *addressable by the security computer* having at least one telephone number corresponding to the intercepted login identification."[107] Plaintiff argues that the subscriber database only being required to be *addressable* by the security computer means the subscriber database does not have to be stored in the security computer or necessarily be in the authentication channel.[108] The court is unconvinced.

Claim 32 concerns "[a]n *out-of-band computer security system* comprising: a security computer . . . ; a subscriber database addressable by the security computer . . . ."[109] Although the specification seemingly interchanges "security computer," "security system," and "security network," this claim points to a slight distinction, at least between security system/network and security computer, the latter being a subset of the

---

[105] '599 patent, 8:46-48 (emphasis added).
[106] '599 patent, 10:1-3 (emphasis added).
[107] '599 patent, claim 32 (emphasis added).
[108] D.I. 114 at 52.
[109] '599 patent, claim 32.

former. With that understanding, the "out-of-band security *system*" of claim 32 includes a security *computer* and an accessible subscriber database. The court has previously determined the out-of-band security system is in the authentication channel, as illustrated by the security network 40 in Figure 1A. Additionally, the subscriber database element requiring the database "hav[e] at least one telephone number corresponding to the intercepted login identification," supports defendant's position that *some* subscriber contact information, though not necessarily a telephone number, must be contained in the subscriber database for the system to contact and authenticate the subscriber/user.

Consequently, the court adopts defendant's proposal and construes "a subscriber database / a database" to mean: "a database in the authentication channel that maintains subscriber contact information for contacting accessors."

7. *demand from an accessor / demand for access / access demand[s] / demand from said accessor / demand to access / a demand* ("the Demand Terms") ('599 patent, claims 30, 32; '698 patent, claims 46, 54; '701 patent, claim 1)

Plaintiff contends no construction of these terms is needed and should be given their plain and ordinary meaning. In the alternative, its proposed construction is: "a request for access by an accessor."

Defendant's proposed construction is: "a request to access the host computer that was sent from an accessor."

The parties agree "demand" means "request" and that "access" means "access" and that this access request is made by an "accessor." Plaintiff states the claims link "a demand" or "demand for access" to "from an accessor for access to said host computer," and therefore reading "the host computer" language into the meaning of the

"Demand Terms" is superfluous and unnecessary.[110] Plaintiff notes defendant does not dispute "the demand for access is a request to access the host computer and the protected media thereon."[111] Defendant agrees that the demand to access is a demand to access the host computer itself as the asserted claims expressly recite. It disagrees that the demand can be to access "protected media" on the host computer.[112] The court has previously determined the claims are directed to accessing a host computer, not protected media thereon. To avoid any future assertion that the claims are directed at access to protected media, rather than access to the host computer itself, and for consistency with its other constructions, the court adopts defendant's proposal and construes the "Demand Terms" to mean: "a request to access the host computer that was sent from an accessor."

8. *control module* ('599 patent, claim 21)

Plaintiff contends there is no need to construe this term and it should be given its plain and ordinary meaning. In the alternative, its proposed construction is: "software and associated hardware."

Defendant's proposed construction is: "software of the security computer that incorporates a finite state machine, a call state model, process monitors, and fail-over mechanisms to interconnect with the other modules to control processing flow and interfacing with the internal and external system components."

Plaintiff contends this term should be given its plain and ordinary meaning, citing

---

[110] D.I. 114 at 54 (citing '599 patent, claim 1, 14:10-11).
[111] *Id.* at 55.
[112] *Id.* at 56.

to the declaration of its expert, Alan T. Sherman, Ph.D., who states "[i]t is my opinion that a skilled artisan would readily recognize 'a control module' as a term of art meaning a logically separable part of a computer program that controls the execution of other computer programs and regulates the flow of work in a computer system."[113] In support of the purported term of art meaning, Sherman cites the IEEE Standard Computer Dictionary, apparently arriving at his definition by combining the definitions of three terms: "control program," "module," and "supervisory program."[114] Defendant's expert, Avi Rubin, Ph.D. disagrees, stating "[o]rdinary skilled artisans would not recognize the term *control module* as a term of art."[115] With no agreement that "control module" is a term of art, and with plaintiff's proposal based on a combination of the definitions of multiple terms, the court rejects plaintiff's suggestion that no construction is necessary. The court also agrees with defendant that plaintiff's alternative construction, "software and associated hardware," does not provide sufficient specificity to the claim term.

The specification provides an understanding of the claim term and support for defendant's proposed construction. As with the "subscriber database" term, "[t]he *security computer 52*, FIG. 2, is structured *to include* various software modules, FIG. 3, namely, *a control module 62* . . . ."[116] "As will be understood from the flow diagram description, . . . the *control module 62* software *of the security computer 52* incorporates *a finite state machine, a call state model, process monitors, and fail over mechanisms*."[117] "The *control module 62* functions and *interconnects with the other*

---

[113] D.I. 114, Ex. B at ¶ 43.
[114] *Id.*, Ex. B at ¶ 43, Ex. 17.
[115] *Id.*, Ex. A at ¶ 76.
[116] '599 patent, 6:55-57 (emphasis added).
[117] '599 patent, 6:66-7:2 (emphasis added).

*modules* (line, speech, administration, client/server and database modules) *to control the processing flow and the interfacing with the internal and external system components*."[118]

In light of such specification support, the court adopts defendant's proposal and construes "control module" to mean: "software of the security computer that incorporates a finite state machine, a call state model, process monitors, and fail-over mechanisms to interconnect with the other modules to control processing flow and interfacing with the internal and external system components."

9. *re-enter predetermined data* ('599 patent, claims 21, 32);

*retransmit predetermined data* ('599 patent, claims 21, 32)

A. **re-enter predetermined data**

Plaintiff contends there is no need to construe this term and it should be given its plain and ordinary meaning. In the alternative, its proposed construction is: "enter previously specified data."

Defendant's proposed construction is: "enter again predetermined data that a user initially entered."

Claim 32 of the '599 patent includes "prompt means for outputting a second instruction at the telephonic device to *re-enter* predetermined data at and retransmit predetermined data from the telephonic device."[119]

Defendant contends the dispute is whether "re" matters and plaintiff seeks to render "re" meaningless; its proposed construction is to "enter" or "transmit" data, which

[118] '599 patent, 6:60-65 (emphasis added).
[119] '599 patent, claim 32 (emphasis added).

ignores the "re" requiring whoever initially entered or transmitted the "predetermined data" to do so again. It states the original entering or transmitting would happen during an enrollment process: "the SV[, speech verification,] processing unit 88 enables the enrollment of users with the speech password and the interaction of the speech database of database module 72";[120] "the fingerprint processing unit 388 enables the enrollment of users fingerprint and the interaction of the fingerprint database of the COBAS device 340."[121] Defendant further supports its position that whoever initially entered or transmitted the "predetermined data" is required to do so again with the specification's statement that "[t]he *user 24*, who has previously had *his* biometric sample, namely the speech pattern, registered with the speech database 128 . . ."[122]

The court disagrees that the previous citation requires the user to be solely responsible for both entering and transmitting enrollment data, and then re-entering and retransmitting that predetermined data. The intrinsic record includes no such requirement; it merely states the user previously had his biometric sample registered, not that the user himself is solely responsible for that registration. As plaintiff emphasizes, the previously specified data could be entered into storage by someone other than the user who is associated with the out-of-band authentication network, e.g., a network administrator, or the data could be pulled into the system automatically from other networked devices. Plaintiff insists all that is required for re-entering data is

[120] '599 patent, 7:43-45.
[121] '599 patent, 13:12-15.
[122] '599 patent, 11:3-5 (emphasis added).

preexisting knowledge of that data.[123] The court agrees.[124]

Therefore, the court adopts plaintiff's proposal and construes "re-enter predetermined data" to mean: "enter previously specified data."

B. **retransmit predetermined data**

Plaintiff contends construing this term is unnecessary and it should be given its plain and ordinary meaning. In the alternative, plaintiff's proposed construction is: "transmit previously specified data."

Defendant's proposed construction is: "transmit again predetermined data that a user initially transmitted."

For the same reasons discussed in connection with "re-enter predetermined data," the court adopts plaintiff's proposal and construes "retransmit predetermined data" to mean: "transmit previously specified data."

10. *comparator means in said security computer for authenticating the access demand in response to the retransmission of the predetermined data from the telephonic device* ('599 patent, claim 32)

Plaintiff's proposed function is: "authenticating the access demand in response to the retransmission of the predetermined data from the telephonic device." It contends the structure includes software, associated hardware, and all equivalents as identified in the Amended Joint Claim Construction Chart.[125]

---

[123] D.I. 114 at 60.

[124] Defendant also notes claim 1 of the '701 patent recites "a prompt mechanism for instructing said accessor to *enter* predetermined data at and *transmit* said predetermined data from said peripheral device," and claim 47 of the '698 patent recites "further comprising outputting to the peripheral device over the authentication channels a prompt to *enter* the predetermined data." (emphases added). The court is unconvinced that similar claim language from different patents mandates that the asserted claims of the '599 patent be limited as suggested by defendant, particularly since the common specification contains no such limitation.

[125] D.I. 113 at 13-14.

Defendant's proposed function is: "authenticating the access demand in response to retransmission of the predetermined data from the telephonic device." It argues this term is indefinite for lack of sufficient structural disclosure because the specification does not disclose any algorithm for the security computer to perform the function associated with this limitation or, in the alternative, does not adequately disclose an algorithm for the security computer to perform such function.

**Function**

The parties agree that the function of the "comparator means" is "authenticating the access demand in response to the retransmission of the predetermined data from the telephonic device." The court adopts that function.

**Structure**

Defendant maintains this term requires authenticating "access demands" but the specification is silent on *how* to authenticate access demands. It argues ordinary skilled artisans would understand the specification does not disclose any algorithm for authenticating access demands and, thus, this term is invalid.

Defendant maintains several terms are indefinite for failure to disclose an algorithm showing how to do certain tasks. Plaintiff, however, argues it does not claim the generic algorithm for performing the specified tasks, such as comparing one piece of data to another: rather, it claims the comparator means as it interacts with the broader system. It asserts there is sufficient disclosure of such an algorithm.[126]

"Claim definiteness . . . depends on the skill level of a person of ordinary skill in

[126] D.I. 114 at 65.

the art. In software cases, therefore, algorithms in the specification need only disclose adequate defining structure to render the bounds of the claim understandable to one of ordinary skill in the art."[127] In *AllVoice*, the Federal Circuit disagreed that a term was indefinite for failure to disclose sufficient algorithm where the disclosed algorithm could be implemented using third-party software. "[The expert's] statement set forth several straightforward ways that the algorithm represented in Figure 8A could be implemented by one skilled in the art using well-known features of the Windows operating system . . . ."[128] The expert concluded "'[a] person skilled in the art reading the '273 specification would know that any of these techniques could be used to determine the position of a recognized word in the third party application, would know the software to use and how to implement it.'"[129]

Here, plaintiff's expert Sherman asserts:

> The concept of comparing one piece of data to another is one of the most fundamental concepts in computer science. The action of comparing data in a computer is the most basic of functions, one clear to even those with the most basic understanding of computer software. . . . Indeed, in a patent from 1999, "a comparator means" is specifically described in a biometric concept. Teitelbaum, U.S. Pat. No. 5,872,834.[130]

Sherman opines "that an ordinary skilled artisan would find ample disclosure in the specification supporting an algorithm with the steps of comparing inputted passwords and biometric data with store parameters, and returning a signal based on the results of

---

[127] *AllVoice Computing PLC v. Nuance Commc'ns, Inc.*, 504 F.3d 1236, 1245 (Fed. Cir. 2007) (citations omitted).

[128] *Id.*

[129] *Id.* at 1246 (alteration in original); *see also Medical Instrumentation & Diagnostics Corp. v. Elekta AB*, 344 F.3d 1205, 1214 (Fed. Cir. 2003) ("[H]ere there would be no need for a disclosure of the specific program code if software were linked to the converting function and one skilled in the art would know the kind of program to use.").

[130] D.I. 114, Ex. B at ¶ 35.

that comparison in order to authenticate access demand."[131]

Moreover, the inventor stated to the PTO that third-party software was used in conjunction with his invention.

> The server ran the security system software which had its *main program* written by me in Visual Basic and C++. The *main program* also used third party software libraries from VBVoice (to communicate with the Dialogic card) and Nuance (to perform speech recognition and verification). The *main program* also communicated with a Microsoft Access database software (located on the same server) which stored the user profile and system configuration databases. The announcement database was a part of VBVoice and the speech verification database was a part of Nuance.[132]

Finally, in the Notice of Allowance involving reexamination of the '599 patent, issued following Board review of plaintiff's appeal brief for the '599 Application, the Patent Office stated:

> The Examiner *has found proper support for the means plus function language* of the limitations of claims 1, 7, 9, 11, 16, 18, 30, and 32-34: interception means in at least [0052-0053] of the specification, prompt means in at least [0056-0058] of the specification, *comparator means* in at least [0057], authentication program means in at least [0072] of the specification, sampling means in at least [0041], voice sampling means and voice recognition means in at least [0039-0041] of the specifications.[133]

Therefore, the court finds defendant has not demonstrated by clear and convincing evidence the absence of a sufficient algorithm to perform the claimed function[134] and adopts plaintiff's algorithm, as presented at the *Markman* hearing:[135]

---

[131] *Id.*, Ex. B at ¶ 38.

[132] D.I. 86, Ex. S at SF000951 (emphasis added).

[133] *Id.*, Ex. Z at SF000467 (emphasis added).

[134] The court also rejects defendant's argument that the comparator means authenticates only the access demand, not the accessor. Sherman states defendant's expert Rubin "does not explain how a comparator means could possibly authenticate an access demand, including the user's credentials, without authenticating the user. It is not possible. Any comparator means that authenticates user credentials must authenticate the user herself, since both are inextricably linked. . . . [T]he 'wherein' clause of claim 32 of the '599 Patent cited by Dr. Rubin in paragraph 50 refers to a signal from the security computer to the host computer that the user's access rights have been confirmed. This refers to the

'599 patent, FIG. 9C, steps 186-196, 10:23-42 and/or '599 patent, FIGs. 9C-9D, steps 200-208, 11:1-31.

11. *biometric analyzer . . . for analyzing a monitored parameter of [said] / [the] accessor* ('599 patent, claim 28; '701 patent, claim 7)

Plaintiff argues this is not a means-plus-function term and no construction is necessary. If the term is construed, it proposes: "a program that extracts relevant data from a biometric sample and compares the data with that stored for the user." If means-plus-function applies, plaintiff's proposed function is: "extracting relevant data from a biometric sample and comparing the data with that stored for the user." It contends the structure includes software, associated hardware, and all equivalents as identified in the Amended Joint Claim Construction Chart.

Defendant contends this is a means-plus-function term because it is purely functional, and the appropriate structure is an algorithm. Its proposed function is: "analyzing a monitored parameter of an accessor." It contends this term is indefinite for failure to disclose an algorithm to perform the function.[136]

The parties' experts disagree as to whether the term "biometric analyzer" would have an understood meaning to ordinary skilled artisans.[137] Absent such agreement, or

---

conclusion of the second stage, out-of-band authentication. This feature does not preclude, but indeed requires, that the user and her credentials pass through first stage verification. I am therefore of the opinion that an ordinary skilled artisan would find ample disclosure in the specification supporting an algorithm with the steps of comparing inputted passwords and biometric data with stored parameters, and returning a signal based on the results of that comparison in order to authenticate an access demand." D.I. 114, Ex. B at ¶ 38.

[135] D.I. 123 at 94:11-21, 105:7-17.

[136] Defendant also argues the term is indefinite under a *Nautilus* analysis if the court determines it is not subject to means-plus-function treatment. D.I. 123 at 70:13-71:2, 73:9-21. Because the court determines the term is subject to means-plus-function treatment, that argument is not addressed.

[137] D.I. 114, Ex. A at ¶ 31(Rubin asserts "'biometric analyzer' is not a term that had a generally understood structural meaning in the art in 2000 or 2004 and does not recite structure to perform the corresponding function."), *id.*, Ex. B at ¶¶ 26-27 (Sherman asserts "'biometric analyzer' was a term of art

a specific definition in the specification, the court agrees with defendant that this term is purely functional and subject to mean-plus-function treatment.

**Function**

In the Amended Joint Claim Construction Chart, plaintiff stated, if determined to be a means-plus-function term, the function was "as stated in the claim language."[138] At the *Markman* hearing, plaintiff maintained the claimed function is "extracting relevant data from a biometric sample and comparing the data with that stored for the user."[139] That definition is taken from Sherman's expert report opinion on the understanding of biometric analyzer by skilled artisans in 2000 and cites two unrelated patents as support.[140] Rather than rely on that definition based on extrinsic evidence, and in light of plaintiff's original assertion that the function was "as stated in the claim language," the court adopts defendant's proposed function: "analyzing a monitored parameter of the accessor."

**Structure**

The specification states "[w]hile voice recognition is used herein, it is merely exemplary of the many forms of recognizing or identifying an individual person. Others include, iris recognition, retina identification, palms recognition, and face recognition."[141] At the *Markman* hearing, plaintiff presented an algorithm from the specification immediately following that language as carrying out the claimed function should means-

---

and was well understood by skilled artisans in 2000 as denoting a program that extracts relevant data from a biometric sample and compares the data with that stored for the user.").

[138] D.I. 113 at 15.

[139] D.I. 123 at 79:3-13.

[140] D.I. 114, Ex. B at ¶ 26.

[141] '599 patent, 6:25-29.

plus-function be applied: "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor."[142]

Defendant argues the proposed algorithm is insufficient because the specification does not described *how* to do any comparing.[143] Plaintiff again relies on the determination in *AllVoice* that algorithms are not required for well-known, widely available, third-party software that could be employed to implement the algorithm disclosed in the specification.[144]

Although Rubin disagrees, Sherman states biometric analyzers, and how to conduct biometric analysis, were well known in the art in 2000.[145] Sherman points to the same specification citation plaintiff relied on at the *Markman* hearing as supporting its proposed algorithm for his opinion that "[b]ased on the intrinsic evidence, . . . an ordinary skill artisan would readily understand what is meant by 'biometric analyzer' from both a structural and functional standpoint."[146] The inventor told the PTO he wrote the main, controlling, program but "used third-party software libraries from . . . Nuance (to perform speech recognition and verification)."[147]

Therefore, the court finds defendant has not shown by clear and convincing

---

[142] D.I. 123 at 67:21-68:6, 77:11-24 (citing '599 patent, 6:29-35).
[143] *Id.* at 68:9-22.
[144] *Id.* at 79:18-80:4.
[145] D.I. 114, Ex. B at ¶¶ 26-27.
[146] *Id.*, Ex. B at ¶ 27.
[147] D.I. 86, Ex. S at SF000951; *see also* D.I. 114, Ex. B at ¶ 29 (Sherman stated, "it is my understanding that the inventor actually reduced the system to practice and demonstrated it in October of 1998 . . ., using commercially available off-the-shelf software for biometric analysis."). The inventor's representation to the PTO during the reexamination process that he wrote a main program which required implementation of third-party software counters defendant's reliance on statements made to the PTO in response to an office action which it contends shows claiming the actual algorithm used for voice verification. D.I. 114 at 66 (quoting D.I. 86, Ex. F at SF000201 (distinguishing the *Picket* reference)).

evidence that an ordinary skilled artisan would fail to understand the bounds of the invention and adopts plaintiff's algorithm, as presented at the *Markman* hearing: "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor," '599 patent, 6:29-35.

12. *a component for receiving the transmitted data and comparing said transmitted data to predetermined data, such that, depending on the comparison of the transmitted and the predetermined data, said security computer outputs an instruction to the host computer to grant access to the host computer or deny access thereto* ('698 patent, claim 54)

Plaintiff argues this is not a means-plus-function term and no construction is necessary. If a construction is needed, it proposes: "component" means: "software and associated hardware." If means-plus-function applies, its proposed function is: "receiving the transmitted data and comparing said transmitted data to predetermined data." Plaintiff contends the structure includes software, associated hardware, and all equivalents as identified in the Amended Joint Claim Construction Chart.

Defendant's proposed function is: "receiving the transmitted data and comparing said transmitted data to predetermined data, such that, depending on the comparison of the transmitted and the predetermined data, said security computer outputs an instruction to the host computer to grant access to the host computer or deny access thereto." Defendant contends this term is indefinite for failure to disclose an algorithm to perform the function.

The court agrees with defendant that "component for receiving . . ." is synonymous with "means for receiving . . . ." As the term recites a function without reciting sufficient structure for performing that function it will be construed as a means-

plus-function term.

**Function**

The parties proposed functions each include "receiving the transmitted data and comparing said transmitted data to predetermined data." Defendant contends the function also includes "such that, depending on the comparison of the transmitted and the predetermined data, said security computer outputs an instruction to the host computer to grant access to the host computer or deny access thereto." The court declines to include the additional language urged by defendant. The security computer includes a "component." That component receives and compares the transmitted data to predetermined data. Based on the result of that comparison, the security computer then sends an instruction to the host computer to grant or deny access thereto. Thus the language following "such that" is not part of the function of the "component." Therefore, the court adopts plaintiff's proposed function: "receiving the transmitted data and comparing said transmitted data to predetermined data."

**Structure**

Defendant argues because the scope of "predetermined data" extends to biometric data, such as voice, the specification must disclose a sufficient algorithm to describe *how* to do the comparing but fails to do so, invalidating the claim.[148] Under the *AllVoice* case, however, the patentee does not have to provide algorithms for well-known, widely available, third-party software that could be employed to implement the algorithm disclosed in the specification. Plaintiff provided such algorithm during the

[148] D.I. 114 at 69.

*Markman* hearing, citing portions of Figure 9.[149]

As previously noted, the inventor told the PTO he wrote the main, controlling, program, that utilized third-party software to compare data.[150] With regard to this term, Sherman opines "there is ample disclosure in the specification of both the structure and function of the particular components described in the Asserted Patents, such that a skilled artisan would understand both structure and function" and cites to Figure 9 as support.[151]

Therefore, the court finds defendant has not demonstrated by clear and convincing evidence the absence of a sufficient algorithm to perform the claimed function and adopts plaintiff's algorithm, as presented at the *Markman* hearing: '599 patent, FIG. 9C, steps 186-196, 10:23-42 and/or '599 patent, FIGs. 9C-9D, steps 200-208, 11:1-31.[152]

13. *prompt means for outputting a second instruction at the telephonic device to re-enter predetermined data at and retransmit predetermined data from the telephonic device* ('599 patent, claim 32) / *prompt mechanism for instructing said accessor to enter predetermined data at and transmit said predetermined data from said peripheral device* ('701 patent, claim 1)

The parties agree these terms are subject to means-plus-function treatment.

Plaintiff states the function is: "instructing said accessor to enter predetermined

---

[149] D.I. 123 at 89:21-91:10.
[150] D.I. 86, Ex. S at SF000951.
[151] D.I. 114, Ex. B at ¶ 41.
[152] This is the same algorithm as adopted for the "comparator means" term. According to plaintiff, "the component that is claimed in Claim 54 is essentially claiming the comparator means. It's just two different ways to claim the same thing." D.I. 123 at 89:12-15. "As I said, the comparator means is just another way of claiming the components." *Id.* at 94:14-16. Defendant did not disagree with plaintiff's assertion. Instead it argued plaintiff's statement supported its position that "comparator" must be construed as a means-plus-function term: "I think [plaintiff], the argument . . . just made helps to confirm [defendant's] position. [Plaintiff] just said component for is basically equivalent to a comparator means. So if you just substitute component for comparator means for, those two are equivalent." *Id.* 91:19-24.

data at and transmit said predetermined data from said peripheral device."[153] At the *Markman* hearing, plaintiff pointed to specific steps from Figure 9 as the algorithm that performs the claimed function.[154]

Defendant's proposed function is: "voicing instructions to said accessor to re-enter predetermined data at and retransmit predetermined data from a peripheral device." Its proposed structure are the series of steps of Figure 9 identified in briefing and the Amended Joint Claim Construction Chart.[155]

**Function**

Defendant contends the claimed function must include the requirement that the instruction to the accessor be via voice instruction. The court disagrees. The claims include no such limitation. The specification, likewise, indicates no such requirement.

Claim 32 of the '599 patent recites: "prompt means for outputting a second instruction at the telephonic device to re-enter predetermined data at and retransmit predetermined data from the telephonic device." Based on that language, defendant argues the proper algorithm includes requesting the user to provide two instances of predetermined data (the first being what was "re-entered" and the second being what was "retransmitted").[156] Claim 1 of the '701, however, recites: "prompt mechanism for instructing said accessor to enter predetermined data at and transmit *said* predetermined data from said peripheral device."[157] That language makes clear there is only a single entry of predetermined data. The court agrees with plaintiff that an

---

[153] D.I. 123 at 114:6-16.
[154] *Id.* at 115:1-7.
[155] D.I. 114 at 72.
[156] D.I. 114 at 72.
[157] '701 patent, claim 1 (emphasis added).

ordinary skilled artisan would read the specification as requiring only a single entry. Therefore, the court adopts plaintiff's proposed function: "instructing said accessor to enter predetermined data at and transmit said predetermined data from said peripheral device."

**Structure**

At the *Markman* hearing, the parties each presented algorithms including substantially the same steps from Figures 9B-9C. The dispute is whether the accessor is required to enter two different types of information, e.g., a PIN *and* biometric, or whether the accessor can enter one, the other, or both. The court agrees with plaintiff the accessor is not required to enter two different types of information. The embodiment of Figure 1A uses only "a *biometric validation* which, in this case, is in the form of *voice recognition* and is within voice network 42."[158] The embodiment of Figure 11, in contrast, requires two different types of information. "The user answers the phone and is *prompted to enter a password* for password verification *and to enter a biometric identifier*, such as a fingerprint."[159] Because the claims do not require entry of two different types of information, and because the specification contemplates entry of one *or* two types of information, the court rejects defendant's argument. Consequently, the court adopts the algorithm proposed by plaintiff at the *Markman* hearing: '599 patent, FIGs. 9B-9C, steps 182-188, 10:12-30 and/or '599 patent, FIG. 9C, steps 198-202, 10:59-11:8.

14. *voice recognition means for authenticating at least one access demand in*

[158] '599 patent, 6:23-25 (emphasis added).
[159] '599 patent, 12:61-63 (emphasis added).

*response to transmission of the predetermined auditory statement* ('599 patent, claim 30); *voice sampling means for instructing the accessor to repeat back and transmit a predetermined auditory statement over the peripheral device* ('599 patent, claim 30)

The parties agree these are means-plus-function terms.

A. **Voice recognition means**

Plaintiff's proposed function is: "authenticating at least one access demand in response to transmission of the predetermined auditory statement."[160] At the *Markman* hearing, plaintiff presented a disclosed algorithm for carrying out that function: "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor" and Figures 9C-9D, steps 198-208 of the '599 patent.[161]

Defendant's proposed function is "performing voice sampling and instructing the accessor to repeat back and transmit a predetermined auditory statement over the peripheral device." It argues the term is indefinite for failure to disclose any algorithm to perform the claimed function.

**Function**

Plaintiff's proposed function tracks the language of the claim, the court sees no need to include "performing voice recognition" as suggested by defendant as the term itself identifies it as a "voice recognition means." The court, therefore, adopts plaintiff's proposed function: "authenticating at least one access demand in response to

[160] D.I. 123 at 117:6-15.
[161] *Id.* at 118:9-119:3 (citing '599 patent, 6:23-35).

transmission of the predetermined auditory statement."

**Structure**

As with other means-plus-function terms, defendant argues "voice recognition means" and "voice sampling means" are indefinite for failure to disclose specific voice recognition/sampling algorithms. Plaintiff again asserts it did not invent voice recognition/sampling; it invented the main algorithm it cites which uses generic, well-known, third-party software that samples or recognizes an accessor's voice. Claim 28 of the '599 patent introduces "a biometric analyzer for analyzing a monitored parameter of the accessor."[162] Claim 29 further specifies "[t]he method according to claim 28, wherein the biometric analyzer comprises *a voice recognition device*."[163] Claim 30 recites "[t]he method according to claim 29, wherein the *voice recognition program* comprises: a . . . *voice sampling means* . . . and *voice recognition means* . . . ."[164]

Thus voice recognition and sampling are specific forms of a biometric analyzer, e.g., part of the biometric analysis. Sherman opines a "'biometric analyzer' was a term of art and was well understood by skilled artisans in 2000 as denoting a program that extracts biometric sample and compares the data with that stored for a user."[165] The inventor told the PTO during reexamination the invention's main program he wrote used third-party software.[166] The Examiner found "proper support for the means plus function of the limitations of claim[ ] . . . 30: *voice sampling means and voice recognition means*

---

[162] '599 patent, claim 28.

[163] '599 patent, claim 29 (emphasis added); *see also* '701 patent, claim 8 ("A security system as described in claim 7, [wherein] said *biometric analyzer is a voice recognition program*.") (emphasis added).

[164] '599 patent, claim 30 (emphasis added).

[165] D.I. 114, Ex. B at ¶ 26.

[166] D.I. 86, Ex. S at SF000951.

in at least [0039-0041] of the specifications."[167] Therefore, again the court finds defendant has not demonstrated by clear and convincing evidence the absence of a sufficient algorithm to perform the claimed function[168] and adopts plaintiff's algorithm, as presented at the *Markman* hearing: "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor," '599 patent, 6:23-35, 5Figures 9C-9D, steps 198-208, 10:55-11:31.

B. **Voice Sampling Means**

Plaintiff's proposed function is: "instructing the accessor to repeat back and transmit a predetermined auditory statement over a peripheral device."[169] At the *Markman* hearing, plaintiff presented a disclosed algorithm for carrying out that function: "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor."[170]

Defendant's proposed function is: "performing voice sampling and instructing the accessor to repeat back and transmit a predetermined auditory statement over the

---

[167] *Id.*, Ex. Z at SF000467 (emphasis added).

[168] The court also rejects defendant's arguments based on the Federal Circuit's opinion in *Noah Sys., Inc. v. Inuit Inc.*, 675 F.3d 1302 (Fed. Cir. 2012). There, the court held "where a disclosed algorithm supports some, but not all, of the functions associated with a means-plus-function limitation, we treat the specification as if no algorithm has been disclosed at all. In such instances, we are not faced with a disclosure which addresses itself to an identifiable function, but arguably does so inadequately. We are faced with an identifiable function, which all parties concede is claimed, but as to which there is a total absence of structure. We cannot allow disclosure as to one function to fill the gaps in a specification as to a different, albeit related function." *Id.* at 1318-19. Here, plaintiff is not attempting to fill the gaps in the specification as to a different function; it provides an algorithm for performing biometric analysis, the specific performance of which utilizes third-party software (as disclosed in the intrinsic record).

[169] D.I. 123 at 119:3-9.

[170] *Id.* at 119:15-120:2 (citing '599 patent, 6:23-35).

peripheral device." It argues the term is indefinite for failure to disclose any algorithm to perform the claimed function.

**Function**

As with "voice recognition means," plaintiff's proposed function tracks the language of the claim; the court sees no need to include "performing voice sampling" as suggested by defendant as the term itself identifies it as a "voice sampling means." The court, therefore, adopts plaintiff's proposed function: "instructing the accessor to repeat back and transmit a predetermined auditory statement over a peripheral device."

**Structure**

For the same reasons discussed with regard to "voice recognition means," the court determines "voice sampling means" is definite and adopts plaintiff's algorithm, as presented at the *Markman* hearing: "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor," '599 patent, 6:23-35.

15. *authentication program mechanism for authenticating access to said host computer* ('701 patent, claim 7)

The parties agree this is a means-plus-function term.

Plaintiff's proposed function is: "authenticating access to said host computer."[171] At the *Markman* hearing, it proposed the supporting algorithm as: '599 patent, FIGs. 9B-9E, steps 174-219, 9:64-12:2.[172]

[171] D.I. 123 at 137:10-16.
[172] *Id.* at 138:13-17.

Defendant's proposed function is: "authenticating access to said host computer." Defendant contends the term is indefinite for failure to disclose any algorithm.

**Function**

The parties agree the claimed function is "authenticating access to said host computer." The court adopts that function.

**Structure**

The parties provided almost no briefing and very little in the way of argument at the *Markman* hearing for this term. Neither parties' expert discussed this term in their declarations attached to the Amended Joint Claim Construction Brief. The court concludes, therefore, defendant has not carried its burden to demonstrate by clear and convincing evidence the absence of a sufficient algorithm to perform the claimed function. The court adopts plaintiff's proposed construction presented at the *Markman* hearing: '599 patent, FIGs. 9B-9E, steps 174-219, 9:64-12:2.

16. *login identification demand to access* ('698 patent, claim 1)

The parties agree that this term should be construed to mean: "login identification and demand for access." The court adopts that agreed-upon construction.

**Order: The Court's Claim Construction**

At Wilmington, this 29th day of January, 2015, having heard oral argument, having reviewed the papers submitted with the parties' proposed claim constructions, and having considered all of the parties' arguments (whether or not explicitly discussed herein);

IT IS ORDERED that the disputed claim language in asserted claims of the

patent-in-suit, as identified by the parties, shall be construed below consistent with the tenets of claim construction set forth by the United States Court of Appeals for the Federal Circuit in *Phillips v. AWH Corp.*,[173] as follows:

| Claim Term | Construction |
|---|---|
| 1A. intercepting (as a general concept) | preventing the host computer from receiving |
| 1B. intercepted ('599 patent, claims 21, 30, 32) | prevented from being received by the host computer |
| 1C. an interception device / a device ('698 patent, claims 1, 2, 46, 54) | a device that prevents the host computer from receiving [what the interception device received instead] |
| 1D. an interception device for receiving a login identification originating from an accessor for access to said host computer ('701 patent, claim 1) | **Function:** receiving a login identification originating from an accessor for access to said host computer and preventing the host computer from receiving the login identification<br><br>**Structure:** router 36 (positioned before and separate from the host computer) |
| 2A. access channel / first channel ('599 patent, claims 21, 32; '698 patent, claims 46, 48; '701 patent, claim 1) | an information channel that is separate from and does not share any facilities with the authentication channel |
| 2B. authentication channel / second channel ('599 patent, claims 21, 28, 32; '698 patent, claims 1, 46, 47, 48, 50, 54; '701 patent, claims 1, 8) | a channel for performing authentication that is separate from and does not share any facilities with the access channel |
| 3A. security computer ('599 patent, claims 21, 32; '698 patent, claims 1, 2, 46, 48, 54; '701 patent, claims 1, 7) | a computer in the authentication channel that can grant authenticated users access to but is isolated from the host computer |

[173] 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

| Claim Term | Construction |
|---|---|
| 3B. host computer (‘599 patent, claims 21, 28, 32; ‘698 patent, claims 1, 46, 48, 54; ‘701 patent, claims 1, 7) | a computer to which the accessor is attempting to gain access, but which no information from an accessor is allowed to enter unless access is granted by the security computer |
| 4. a multichannel security system / an out-of-band computer security system / a security system (‘599 patent claim 32; ‘698 patent, claims 1, 46, 48, 54; ‘701 patent, claim 1) | a system that operates without reference to a host computer or any database in a network that includes the host computer |
| 5. verifying the login identification (‘698 patent, claim 1) | confirming at the security computer that the information used by an accessor to login to the host computer is valid |
| 6. subscriber database / a database (‘598 patent, claims 21, 32; ‘698 patent, claims 46, 48; ‘701 patent, claim 1) | a database in the authentication channel that maintains subscriber contact information for contacting accessors |
| 7. demand from an accessor / demand for access / access demand[s] / demand from said accessor / demand to access / a demand (“the Demand Terms”) (‘599 patent, claims 30, 32; ‘698 patent, claims 46, 54; ‘701 patent, claim 1) | a request to access the host computer that was sent from an accessor |
| 8. control module (‘599 patent, claim 21) | software of the security computer that incorporates a finite state machine, a call state model, process monitors, and fail-over mechanisms to interconnect with the other modules to control processing flow and interfacing with the internal and external system components |
| 9A. re-enter predetermined data (‘599 patent, claims 21, 32) | enter previously specified data |
| 9B. retransmit predetermined data (‘599 patent, claims 21, 32) | transmit previously specified data |

| Claim Term | Construction |
|---|---|
| 10. comparator means in said security computer for authenticating the access demand in response to the retransmission of the predetermined data from the telephonic device ('599 patent, claim 32) | **Function:** authenticating the access demand in response to the retransmission of the predetermined data from the telephonic device<br><br>**Structure:** '599 patent, FIG. 9C, steps 186-196, 10:23-42 and/or '599 patent, FIGs. 9C-9D, steps 200-208, 11:1-31 |
| 11. biometric analyzer . . . for analyzing a monitored parameter of [said] / [the] accessor ('599 patent, claim 28; '701 patent, claim 7) | **Function:** analyzing a monitored parameter of the accessor<br><br>**Structure:** "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor," '599 patent, 6:29-35 |
| 12. a component for receiving the transmitted data and comparing said transmitted data to predetermined data, such that, depending on the comparison of the transmitted and the predetermined data, said security computer outputs an instruction to the host computer to grant access to the host computer or deny access thereto ('698 patent, claim 54) | **Function:** receiving the transmitted data and comparing said transmitted data to predetermined data<br><br>**Structure:** '599 patent, FIG. 9C, steps 186-196, 10:23-42 and/or '599 patent, FIGs. 9C-9D, steps 200-208, 11:1-31 |
| 13. prompt means for outputting a second instruction at the telephonic device to re-enter predetermined data at and retransmit predetermined data from the telephonic device / prompt mechanism for instructing said accessor to enter predetermined data at and transmit said predetermined data from said peripheral device ('599 patent, claim 32; '701 patent, claim 1) | **Function:** instructing said accessor to enter predetermined data at and transmit said predetermined data from said peripheral device<br><br>**Structure:** '599 patent, FIGs. 9B-9C, steps 182-188, 10:12-30 and/or '599 patent, FIG. 9C, steps 198-202, 10:59-11:8 |

| Claim Term | Construction |
|---|---|
| 14A. voice recognition means for authenticating at least one access demand in response to transmission of the predetermined auditory statement ('599 patent, claim 30) | **Function:** authenticating at least one access demand in response to transmission of the predetermined auditory statement<br><br>**Structure:** "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor," '599 patent, 6:23-35, 5Figures 9C-9D, steps 198-208, 10:55-11:31 |
| 14B. voice sampling means for instructing the accessor to repeat back and transmit a predetermined auditory statement over the peripheral device ('599 patent, claim 30) | **Function:** instructing the accessor to repeat back and transmit a predetermined auditory statement over a peripheral device<br><br>**Structure:** "[1] [m]onitoring a particular parameter of the individual person; [2] . . . retrieving a previously stored sample (biometric data), thereof from a database [3] and comparing the stored sample with the input of the accessor," '599 patent, 6:23-35 |
| 15. authentication program mechanism for authenticating access to said host computer ('701 patent, claim 7) | **Function:** authenticating access to said host computer<br><br>**Structure:** '599 patent, FIGs. 9B-9E, steps 174-219, 9:64-12:2 |
| 16. login identification demand to access ('698 patent, claim 1) | login identification and demand for access |

Pursuant to 28 U.S.C. § 636(b)(1)(A) and (B), FED. R. CIV. P. 72(b)(1), and D. DEL. LR 72.1, any objections to the Report and Recommendation shall be filed within fourteen (14) days limited to twenty (20) pages after being served with the same. Any response shall be limited to twenty (20) pages.

The parties are directed to the Court's Standing Order in Non-Pro Se Matters for Objections Filed under FED. R. CIV. P. 72 dated October 9, 2013, a copy of which is found on the Court's website (www.ded.uscourts.gov).

Dated: January 29, 2015

/s/ Mary Pat Thynge
UNITED STATES MAGISTRATE JUDGE