UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CIVIL ACTION NO. 17-10422-RGS

STRIKEFORCE TECHNOLOGIES, INC.

v.

GEMALTO, INC., ET AL.

CIVIL ACTION NO. 17-10423-RGS

STRIKEFORCE TECHNOLOGIES, INC.

v.

VASCO DATA SECURITY, INC.

MEMORANDUM AND ORDER
ON PRE-DISCOVERY CLAIM CONSTRUCTION

August 31, 2017

STEARNS, D.J.

In these intellectual property disputes, plaintiff StrikeForce Technologies, Inc., asserts infringement claims of U.S. Patents Nos. 8,484,698 (the '698 patent) and 8,713,701 (the '701 patent) against two sets of defendants: Gemalto, Inc., Gemalto N.V., and SafeNet, Inc. (collectively Gemalto); and Vasco Data Security, Inc. Given the similar subject matter, the parties elected to consolidate pre-trial proceedings.

Accepting their proposal, the court bifurcated the *Markman* hearing and agreed to undertake pre-discovery claim construction of three groups of key disputed terms. *See Markman v. Westview Instruments, Inc.*, 517 U.S. 370 (1996). The court received tutorials in the underlying technology and heard argument on August 30, 2017.

THE ASSERTED PATENTS

Both the '698 and '701 patents are entitled "Multichannel Device Utilizing a Centralized Out-of-Band Authentication System (COBAS)." Both patents list Ram Pemmaraju as the sole inventor. The '698 patent was issued on July 9, 2013. The '701 patent was issued on April 29, 2014.

The '701 patent's application is a continuation of the application that led to the issuance of the '698 patent.[1] Both patents are directed to "[a] multichannel security system . . . for granting and denying access to a host computer in response to a demand from an access-seeking individual and computer." '698 patent, Abstract. According to the inventor, at the time of the invention, computer security "access control products authenticate[d] only the user and not the location." *Id.* col. 2, ll. 40-41.

[1] The '698 patent is a continuation of U.S. Patent No. 7,870,599 (the '599 patent). The '599 patent is a continuation-in-part of abandoned application no. 09/655,297 (the '297 application). All three issued patents share virtually identical specifications. Because of the identicality, all citations are to the '698 patent specification.

> Typically, access-control security products [such as simple password, random password, and biometric systems] are in-band authentication systems with the data and the authentication information on the same network. Thus, upon accessing a computer, a computer prompt requests that you enter your password and, upon clearance, access is granted. In this example, all information exchanged is on the same network or in-band. The technical problem created thereby is that the hacker is in a self-authenticating environment.

Id. col. 2, ll. 31-36. Dialing back to the originating modem was a feasible means of location verification when computer networks could be accessed only through modems. *See id*. col. 2, ll. 42-45. However, today's computer networks are typically accessible by modem-independent internet connections and "there is no necessary connection between the internet address and a location." *Id*. col. 2, ll. 46-53.

The asserted patents address the perceived security weakness through a "unique combination of user and host authentication." *Id*. col. 4, ll. 34-35.

> The security system of the present invention is out-of-band with respect to the host computer and is configured to intercept requests for access. 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.

Id. col. 4, ll. 34-42. Figure 1A, reproduced below, exemplifies an embodiment of the invention in a wide area network (WAN) environment.

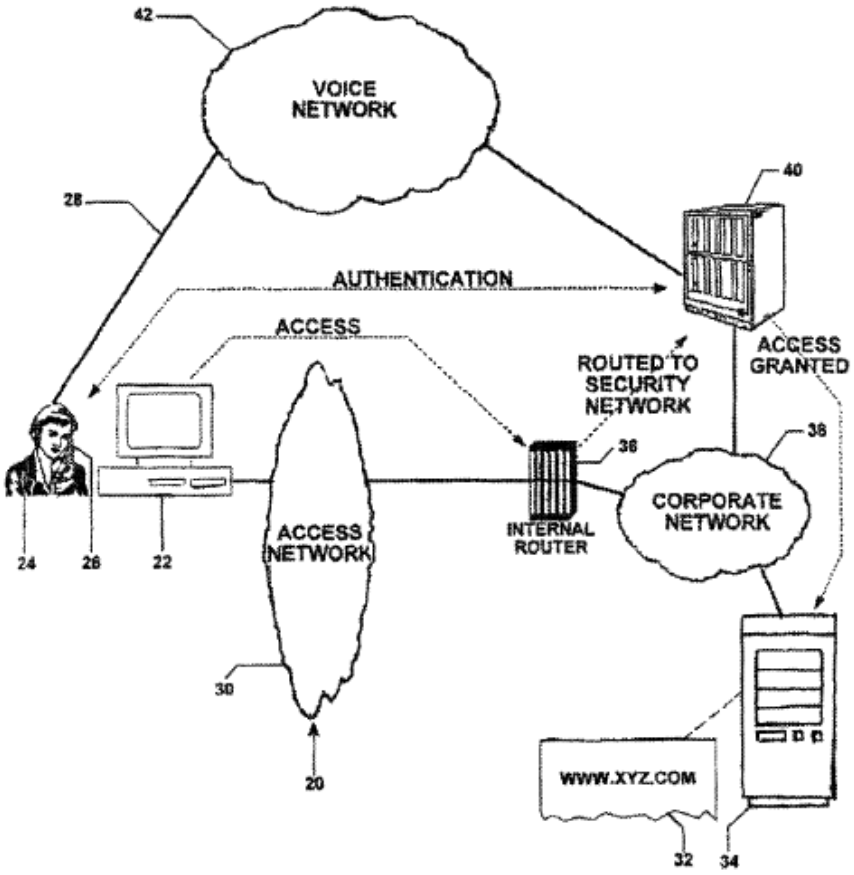

FIGURE 1A

> Here the accessor is the computer equipment 22, including the central processing unit and the operating system thereof, and the person or user 24 whose voice is transmittable by the telephone 26 over telephone lines 28. The access network 30 is constructed in such a manner that, when user 24 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. Authentication occurs in the out-of-band security network 40.

Id. col. 6, ll. 33-43.

The patents also disclose embodiments in local area network (LAN) and internet settings. The second embodiment is "applied to the intranet in which an internal accessor in a local area network seeks entry into a restricted portion of the host system." *Id*. col. 5, ll. 46-48.

> 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 an 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.

Id. col. 12, ll. 43-50; *see also* Fig. 10. "Th[e third] embodiment describes the application of the security system to access over the Internet." *Id*. col. 12, ll. 65-67.

> The [is the] case of [a] user accessing a web application, such as an online banking application, (located on a web server 334) 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 340, also referred to as the centralized out-of-band authentication system (COBAS). COBAS 340 proceeds with authenticating the user through the user's cellular telephone over an authentication channel. The security system 340 calls the access-seeking user at the cellular telephone 326. 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. The security system 340 authenticates the user and sends the result to the web server 334. Upon a positive authentication and after disconnecting from the authentication

channel, access is granted along the access channel to the USER'S PC device 322.

Id. col. 13, ll. 7-23; *see also* Fig. 11.[2]

Claim 1 of each asserted patent is emblematic.

'698 patent claim 1.

A software method for employing a multichannel security system to control access to a computer, comprising the steps of:

receiving at an interception device in a first channel a login identification demand to access a host computer also in the first channel;

verifying the login identification;

receiving at a security computer in a second channel the demand for access and the login identification;

outputting from the security computer a prompt requesting transmission of data;

receiving the transmitted data at the security computer;

comparing the transmitted data to predetermined data; and

depending on the comparison of the transmitted and the predetermined data, outputting an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto.

[2] A fourth embodiment, illustrated by Figure 13, is largely equivalent to the third embodiment, with the difference that it "describes the application to wireless networks including peripherals, such as PDAs and cellular telephones." *Id*. col. 13, ll. 62-64.

’701 patent claim 1.

A security system for accessing a host computer comprising:

an access channel comprising:

an interception device for receiving a login identification originating from an accessor for access to said host computer; and

an authentication channel comprising:

a security computer for receiving from said interception device said login identification and for communicating access information to said host computer and for communicating with a peripheral device of said accessor;

a database having at least one peripheral address record corresponding to said login identification;

a prompt mechanism for instructing said accessor to enter predetermined data at and transmit said predetermined data from said peripheral device; and

a comparator for authenticating access demands in response to the transmission of said predetermined data by verifying a match between said predetermined data and said entered and transmitted data,

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.

(Emphasis added to highlight disputed terms.) For purposes of this threshold *Markman* proceeding, the parties dispute the construction of the terms “host computer,” “access channel” / “first channel” and

"authentication channel" / "second channel," and "multichannel security system" / "security system."[3]

DISCUSSION

Claim construction is a matter of law. *See Markman*, 517 U.S. at 388-389. Claim terms are generally given the ordinary and customary meaning that would be attributed by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-1313 (Fed. Cir. 2005) (en banc) (citations omitted). In determining the understanding of this hypothetical person of ordinary skill in the art, the court looks to the specification of the patent, its prosecution history, and in those instances where appropriate, extrinsic evidence such as dictionaries, treatises, or expert testimony. *Id.* at 1315-1317. Ultimately, "[t]he construction that stays true to the claim language

[3] These three sets of claim terms, *inter alia*, were previously construed in *StrikeForce Techs. Inc. v. PhoneFactor Inc.*, 2015 WL 5708577 (D. Del. Sept. 29, 2015). Because that case was not litigated to a final judgment, the claim construction order has no preclusive effect. *See Vargas-Colon v. Fundacion Damas, Inc.*, 864 F.3d 14, 26 (1st Cir. 2017). In any event, the Federal Circuit requires each district court to perform a claim analysis independent of another court's claim construction. *See Lexington Luminance LLC v. Amazon.com Inc.*, 601 F. App'x 963, 969 (Fed. Cir. 2015).

and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." *Id*. at 1316 (citation omitted).

"host computer"

The parties agree that a "host computer" is something "to which an accessor is attempting to gain access." However, they part company on two particulars. First, StrikeForce contends that, consistent with instances where a user accesses a secure website on a web server or a secure portion of a website, *see* '698 patent, claim 3 ("wherein a host computer is a web server"), a "host computer" may be "a computer or a restricted portion thereof." Defendants protest the inclusion of the phrase "restricted portion." As defendants see it, while the patentee certainly knew how to describe a "restricted portion of the host system," as he did in explicating Figure 10, *see id*. col. 5, ll. 45-48; he nonetheless expressly directed his claims simply to a "host computer." Consequently, both the "restricted portion" and the embodiment illustrated in Figure 10 are excluded by the claims.

In the court's view, defendants' reading of the specification is much too narrow. Although it is true that the "restricted portion" language was used

only in describing Figure 10, it is not a unique feature of that embodiment.[4] In all the embodiments of the patents, a user may attempt to access a specific portion of a computer rather than the undivided system. Figure 1A, which defendants concede discloses a covered embodiment, shows a user attempting to access specific content in the form of a webpage "xyz.com" – that is, a restricted portion of a computer – hosted on a web server. In describing the details of this embodiment, the patents in numerous instances recite a web server as an exemplar of a "host computer." *See id*. Fig. 7 (block numbered 34 is "host computer or web server or router;" *id*. col. 7, l. 36 ("host computer or web server"); *id*. col. 8, ll. 41-42 (same); *id*. col. 8, l. 45 (same); *id*. col. 9, ll. 25-26 (same); *id*. col. 12, l. 24 (same). Indeed, claim 40 of the '698 patent expressly delineates a "host computer or web server." In addition, the patentee used parallel language in describing access to the webpage of the Figure 1 WAN embodiment as well as the secure database of the Figure 10 LAN embodiment. *Compare id*. col. 6, ll. 38-39 ("user 24 requests access to a web page 32 located at a host computer or web server

[4] Even if accessing a restricted portion of a host computer was unique to the Figure 10 illustration, a construction that excludes a preferred embodiment "is rarely, if ever, correct and would require highly persuasive evidentiary support." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1583 (Fed. Cir. 1996).

34.") *with id*. col. 12, ll. 44-46 ("user 224 requests access to a high security database 232 located at a host computer 234 through computer 222."). A construction of a "host computer" must therefore, consistent with all the embodiments, encompass seeking access to a restricted portion of a computer.

Second, defendants maintain that a "host computer" is one to which "no information from an accessor is allowed to enter unless access is granted by the security computer." Defendants offer several arguments in support of the additional constraint. Because the purpose of the claims is to determine whether a user is authorized to access the host computer, until the security computer "output[s] an instruction . . . to the host computer to grant access," *id*. claim 1, the user is denied access to the host computer. In the specification, the patentee emphasized the interception feature of the invention. *See*, *e.g.*, *id*. col. 6, ll. 40-42 ("[T]he request-for-access is diverted by a router 36 internal to the corporate network 38 to an out-of-band security network 40."). In like fashion, during the reexamination of the parent '599 patent, the patentee distinguished prior art on the concept of interception. *See*, *e.g.*, Gabberty Decl., Defs.' Ex. 20 at SF_1016 ("[T]he *Walker* patent does not disclose intercepting a user's (accessor's) login prior to allowing the user access to a host computer."). According to defendants, because the login

information is diverted to the out-of-band security network, it follows that no user information reaches the host computer unless and until the security computer grants access.

StrikeForce counters, and the court agrees, that while the claims require that a user is not granted *access* to the host computer until the security computer gives permission, the user may have prior *contact* with the host computer. As a threshold matter, how or when a user may contact a host computer is not an attribute inherent in the "host computer" itself. Nor did the patentee suggest that it is. It is the claimed components and steps of the invention that control user authentication and access. Although the majority of the claims of the asserted patents include an interception limitation,[5] not all do. Claims 25 and 53 of the '698 patent

[5] Each claim of the '599 parent patent recites an "interception means," "an intercepted demand for access," or "an intercepted login identification" limitation. It is therefore unsurprising that the patentee distinguished the '599 claims from prior art on this ground (among others). Defendants also cite the patentee's argument made during the prosecution of the '698 patent to distinguish the *Picket* prior art, that to modify *Picket* to result in the claimed invention would "require one of ordinary skill in the art to . . . find a way to capture a user request for accessing a host computer." Defs.' Ex. 22 at SF_1617-1618. However, that argument was made in the context of then-pending claims 21-29, 35-44, 60-62, and 64-66, *see id*. at SF_1617, all of which contained limitations either for an "interception device" (then-pending claims 21-29 and 35-44), or "a line program for intercepting a login identification" (then-pending claims 60-62 and 64-66), *see id*. at SF_1604-1611. The patentee did not rely on the interception limitation as the sole

both recite a "host computer" but do not claim an interception device or step. *See Phillips*, 415 F.3d at 1314 ("Because claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims.").

'698 patent claim 53.

> A software method for employing a multichannel security system to control access to a computer, comprising the steps of:
>
> receiving in a first channel a login identification demand to access a host computer also in the first channel;
>
> verifying the login identification;
>
> receiving at a security computer in a second channel the demand for access and the login identification;

---

differentiating characteristic. The patentee in the same Office Action Reply distinguished *Picket* on several other grounds, notably that

> the system described in *Picket* is one in which a user already has permission to access a website (i.e. a web server, which is a type of "host computer") to make a credit card purchase. Thus, *Picket* does not involve the step of "outputting an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto" . . . .

Id. at SF_1617. The patentee also noted that at the time of the invention a person of ordinary skill in the art would not have had the motivation to modify *Picket* to arrive at the claimed invention as "[s]uch a modified system would add an additional layer of authentication that is needed by the system disclosed in *Picket*, and would make the system . . . overly complicated and more expensive to implement, maintain, and operate, and more cumbersome to the user." *Id*.

> outputting from the security computer a prompt requesting a transmission of data;
>
> receiving the transmitted data at the security computer;
>
> comparing the transmitted data to predetermined data; and
>
> depending on the comparison of the transmitted and the predetermined data, outputting an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto.

Unlike claims that recite an interception device or step, claim 53 does not identify a specific component that must receive the login information in the first channel.[6] Without such a limitation, claim 53 is broad enough to encompass methods whereby the host computer itself receives the login information before relaying it to the security computer. Indeed, this is disclosed in both the third and fourth embodiments of the patent. "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 340*, also referred to as the centralized out-of-band authentication system (COBAS)." *Id*. col. 13, ll. 9-13 (emphasis added); *see*

[6] Likewise, claim 25, directed to "[a] software method for controlling access to a host computer," includes the step of "receiving an identification and first password from the client computer" without specifying an interception device or step.

also id. col 14, ll. 7-10. Figure 11, which illustrates the third embodiment, is reproduced below.[7, 8]

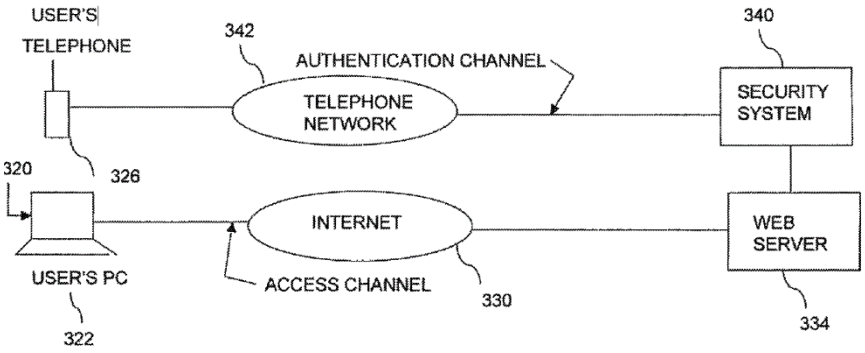

FIGURE 11

Because diverting the user login information is a function of an interception device or step, and not a function of the host computer, the court will not read the diversion requirement into the term "host computer." *See Ventana Med. Sys., Inc. v. Biogenex Labs., Inc.*, 473 F.3d 1173, 1181 (Fed. Cir. 2006) ("When the claim addresses only some of the features disclosed in the specification, it is improper to limit the claim to other, unclaimed features."). "Host computer" will therefore be construed

[7] Figure 13 illustrates the fourth embodiment. When the patentee amended the application to add what became issued claim 53 (then pending claim 74), he noted that it was supported, inter alia, by Figures 1A, 11, and 13. Defs.'s Ex. 22 at SF_1615.

[8] StrikeForce also notes that, even in the context of the Figure 1A embodiment, the user initially contacts the host computer to request access, and the "entry of the user identification and password [] is requested by the host computer." '698 patent, col. 9, ll. 29-31.

as "a computer (or a restricted portion thereof) to which the accessor is attempting to gain access."

"access channel" / "first channel" & "authentication channel" / "second channel"

In essence this is a dispute over the meaning of the term "out-of-band." Although the term "out-of-band" does not appear in any claim, it figures prominently in the title of the patents and the written description. Unlike prior art "in-band authentication systems with the data and the authentication information on the same network," '698 patent, col. 2, ll. 33-34, "[t]he security system of the present invention is out-of-band with respect to the host computer," *id*. col. 4, ll. 34-35.

> It is an object of the present invention to provide a host computer with a cost effective, out-of-band security network that combines high security and tokenless operation. It is a further object of the present invention to provide a network to isolate the authentication protocol of a computer system from the access channel therefor.

Id. col. 4, ll. 52-57. "[A]n 'out-of-band' system is defined herein as one having an authentication channel that is separated from the information channel." *Id*. col. 6, ll. 19-20.

Consistent with the specification, the parties agree that the "access channel" or "first channel" is "an information channel," that the "authentication channel" or "second channel" is "a channel for performing

authentication," and that the two channels are separate in the sense that the authentication channel is "out-of-band." They dispute, however, the degree of separation required for a channel to be "out-of-band." StrikeForce argues that information in the two channels may be "carried over separate facilities, frequency channels, or time slots than those used by the authentication channel/ second channel." Defendants maintain that the two channels must "not share any facility."

In support of its position, StrikeForce notes that its understanding of "out-of-band" is a meaning accepted by persons of ordinary skill in the art, demonstrated by the standard definition for "out-of-band signaling" contained in *Newton's Telecom Dictionary*. *See* Pl.'s Ex. 8. In addition, StrikeForce's proposed definition is also explicitly recited in the specification of the patents.

> For purposes of this discussion "in-band" operation is defined as one conducted wholly within a single channel or loop. Likewise, an "out-of-band" operation is defined as one using an authentication channel that is separated from the channel carrying the information and therefore is nonintrusive as it is carried over separate facilities, frequency channels, or time slots than those used for actual information transfer.

Id. col. 3, ll. 12-19.

Defendants point out that the broader "out-of-band" definition relied on by StrikeForce is set out in the BACKGROUND section of the

specification discussing and disparaging prior art, and does not describe the patented invention. With respect to the invention itself, defendants contend, and the court agrees, that the patentee acted as his own lexicographer in adopting a narrower definition. *See Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) ("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." (citation omitted)). "[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." '698 patent, col. 6, ll. 19-23 (emphasis added).

This understanding is also the one that was relied upon by the patentee during prosecution. During prosecution of the '297 application, the patentee distinguished the *Tuai* prior art on the in-band/out-of-band distinction. *Tuai* disclosed a "controller 15 [] interconnected between the host computer 10 and the modem 12," U.S. Patent 5,153,918, col. 4, ll. 2-3, and that "the capabilities of the central access controller 15 also include the optional call-back measure to enhance the security of the communication system," *id.* col. 8, ll. 3-5. The patentee argued that the central controller was "in-band" and

while it performs either an access or an authentication function at different times, "an in-band call back device operating after verification is not an out-of-band device which is integral in providing verification." Defs.' Ex. 15 at SF_714.

Similarly, during the prosecution of the '599 parent patent, the patentee distinguished the *LaDue* prior art, which disclosed "logically defined control channels," U.S. Patent No. 6,088,431, col. 8, l. 47, including an "authentication channel," *id*. col. 8, ll. 52-53. The patentee argued that the logically defined channels would not, in combination with *Tuai*, motivate the patented invention because the claimed system involved "the extra step of . . . adding a completely separate authentication channel." Defs.' Ex. 16 at SF_121.

Finally, during the reexamination of the '599 parent patent, the patentee summarized his invention as "an 'out-of-band' network security system having an authentication channel that is separated from an information (i.e. 'access') channel and therefore is noninstrusive as the authentication channel is carried over separate facilities than those used for actual information transfer." Defs.' Ex. 19 at SF_994. In support of the same reexamination, the patentee also submitted an expert declaration distinguishing the *Woodhill* prior art, inter alia, as not disclosing "an out-of-

band authentication channel that is separate from an access channel," because although *Woodhill* disclosed two channels, "both access and authentication merge in the same network (like the Internet)." Gabberty Decl., Defs.' Ex. 20 at SF_1017.

In light of the specification's clear and consistent definition (as reflected in the prosecution history), StrikeForce's rebuttal arguments fail. StrikeForce insists that because the patents require communication between the access and authentication channels, *see*, *e.g.*, '698 patent, claim 2 ("the security computer receives the demand and login identification from the interception device"), the two channels necessarily share facilities. However, that a security computer may receive data from two channels does not place the security system into both channels. Claim 1, upon which claim 2 depends, is clear that while the "interception device [is] in a first channel," the "security computer [is] in a second channel."

StrikeForce also suggests that weight should to be accorded to the dropping of a narrower interpretation of "out-of-band" that appeared in the abandoned '297 application from the issued patents. *See MPHJ Tech. Investments, LLC v. Ricoh Americas Corp.*, 847 F.3d 1363, 1369 (Fed. Cir. 2017) ("[I]t is the deletion from the '798 Provisional application that contributes understanding of the intended scope of the final application.").

During the prosecution of the '297 application, the patentee inserted in the specification the admonition that "[a]n 'out-of-band' operation is defined herein as one conducted without reference to the host computer or any database in the network." Defs.' Ex. 13 at SF_657. The "without reference" sentence was removed from the specification when the patentee submitted the applications for the subsequently issued patents.

In *MPHJ*, the Court found the deletion of the provisional application step significant because "[t]he '173 Patent in its final form contains no statement or suggestion of an intent to limit the claims to the deleted one-step operation." 847 F.3d at 1369. In contrast, while the admonitory language does not appear *verbatim* in the patents at issue here, the specification continues to emphasize the physical independence of the authentication channel from the access channel. *See* '698 patent, col. 6, ll. 44-47 ("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."); *id*. col. 12, ll. 58-61 ("This is in contradistinction to present authentication processes as the out-of-band security network 240 is isolated from the corporate network 238 and does not depend thereon for validating data."); *id*. col. 14, ll. 4-7 ("The security system 420 has two distinct and independent channels of operation,

namely, the access channel and the authentication channel."). The persistent emphasis on "isolat[ing]" the "distinct and independent" authentication channel from the access channel in all the disclosed embodiments also traverses StrikeForce's contention that the narrower definition was only descriptive of the Figure 1A WAN embodiment and not of the invention as a whole.[9]

Consistent with the patentee's own definition and use of the term "out-of-band" in the specification and the prosecution history, the court will construe "access channel" / "first channel" as "an information channel that is separate from and does not share any facility with the authentication channel;" and "authentication channel" / "second channel" as "a channel for performing authentication that is separate from and does not share any facilities with the access channel."

[9] StrikeForce additionally asserts that during the prosecution of the '297 application the patentee struck a bargain with the patent examiner and accepted the proposal to incorporate the broader *Newton's* definition. Although the patentee noted that his own definition is "consistent" with *Newton's*, '698 patent, col. 6, l. 18-19, he only accepted *Newton's* definition to the extent that the "agreeable portion of the definition is used." Pl.'s Ex. 9 at SF_711. There is no evidence anywhere in the intrinsic record that the patentee ever accepted the "frequency channels" or "time slots" aspect of the definition as applied to his own invention.

"multichannel security system"/ "security system"

The terms "multichannel security system" and "security system" appear in the preamble of all but one of the independent claims.[10] Defendants contend that these terms are limiting, arguing that they should be construed as "a system that operates without reference to a host computer or any database in a network that includes the host computer." StrikeForce maintains that the terms are not limiting, but proposes in the alternative the following construction: "a security system including an access/first channel and an authentication/second channel."

Defendants' proposed construction incorporates the language that was removed from the '297 application. Although defendants accurately note that during prosecution the patentee distinguished prior art based on the multichannel/out-of-band nature of the claimed invention, *see Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) ("[C]lear 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."), the court agrees with StrikeForce that the claim elements set out the comprehensive constituent components

[10] Claim 25 of the '698 claim does not recite a security system.

or steps of the claimed systems and methods independent of the disputed preamble terms, *see id*. at 808 ("[A] preamble is not limiting 'where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention.'" (citation omitted)). That the claimed systems or methods are "out-of-band" is already captured by the incorporation of that requirement in the construction of the access and authentication channels.[11] Inserting the same limitation into the preamble but using different words is both redundant and confusing. *See O2 Micro Intern. Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1362 (Fed. Cir. 2008), *quoting U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997) (The purpose of claim construction is to "clarify," "not an obligatory exercise in redundancy."). Thus, the court will not construe the preamble's recitation of a "multichannel security system" / "security system" as a claim limitation.

[11] The two channel limitations appear in each claim that recites a "multichannel security system" or "security system."

ORDER

The three sets of claim terms at issue will be construed for the jury and for all other purposes in a manner consistent with these rulings of the court.

SO ORDERED.

/s/ Richard G. Stearns

_____

UNITED STATES DISTRICT JUDGE