IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX, INC.,	§	
	§	
Plaintiff,	§	
	§	
vs.	§	**Civil Action No. 6:10-cv-417**
	§	
CISCO SYSTEMS, INC., et al.	§	
	§	**JURY TRIAL DEMANDED**
Defendants.	§	
	§	

VIRNETX'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES **PAGE(S)**

I. TECHNOLOGY OVERVIEW

There are six patents at issue in this lawsuit: U.S. Patent Nos. 6,502,135 (the '135 patent), 6,839,759 (the '759 patent), 7,188,180 (the '180 patent), 7,418,504 (the '504 patent), 7,490,151 (the '151 patent), and 7,921,211 (the '211 patent). The patents are attached in Exhibits 1-6.

The Court has previously construed terms for the '135, '759, and '180 patents in *VirnetX Inc. v. Microsoft Corp.*, Civ. No. 6:07-cv-80 (E.D. Tex.). The Court's claim construction opinion from the *Microsoft* litigation is attached at Ex. A. The new patents belong to the same family of patent applications.[1] As such, the technology at issue in the new patents will be familiar to the Court.

The patents are all concerned with secure communications. At a high level, the '135 patent discloses and claims systems and methods that create a virtual private network (VPN) based on a DNS request. Similarly, the '504 and '211 patents disclose and claim a domain name service system for establishing a secure communication link, and the '151 patent discloses and claims a domain name system that establishes an encrypted channel based on a DNS request. The '759 patent discloses and claims systems and methods that establish a VPN link using DNS without a user entering cryptographic information, such as encryption keys. The '180 patent discloses and claims systems and methods for a secure domain name service.

These inventions solve several problems known in the prior art. For example, the prior art required a user to manually set up the VPN *e.g.*, manually configuring the cryptographic keys required to encrypt and decrypt the messages. Manually-created VPNs were neither flexible nor easy to use. And business travelers trying to remotely connect to their corporate networks

[1] Specifically, the '211 patent is a continuation of the '504 patent, which is itself a continuation of a continuation-in-part of the application that became the '135 patent. The '151 patent is a division of the '135 patent application.

through VPNs had difficulty setting up and using VPNs. *See* '135::2:52-63. The inventions of the patents-in-suit made it easier to create VPNs and other secure communication links. This is an immense benefit to both users and computers that establish VPNs considering that, in the prior art, VPN and other secure communications that were difficult to set up were infrequently used, leaving sensitive communications unprotected.

II. PRINCIPLES OF CLAIM CONSTRUCTION

VirnetX proposes constructions of the claims of the patents-in-suit in accordance with long-established principles of claim construction—giving a claim term its ordinary meaning that one of skill in the art, at the time of the invention and in light of the patent's specification and prosecution history, would have given it, except in two unusual circumstances: (1) where the intrinsic record provides a special definition for the term; or (2) where the patentee disclaims a portion of the term's ordinary meaning. *See, e.g., Phillips v. AWH Corp.*, 415 F.3d 1303, 1316–17 (Fed. Cir. 2005). "[A]lthough the specification often describes very specific embodiments of the invention, [the Federal Circuit has] repeatedly warned against confining the claims to those embodiments." *Phillips*, 415 F.3d at 1323 (citing *Nazomi Communications, Inc. v. ARM Holdings, PLC*, 403 F.3d 1364, 1369 (Fed. Cir. 2005)). Limitations from the specification should not be read into the claims unless the patentee "acted as his own lexicographer and imbued the claim terms with a particular meaning or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction." *E-Pass Techs., Inc. v. 3COM Corp.*, 343 F.3d 1364, 1369 (Fed. Cir. 2003) (citations omitted).

Defendants seek to construe the claims in ways that have no basis in these or other principles of construction. Because the Court is familiar with the law of claim construction as well as the patents-in-suit, VirnetX will discuss specific claim construction principles only where applicable to each dispute.

III. LEVEL OF ORDINARY SKILL IN THE ART

Just as in the *Microsoft* litigation, VirnetX proposes that a person of ordinary skill in the art would have a Master's degree in computer science or computer engineering as well as two years of experience in computer networking with some accompanying exposure to network security. *See* Jones Decl. at ¶ 5. The Defendants have not disclosed a contention as to the level of ordinary skill in the art.

IV. DISPUTED CLAIM CONSTRUCTIONS

A. Disputes Concerning Types of Communication Links

1. "virtual private network" [included in asserted claims of the '135, '180, and '759 patents]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers	a network of computers which privately and directly communicate with each other by encrypting traffic on insecure communication paths between the computers where the communication is both secure and anonymous.

For the term "virtual private network," or "VPN," VirnetX proposes a construction identical to the Court's construction in the *Microsoft* case. *See* Ex. A (the Court's claim construction Memorandum in *VirnetX Inc. v. Microsoft Corp.*, 6:07-cv-80) at 35. The Defendants propose the same construction, but with two modifications: (i) the "where the communication is both secure and anonymous" language; and (ii) the "directly" language. As explained below, there is no legally justifiable basis for these modifications, and they would impose erroneous, extraneous limitations into the claim.

"Anonymous." The Defendants' proposed language comes from the Court's Microsoft claim construction opinion, which states that the term "virtual private network" requires "both data security and anonymity." *See* Ex. A. at 9. Respectfully, VirnetX submits that the Court was incorrect in requiring anonymity.

The Court was correct that the '135 patent discloses a way to achieve anonymity, i.e., "preventing[ing] an eavesdropper from discovering that terminal 100 is in communication with terminal 110." *See* Ex. A at 8 (citing the patent). But it does not follow that every claim in the patent is directed toward achieving anonymity. Rather, only the dependent, "IP address hopping" claims of the '135 patent (e.g., claims 6, and 14-17) achieve the anonymity contemplated by the patent. Specifically, the patent discusses how traffic analysis can defeat anonymity by determining the identities of transmitters and receivers and how this is a problem for various prior art communication schemes. *See* Background of the Invention, '135::1:57-59[2] ("[P]roxy schemes are **vulnerable to traffic analysis** methods of determining identities of transmitters and receivers.") (emphasis added) *see also* '135::2:46-47 ("[O]nion-routing . . . **can be defeated using traffic analysis**.") (emphasis added). The patent addresses the threat of traffic analysis through its disclosed IP address hopping scheme. *See* '135::5:13-20 ("IP address changes [i.e., IP address hopping] made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of 'attacks.' The variation of IP addresses **hinders traffic analysis** that might reveal which computers are communicating, and also provides a degree of immunity from attack.") (emphasis added).

Separate and apart from the problem of traffic analysis vis-à-vis anonymity, the patent also disclosed a new, better way to establish VPNs. *See* '135::32:29-35 ("The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) . . . (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry[.]"). Claims 1, 10, and 13 claim

[2] This brief uses the notation such as "'135::1:57-59" to refer to the lines 57 through 59 of column 1 of the '135 patent.

are directed to this improvement, and these claims do not include the "IP address hopping" limitation.[3]

In addition to revisiting the Court's opinion regarding the requirement of anonymity, it is important to revisit Microsoft's arguments that supported it. Microsoft argued that anonymity is a "primary purpose" of all VPNs. *See* Claim Construction Tr. from the *Microsoft* case, attached as Ex. C, at 34:18-24.[4] Microsoft's lawyer then discussed an example VPN scheme—encapsulation—to attempt to demonstrate that this is true. *See* Ex. C at 35:9-25. But contrary to Microsoft's lawyer's representations, the purpose of encapsulation is not to hide the IP addresses of the inner IP packet. *See* Jones Decl. at ¶ 6. Rather, the purpose of encapsulation is to enable computers to communicate as though they were on the same, private network. *See* id. Namely, in an encapsulation scheme, the outer IP packet transports the inner IP packet across the Internet and to the private network. *See* id. The private network then extracts the inner IP packet and routes it just as if the packet had originated within the network. In this way, the "anonymity" of the inner packet's IP addresses is merely a consequence of the true purpose of encapsulation—enabling computers to communicate as if they were on the same private network. *See* id. This

[3] The Court cited the specification's discussion of IP addresses "still be hopped" for the proposition that "the modifications of the invention retain the anonymity feature." *See* Ex. A at 9 (citing '135::23:20-25). The modification claimed in claims 1, 10, and 13, however, is discussed under the subheading "B. Use of a DNS Proxy to Transparently Create Virtual Private Networks," which begins at col. 37, line 17. In that section, IP address hopping is described as merely "one embodiment." *See* '135::38:33-35 ("In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604.").

[4] The page numbers that VirnetX cites refer to the transcription page number and not the page numbers of the *.txt file. For clarity, 34:18-24 refers to the following argument: "Now, our view is that there are two primary purposes in a private network and VPN, as borne out by the specifications of the patents but also by the ordinary meaning to those skilled in the art. The first is data security, and the second is anonymity."

view of VPNs is entirely consistent with the prosecution history of the '135 patent. *See* Ex. B[5] at 12[6] (explaining that Aventail does not teach a VPN because computers connected via the Aventail system are not able to communicate with each other "as though they were on the same network."). Moreover, this view of VPNs is already supported by the Court's construction for this term in that a VPN allows computers to "privately communicate with each other."

"Directly." The Defendants propose that computers communicating in a VPN must "directly" communicate with each other. Setting aside the ambiguity that this limitation would create,[7] this language should be rejected because there is no limiting language in the claims, written description or prosecution history requiring that computers must communicate "directly" in order to constitute a VPN. *See Clearwater Sys. Corp. v. Evapco, Inc.*, 394 Fed. Appx. 699, 706 (Fed. Cir. 2010) ("There is no limiting language in the claims, written description, or prosecution history requiring that the 'power source' power the entire apparatus. Accordingly, the district court improperly imported an extraneous limitation into the claim.").

[5] Exhibit B contains selected excerpts to the prosecution history from the original examination and re-examination of the '135 patent.

[6] For the Court's convenience, VirnetX included page numbers for all of the prosecution history exhibits. The page numbers that VirnetX added are in blue font in the lower right-hand corner. When VirnetX cites to specific pages of these exhibits, VirnetX is referring to these blue page numbers.

[7] In the context of computer communications, the word "directly" is very ambiguous as most computer topologies include numerous network devices between two computers that are communicating. VirnetX did not argue that the term "directly" precluded the presence of intermediate network connections on the path between the client and the target that relay traffic. Rather, during reexamination, VirnetX explained that computers connected to the Aventail system did not communicate directly because "[a]ll communications between the client and target stop and start at the intermediate SOCKS server." Ex. B at 14. If the Court were to accept the Defendants' "directly" language in their proposed construction, VirnetX fully expects the Defendants to attempt to exploit this ambiguity in asserting non-infringement defenses based on intermediate network devices.

Presumably, the Defendants will rely on the prosecution history as allegedly supporting constituting a disclaimer of scope, but the prosecution history gives no such support. As this Court is well aware, not every description of a prior art reference is automatically a disclaimer of scope. Rather, disclaimer is found when a patentee makes clear and unmistakable prosecution arguments limiting the meaning of a claim term in order to overcome a rejection. *See Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003) ("Where the patentee has unequivocally disavowed a certain meaning to obtain his patent, the doctrine of prosecution disclaimer attaches and narrows the ordinary meaning of the claim congruent with the scope of the surrender."). An exemplary case of prosecution history disclaimer is *Rheox, Inc. v. Entact, Inc.*, 276 F.3d 1319 (Fed. Cir. 2002). In that case, the patentee explicitly disclaimed compounds of higher solubility to overcome an anticipation rejection; as a result, the patentee was barred from later arguing that the claims should encompass such compounds. *See id*. at 1326.

In the re-examination of the '135 patent, VirnetX provided three reasons why Aventail did not teach a VPN. *See* Ex. B at 12-15. The three basic distinctions that VirnetX made over Aventail were: *first*, that "Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network," *see* Ex. B at 12-13; *second* that "Aventail Connect's fundamental operation is incompatible with users transmitting data that is sensitive to network information," *see* Ex. B at 13-14; and *third*, that "Aventail has not been shown to disclose a VPN because computers connected according to Aventail do not communicate directly with each other," *see* Ex. B at 14.[8] As such, unlike the patentee in *Rheox*, VirnetX was not forced to overcome a reference by

[8] VirnetX also disputed that the Aventail reference is prior art. *See* Ex. B at 9-11. After unsuccessfully searching to find evidence establishing Aventail as prior art, the examiner concluded that "Aventail cannot be relied upon as prior art to the '135 patent." *See* Ex. B. at 4-5.

disclaiming a certain scope of VPN taught by Aventail. Rather, VirnetX overcame Aventail on the ground that Aventail did not teach a VPN at all.

Moreover, because VirnetX offered three distinctions over the Aventail reference, there can be no "clear and unmistakable" disclaimer as to any one, isolated distinction. *Momentus Golf, Inc. v. Swingrite Golf Corp.*, 187 Fed. Appx. 981 (Fed. Cir. 2006) is instructive on this point. In that case, a patentee distinguished its patented golf club swing aide over a prior art reference on two grounds during prosecution. Namely the patentee argued to the USPTO that a prior art golf club swing aide did not meet a claim term because the prior art golf club swing aide was hollow and had a 10-25% club head weight. *See id*. at 984. The district court treated the weight distinction—in isolation—as a disclaimer of scope, and the Federal Circuit found that to be an erroneous application of prosecution history disclaimer. *See id*. The Federal Circuit explained that the patentee's statements did not meet the "clear and unmistakable" test because it was unclear whether the patentee disclaimed hollow devices as well as devices with 10-25% club head weight or alternatively whether the patentee merely disclaimed hollow devices with 10-25% club head weights. *See id*. Similarly, the Defendants cannot meet the "clear and unmistakable" test with respect to one of VirnetX's three distinctions over the Aventail reference.

For the foregoing reasons, VirnetX respectfully requests that the Court reconsider its dicta concerning the meaning of "private" and in any event not require anonymity for the claim term "virtual private network."

2. "virtual private link" [included in asserted claims of the '135 patent]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a communication link that permits computers to privately communicate with each other by encrypting traffic on insecure communication paths between the computers	a communication pathway that permits computers to privately communicate with each other by encrypting traffic on insecure communication paths between the computers and accomplishes data security and anonymity through the use of hop tables.

VirnetX's proposed construction for this term is adapted from the Court's construction for "virtual private network" in the *Microsoft* case. *See* Ex. A at 35. The Defendants' proposed construction is identical to VirnetX's, but it includes the phrase "and accomplishes data security and anonymity through the use of hop tables." For the reasons stated in § IV.A.1, *supra*, the Court should reject the Defendants' attempt to impose the "anonymity" and "hop table" limitations into this claim.

Further, the Defendants' proposed construction would render the dependent claims superfluous. Specifically, claims 14 through 17 of the '135 patent add the additional requirements that are directed to IP hopping. For example, claim 16 requires that the IP addresses of a packet be compared against moving window of valid IP addresses. As such, there is a strong presumption that the term "virtual private link" does not require anonymity or IP hop tables. *See, e.g., Zircon Corp. v. Stanley Black & Decker, Inc.*, 2011 U.S. App. LEXIS 20164 (Fed. Cir. Oct. 5, 2011) ("[T]he presumption arising from claim differentiation is a strong one when the very limitation one seeks to import into an independent claim appears in a claim dependent therefrom.") (citing *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004)); *but see Eon-Net LP v. Flagstar Bancorp*, 653 F.3d 1314, at *18 (Fed. Cir. Jul. 29, 2011) ("[C]laim differentiation is a rule of thumb that does not trump the clear import of the specification") (citing *Edwards Lifesciences, LLC v. Cook Inc.*, 582 F.3d 1322, 1331 (Fed. Cir. 2009)).

3. "secure communication link" [included in asserted claims of the '504, '211, and '759 patents]

VirnetX's Proposed Construction	Defendants' Proposed Construction
an encrypted communication link	virtual private network communication link.

As an initial matter, while the claim term "secure communication link" was at issue in the Microsoft case, the Court found that no construction was necessary because the term was defined in the claim as "virtual private network communication link." *See* Ex. A at 25 (citing claims 1 and 16 of the '759 patent). VirnetX does not dispute that "secure communication link" is limited to "virtual private network communication link" for the claims of the '759 patent for this reason. (All claims in the '759 patent define the term within the claims.) The claims in the '504 and '211 patents, however, do not define the "secure communication link" term in this way, and a construction is therefore warranted.

VirnetX's construction for this term is adapted directly from the specification. *See* '504::1:55-56[9] ("Data security is usually tackled using some form of data encryption."); *see also* Ex. A at 25 ("Also, 'communication' and 'link' are common terms that jurors would understand without a claim construction, and the patents do not assign any specialized meaning to these terms."). This is the ordinary scope of "secure communication link" given in the patents, and the Court should therefore adopt this construction.

Conversely, the Court should reject the Defendants' construction for at least three reasons. First, "[h]ad the inventors intended this limitation [to mean virtual private network communication link], they could have drafted claims to expressly include [virtual private network communication link]." *See i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 843 (Fed. Cir. 2010).

[9] Because the '211 patent is a continuation of the '504 patent (and therefore shares the same specification), VirnetX will cite only to the '504 patent in this section to avoid redundancy.

Second, VirnetX did not limit the ordinary scope for this term by assigning it special meaning. Presumably, the Defendants will argue that VirnetX acted as its own lexicographer and defined "secure communication link" to be "a virtual private network communication link" through the statement: "The secure communication link is a virtual private network communication link over the computer network." *See* '504::6:61-63. A careful review of this statement, however, reveals that the patentee was not acting as its own lexicographer but was instead describing a preferred embodiment in which a secure communication link is used to create a virtual private network. Specifically, the text quoted above is one part of a high-level description of the "one-click" preferred embodiment that begins at col. 6, line 36 of the '504 patent. This preferred embodiment is discussed in more detail beginning at col. 49, line 1 under the subheading "One-click Secure On-line Communications and Secure Domain Name Service." This detailed section first describes how the secure communication link between computer 3301 and server computer 3304 is transparently established. *See* '504::50:21-24 ("All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 330l."). The specification then explains how software module 3309 uses the secure communication link to create a virtual private network:

> At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link.
>
> * * *
>
> According to the invention, software module 3309 contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module 3309 accesses a secure portal 3310 that interfaces a secure network 3311 to computer network 3302. Secure network 3311 includes an internal router 3312, a secure domain name service (SDNS) 3313, a VPN gatekeeper 3314 and a secure proxy 3315. The secure network can include other network

> services, such as e-mail 3316, a plurality of chatrooms (of which only one chatroom 3317 is shown), and a standard domain name service (STD DNS) 3318. Of course, secure network 3311 can include other resources and services that are not shown in FIG. 33.

'504::50:25-53. In other words, because software module 3309 enables computer 3301 to communicate in the private network 3311 as though it were physically in that network, the secure communication link is also a virtual private network communication link in this embodiment. As such, the limitation from the specification should not be read into the claims because the patentee did not imbue "the claim terms with a particular meaning or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction." *See E-Pass Techs.*, 343 F.3d at 1369.

Third and finally, VirnetX did not narrow the meaning of this term in this way to overcome a rejection in prosecution, *see* Ex. D and Ex. E (selected pages from the prosecution histories of the '504 and '211 patents respectively); therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324.

In sum, because there is no limiting language in the claims, written description, or prosecution history requiring the Defendants' proposed limitation, they are extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706 ("There is no limiting language in the claims, written description, or prosecution history requiring that the 'power source' power the entire apparatus. Accordingly, the district court improperly imported an extraneous limitation into the claim.").

B. Disputes Concerning Domain Name, Domain Name Service, Secure Domain Name, etc.

1. *"domain name service" [included in asserted claims of the '135, '180, '504, and '211 patents]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
a lookup service that returns an IP address for a requested domain name	a lookup service that returns an IP address for a requested domain name to the requester.

VirnetX's proposed construction is identical to the Court's construction from the *Microsoft* case. *See* Ex. A at 35. The Court's construction was, in turn, adapted directly from the specification and adds no extraneous limitations. *See* Ex. A at 12 (citing '135::37:22-29). As such, the Court should readopt its construction for this term.

The Defendants' proposed construction modifies the construction by imposing the extraneous limitation IP address is returned "to the requester." This language is not consistent with how one skilled in the art would understand the ordinary meaning of this term. *See* Jones Decl. at ¶¶ 7-8. Particularly, one skilled in the art would not consider the Defendants' proposed language of "to the requestor" in determining what is and what is not a "domain name service." *See* Jones Decl. at ¶ 8.

Further, the Defendants have cited no evidence that the patentee "acted as his own lexicographer and imbued the claim terms with [this] particular meaning or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction" and, therefore, this limitation should not be imported from the specification. *See E-Pass Techs.*, 343 F.3d at 1369. Moreover, VirnetX did not narrow the meaning of this term in this way to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language

in the claims, written description, or prosecution history requiring the Defendants' proposed limitation, it is extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706.

2. "domain name" [included in asserted claims of the '135, '180, '504, and '211 patents]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a name corresponding to an IP address	a hierarchical sequence of words in decreasing order of specificity that corresponds to a numerical IP address.

VirnetX's proposed construction is identical to the Court's construction from the *Microsoft* case. *See* Ex. A at 35. The Court adapted its construction from the language of the claims, themselves, which describe the term "domain name." *See* Ex. A at 12-13. The same holds true for the patents not at issue in the Microsoft litigation that contain this term. *See, e.g.*, claim 1 of the '504 patent ("to store a plurality of domain names and corresponding network addresses") and claim 1 of the '211 patent ("store a plurality of domain names and corresponding network addresses). As such, the Court should readopt its construction for this term.

The Defendants' proposed construction seeks to impose a "hierarchical" requirement and further seek to impose a requirement as to the specific order of that hierarchy. The Court previously considered—and rejected—similar requirements in the Microsoft case. Specifically, Microsoft proposed the construction "a hierarchical name for a computer (such as www.utexas.edu) that the Domain Name Service converts into an IP address" for this term. *See* Ex. A at 12. In rejecting this construction, the Court recognized that the only intrinsic evidence that Microsoft cited in support of its construction was "non-limiting language." *See* Ex. A at 14.

The Defendants' proposed language is also inconsistent with how one skilled in the art would understand the ordinary meaning of this term. *See* Jones Decl. at ¶¶ 9-12. The use of hierarchical names on the Internet has proven very successful because it allows for a distributed approach to managing the naming of a huge number of computers around the world. *See* id. at

¶ 10. In contrast, in the patents, a DNS proxy server does not need to provide answers for every domain name on the Internet, and can, for example, provide answers for only a few secure computers, thus alleviating any need for a hierarchical organizational scheme. *See* id.[10] In sum, one skilled in the art would not consider the Defendants' proposed language in determining what is and what is not a domain name. *See* id. at ¶ 12.

Further, the Defendants have cited no evidence that the patentee "acted as his own lexicographer and imbued the claim terms with [these] particular meaning[s] or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction" and, therefore, these limitations should not be imposed onto the claims. *See E-Pass Techs.*, 343 F.3d at 1369. Moreover, VirnetX did not narrow the meaning of this term in this way to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language in the claims, written description, or prosecution history requiring the Defendants' proposed limitations, they are extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706.

[10] The Defendants' proposed construction is also deficient for the reason that it limits a domain name to a sequence of "words." This limitation appears to exclude some domain names that conform to IETF RFCs and are in use on the Internet because those domain names contain information other than names. *See* Jones Decl. at ¶ 11. For example, it is permissible on the Internet to use domain names that include numerical digits as well as characters that do not form words. Examples include virnetx.com, cisco.com, vt.edu, and esd123.org. *See* id. The patents, in some instances, use the term "domain name" when describing the typical operation of the Internet, including domain names, placing no limitation that domain names be limited to a sequence of words. *See* id.

3. "DNS proxy server" [included in asserted claims of the '135 patent]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a computer or program that responds to a domain name inquiry in place of a DNS	a computer or program that responds to a domain name inquiry in place of a DNS, and prevents destination servers from determining the identity of the entity sending the domain name inquiry.

VirnetX's proposed construction is identical to the Court's construction from the *Microsoft* case. *See* Ex. A at 35. This construction is consistent with the intrinsic evidence, and the Court should readopt its construction for this term.

The Defendants seek to impose an extraneous limitation on this claim term, namely the requirement that a DNS proxy server "prevents destination servers from determining the identity of the entity sending the domain name inquiry." This language is not consistent with how one skilled in the art would understand the ordinary meaning of this term. *See* Jones Decl. at ¶¶ 13-16. Moreover, the Defendants' proposed construction would read out a preferred embodiment. Specifically, in Figure 26, computer 2601 communicates directly with computers 2604 and 2611. *See* id. at ¶ 15. Given that authentication and authorization are likely to be required, it is implausible that computers 2604 and 2611 would not know the identity of 2601. *See* id. As this Court is well aware, "[a] claim interpretation that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct." See *Globetrotter Software, Inc. v. Elan Computer Group, Inc.*, 362 F.3d 1367, 1381 (Fed. Cir. 2004).

As support for their construction, the Defendants will presumably rely on the Background of the Invention, particularly the sentence: "Proxy servers prevent destination servers from determining the identities of the originating clients." *See* '135::1:48-51. This statement, however, does not refer to all proxy servers. Rather, this statement refers to proxy servers employed in a specific way known in the prior art to attempt to achieve anonymity:

> To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server.
>
> * * *
>
> This scheme relies on a trusted outside proxy server.

'135::1:46-57. In this setup—using (i) a local proxy server, (ii) a trusted outside proxy server, and (iii) an encrypted communication channel—a proxy server will prevent destination servers from determining the identities of the originating clients. But this statement does not extend to all systems that use proxy servers, and it was not intended to. As such, the patentee did not imbue "the claim terms with [this] particular meaning or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction" and, therefore, this limitation should not be imposed onto the claims. *See E-Pass Techs.*, 343 F.3d at 1369. Moreover, VirnetX did not narrow the meaning of this term in this way to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language in the claims, written description, or prosecution history requiring the Defendants' proposed limitation, it is extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706.

4. "secure domain name service" [included in asserted claims of the '180 patent]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name	a non-standard lookup service that requires authorization for access, recognizes that a query message is requesting a secure computer address, and performs its services accordingly by returning a secure network address for a requested secure domain name.

The Court previously construed this term, *see* Ex. A. at 35, but all parties are seeking a new construction. Importantly, VirnetX is proposing a new construction for this term because

VirnetX clarified the scope of this term for the benefit of the examiner during re-examination, and VirnetX believes that these clarifications would be helpful to a jury. In re-examination, the examiner mistakenly believed that any DNS could be a secure domain name service if it happened to resolve a domain name for a computer used to establish a secure connection. *See* Ex. F (selected pages from the prosecution history of the '180 patent) at 22. VirnetX clarified this point for the examiner by explaining:

> A secure domain name service is not a domain name service that resolves a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name. A secure domain name service of the '180 Patent, instead, recognizes that a query message is requesting a secure computer network address and performs its services accordingly.

See Ex. F at 24 (internal citations removed). Both VirnetX's proposed construction and the Defendants' proposed construction is adapted from this clarification.

The Defendants' proposed construction, however, includes two limitations not found in the specification or prosecution history, namely: (i) "non-standard;" and (ii) "requires authorization for access." While these limitations apply to the "secure domain name" and "secure computer network address" limitations respectively, the Defendants have cited no evidence that the patentee "acted as his own lexicographer and imbued the claim terms with [these] particular meaning[s] or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction" and, therefore, these limitations should not be imposed onto the claims. *See E-Pass Techs.*, 343 F.3d at 1369. Moreover, VirnetX did not narrow the meaning of this term in this way to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language in the claims, written description, or prosecution history

requiring the Defendants' proposed limitations, they are extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706.

5. "domain name service system" [included in asserted claims of the '504 and '211 patents]

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary] alternatively, VirnetX proposes: a computer system that includes a domain name service (DNS)	a DNS that is capable of differentiating between, and responding to, both standard and secure top-level domain names.

No construction is necessary for this term. The claims containing this term describe the required properties of the domain name service system, themselves. For example, claim 1 of the '504 patent claims:

> a domain name service system configured to be connected to a communication network, to store a plurality of domain names and corresponding network addresses, to receive a query for a network address, and to comprise an indication that the domain name service system supports establishing a secure communication link.

As the claim defines the requirements for the term, no construction is necessary. Alternatively, VirnetX proposes that the term be construed to be "a computer system that includes a domain name service (DNS)." This alternative, proposed construction is a straightforward adaptation of the Court's prior construction of "domain name service."

The Defendants' proposed construction would require every "domain name service system" to have the ability to differentiate between, and respond to, both standard and secure top-level domain names. The Defendants, however, have cited no evidence that the patentee "acted as his own lexicographer and imbued the claim terms with [these] particular meaning[s] or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction" and, therefore, this limitation should not be imposed on the claims. *See E-Pass Techs.*, 343 F.3d at 1369. Moreover, VirnetX did not narrow the meaning of this term in

this way to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language in the claims, written description, or prosecution history requiring the Defendants' proposed limitations, they are extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706. Finally, the claim language itself nowhere references a secure domain name; defendants seek to fabricate that claim language without any textual hook. *See MBO Labs., Inc. v. Becton, Dickinson & Co.*, 474 F.3d 1323, 1330-1331 (Fed. Cir. 2007) ("[W] we cannot endorse a construction analysis that does not identify 'a textual reference in the actual language of the claim with which to associate a proffered claim construction.'") (quoting *Johnson Worldwide Assocs., Inc. v. Zebco Corp.*, 175 F.3d 985, 990 (Fed. Cir. 1999)).

6. "top-level domain name" [included in asserted claims of the '504 and '211 patents]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a label that identifies a first level subdomain	a label that identifies a first level subdomain of the DNS root domain.

VirnetX and the Defendants propose similar constructions for this term. The difference is that the Defendants' construction contains the language "of the DNS root domain." This additional language should be rejected because it would have the nonsensical result of rendering dependent claim 3 of the '504 patent impossible. Specifically, claim 3 requires that the top level domain name be a non-standard top level domain name. By definition, a non-standard top level domain name cannot identify a subdomain of a DNS root domain. As such, the Defendants' proposed construction should be rejected. *See AIA Eng'g Ltd. v. Magotteaux Int'l S/A*, 2011 U.S. App. LEXIS 18125 (Fed. Cir. Aug. 31, 2011) (Courts "strive, where possible, to avoid nonsensical results in construing claim language.") (citing *Bd. of Regents of the Univ. of Tex. Sys. v. BENQ Am. Corp.*, 533 F.3d 1362, 1370 (Fed. Cir. 2008).

C. Disputes Concerning Web Site, Secure Web Site, Secure Web Computer, etc.

1. *"web site" [included in asserted claims of the '135 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
a computer associated with a domain name and that can communicate in a network	one or more related web pages at a location on the World Wide Web.

2. *"secure web site" [included in asserted claims of the '135 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
a computer associated with a domain name and that can communicate in a virtual private network	a web site that requires authorization for access and that can communicate in a VPN.

3. *"secure target web site" [included in asserted claims of the '135 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
a target computer associated with a domain name and that can communicate in a virtual private network	a secure web site on the target computer.

VirnetX proposes the same construction for the term "secure web site" as it did in the *Microsoft* litigation. VirnetX's proposed constructions for the terms "web site" and "secure target web site" are adapted from its proposed construction for the term "secure web site." The Court is familiar with VirnetX's position. To avoid unnecessary repetition, VirnetX will incorporate by reference its evidence that support its position from the *Microsoft* case rather than copying it in the body of this brief. *See* Ex. G and H.

As an addendum, VirnetX also notes that the examiner in re-examination applied these terms in a manner consistent with VirnetX's proposed constructions when analyzing an alleged prior art reference. "[A] court in its discretion may admit and rely on prior art proffered by one of the parties, whether or not cited in the specification or the file history. This prior art can often help to demonstrate how a disputed term is used by those skilled in the art. *Vitronics Corp. v. Conceptronic*, 90 F.3d 1576, 1584 (Fed. Cir. 1996). Specifically, the examiner found that Aventail met the "secure web site" and "web site" limitations irrespective of formalized, extrinsic definition of the term "web site"—in other words, irrespective of the "web page" and

"World Wide Web" requirements. Instead, the examiner properly focused his inquiry on communication taking place between computers in the Aventail system:

> determining whether the DNS request transmitted in step (1) is requesting access to a secure web site *(Aventail, Page 12 - Aventail Connect checks the connection request, If the destination hostname matches' a redirection rule create a false DNS entry, If the destination hostname matches a redirection rule ... the host is a part of a domain we are proxying traffic to; ·Page 29 configuration files determine how network connections will be routed and which authentication protocols are enabled)*

Ex. B at 37 (italics, in original, indicate examiner's arguments). This view of the claim terms is precisely what is contemplated and required by the claim language: "determining whether the DNS request . . . is requesting access to a secure web site." *See* also Ex. B at 40 (the examiner similarly did not require "web page" or "World Wide Web" for the claim term web site for claim 10); *see also id*. at 8-16 (not distinguishing the Aventail reference based on the existence or non-existence of "web page" or "World Wide Web" for the claim term "web site."). For these reasons, VirnetX respectfully requests the Court reconsider its constructions and not impose the requirements of the formalized, extrinsic definition of the term "web site" onto the claims. *See Phillips*, 415 F.3d at 1322 (Fed. Cir. 2005) (warning against the deficiencies of technical dictionaries: "There is no guarantee that a term is used in the same way in a treatise as it would be by the patentee. In fact, discrepancies between the patent and treatises are apt to be common because the patent by its nature describes something novel.").

4. "secure web computer" [included in asserted claims of the '135 patent]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a computer that requires authorization for access and that can communicate in a virtual private network	[indefinite or "the target computer that hosts the secure web site"].

As an initial matter, claim 10 of the '135 patent uses the terms "secure web computer" and "secure target computer" interchangeably:

> 10. A system that transparently **creates a virtual private network (VPN) between a client computer and a secure target computer**, comprising:
>
> a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to **create the VPN between the client computer and the secure target computer** if it is determined that access to a secure web site has been requested; and
>
> a gatekeeper computer that allocates resources for **the VPN between the client computer and the secure web computer** in response to the request by the DNS proxy server.

(emphasis added). The secure web computer / secure target computer is described in preferred embodiments labeled "Scenario #1" and "Scenario #2." '135::39:42-60. In these embodiments, a client computer requests to access the target computer, and if the client has authorization to access the target computer, a gatekeeper computer establishes a VPN. *See* '135::39:42-48. If the client computer does not have authorization to access the target computer, the DNS proxy returns a "host unknown" message. *See* '135::39:53-60. The Court, in its claim construction Order in the *Microsoft* case, recognized that "secure" in certain contexts in the patent, refers to authorization for access. *See* Ex. A at 18 (discussing columns 37 and 38: "These italicized portions explain that "secure" relates to registered users who have the ability to set up a virtual private network with a target node. This supports that "secure" means "requiring authorization for access."). In this way, VirnetX's proposed construction is consistent with the specification of the '135 patent and should be adopted.

The Defendants' proposed construction would require the secure web computer to "host" the secure web site. The Defendants, however, have cited no evidence that the patentee "acted as his own lexicographer and imbued the claim terms with [this] particular meaning or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or

restriction" and, therefore, this limitation should not be imposed on the claims. *See E-Pass Techs.*, 343 F.3d at 1369. Moreover, VirnetX did not narrow the meaning of this term in this way to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language in the claims, written description, or prosecution history requiring the Defendants' proposed limitation, it is extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706.

5. "secure server" [included in asserted claims of the '151 patent]

VirnetX's Proposed Construction	Defendants' Proposed Construction
a server that requires authorization for access and that can communicate in an encrypted channel	a server that requires authorization for access and communicates in a VPN.

VirnetX's proposed construction for this term is essentially the same as its proposed construction for the term "secure web computer," discuss in § IV.C.4, *supra*. But unlike the claims of the '135 patent, which are directed toward the establishment of VPNs, the claims of the '151 patent are directed toward the establishment of encrypted channels. As such, VirnetX respectfully proposes that its construction be adopted for the same reasons given in § IV.C.4.[11]

6. "target computer" [included in asserted claims of the '135 patent]

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary] alternatively, VirnetX proposes: a computer with which the client computer seeks to communicate	the ultimate destination with which the client computer seeks to communicate.

No construction is necessary for this term. The terms "target" and "computer" are common terms that jurors would understand without construction. Alternatively, VirnetX proposes that the Court construe this term to mean "a computer with which the client computer seeks to communicate."

[11] For the Court's convenience, VirnetX has also included selected pages from the prosecution history of the '151 patent in Ex. I.

The Defendants' proposed construction should be rejected because would require the target computer to be the "ultimate" destination. This language is not consistent with how one skilled in the art would understand the ordinary meaning of this term. *See* Jones Decl. at ¶¶ 17-20. Unlike "computer," the phrase "ultimate destination" does not hold a particular or specific meaning in the art. *See* id. at ¶ 18. Also, when a client computer forms a VPN, it may communicate with multiple computers in a private network virtually as if it were in that private network. *See* id. at ¶ 19. In sum, one skilled in the art would not consider the Defendants' proposed language in determining what is and what is not a target computer. *See* id. at ¶ 20.

Also, "[h]ad the inventors intended this limitation, they could have drafted claims to expressly include it." *See i4i*, 598 F.3d at 843. Further, the Defendants have cited no evidence that the patentee "acted as his own lexicographer and imbued the claim terms with [this] particular meaning or disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction." *See E-Pass Techs.*, 343 F.3d at 1369. In fact, the '135 patent does not mention the word "ultimate" at all. Also, VirnetX did not narrow the meaning of this term in this way to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language in the claims, written description, or prosecution history requiring the Defendants' proposed limitation, it is extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706.

D. Disputes Concerning Defendants' Attempt to Rewrite the Claims

1. *"between [A] and [B]" [included in asserted claims of the '135, '151, '504, '211, and '759 patents]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary]	extending from [A] to [B][12]

2. *"determining whether the DNS request transmitted in step (1) is requesting access to a secure web site" [included in asserted claims of the '135 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary]	determining on a DNS proxy server whether the DNS request transmitted in step (1) is requesting access to a secure web site.

3. *"generating from the client computer a Domain Name Service (DNS) request" [included in asserted claims of the '135 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary]	creating and transmitting from the client computer a DNS request.

4. *"an indication that the domain name service system supports establishing a secure communication link" [included in asserted claims of the '504 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary]	a visible message or signal that informs the user that the domain name service system supports establishing a secure communication link.

5. *"indicate/indicating… whether the domain name service system supports establishing a secure communication link" [included in asserted claims of the '211 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary]	display/displaying a visible message or signal that informs the user whether the domain name service system supports establishing a secure communication link.

[12] For example, the Defendants propose that the phrase "between the client computer and the target computer" should be construed to mean "extending from the client computer to the target computer." The Defendants propose numerous such constructions—one for every instance where the word "between" is found in the claim language. All of the Defendants' proposed constructions follow the pattern of rewriting "between [A] and [B]" to "extending from [A] to [B]."

6. *"enabling a secure communication mode of communication" [included in asserted claims of the '759 patent]*

VirnetX's Proposed Construction	Defendants' Proposed Construction
[no construction necessary]	using an input device to select a secure communication mode of communication.

The six disputes above concern the Defendants' attempts to rewrite wide swaths of claim language. As a threshold matter, the Defendants fail to consider whether these purported "claim terms"—which are really entire paragraphs—are even claim terms that are eligible for construction. They are not:

> A troubling aspect of this case is the submission by [Defendant] of entire paragraphs of certain claims for construction when there was really no dispute over the meaning of any particular word or term. The court expects the parties and their attorneys to limit the terms they ultimately submit for construction to those that might be unfamiliar or confusing to the jury, or which are unclear or ambiguous in light of the specification and patent history. *See United States Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997); *Orion IP, LLC v. Staples, Inc.*, 406 F.Supp.2d 717, 738 (E.D. Tex. 2005) ("although every word used in a claim has a meaning, not every word requires a construction."). One hopes this was not merely an effort to pollinate the record with alleged error. Claim interpretation does not consist of defining a step in a claim by restating other limitations that are spelled out elsewhere in the claim. In spite of protestations of "confusion" from one side or the other, the court construes a claim from the point of view of the artisan of ordinary skill, not from the vantage point of the hyper-technical grammarian, who can not quite grasp the meaning of "is" in a particular context.

Grantley Patent Holdings, Ltd. v. Clear Channel Communs., Inc., 2008 U.S. Dist. LEXIS 1588, at *12-13 (E.D. Tex. Jan. 8, 2008) (Clark, J.).

In any event, these phrases have an ordinary meaning that a jury would understand without construction. Moreover, "[h]ad the inventors intended this limitation, they could have drafted claims to expressly include it." *See i4i*, 598 F.3d at 843. Further, the Defendants have cited no evidence that the patentee "acted as his own lexicographer and imbued [these] claim[s] terms with [these] particular meaning[s] or disavowed or disclaimed scope of coverage, by using

words or expressions of manifest exclusion or restriction." *See E-Pass Techs.*, 343 F.3d at 1369. Also, VirnetX did not narrow the ordinary meaning of these terms to overcome a rejection in prosecution; therefore, prosecution history disclaimer does not attach. *See Omega Eng'g*, 334 F.3d at 1324. In sum, because there is no limiting language in the claims, written description, or prosecution history requiring the Defendants' proposed limitations, they are extraneous and should be rejected. *See Clearwater Sys.*, 394 Fed. Appx. at 706.

E. Miscellaneous Dispute

1. "cryptographic information" [included in asserted claims of the '759 patent]

VirnetX's Proposed Construction	Defendants' Proposed Construction
information that is used to encrypt data or information that is used to decrypt data	information that is required in order to encode/decode or encrypt to ensure secrecy.

Finally, the parties dispute the construction of the claim term "cryptographic information." The Court previously construed this to mean "information that is encoded/decoded or encrypted to ensure secrecy." Both parties seem to agree that the "cryptographic information" refers to the information (*e.g.*, an encryption key) that is used to encrypt or decrypt data as opposed to the encrypted or decrypted information itself. VirnetX favors its proposed construction over the Defendants' because the Defendants' proposed construction is ambiguous at points. Specifically, the Defendants' proposed construction seems to require the inclusion of all conceivable information that is required to encrypt and decrypt information in order for it to be "cryptographic information." Also, the requirement of "ensur[ing] secrecy" seems that it might unnecessarily invite a collateral dispute over the encryption strength of the cryptographic information. For these reasons, the Court should adopt VirnetX's proposed construction for this term.

V. CONCLUSION

For the foregoing reasons, VirnetX respectfully requests that the Court adopt its proposed constructions of the disputed claim terms, and refuse Defendants' repeated invitations to rewrite entire blocks of claim language and to impermissibly import extraneous limitations.

DATED: November 4, 2011

Respectfully submitted,

McKOOL SMITH, P.C.
/s/ *Douglas A. Cawley*
Douglas A. Cawley, *Lead Attorney*
Texas State Bar No. 04035500
E-mail: dcawley@mckoolsmith.com
Bradley W. Caldwell
Texas State Bar No. 24040630
E-mail: bcaldwell@mckoolsmith.com
Luke F. McLeroy
Texas State Bar No. 24041455
E-mail: lmcleroy@mckoolsmith.com
Jason D. Cassady
Texas State Bar No. 24045625
E-mail: jcassady@mckoolsmith.com
John Austin Curry
Texas State Bar No. 24059636
E-mail: acurry@mckoolsmith.com
Daniel R. Pearson
Texas State Bar No. 24070398
E-mail: dpearson@mckoolsmith.com
Stacie Lynn Greskowiak
Texas State Bar No. 24074311
E-mail: sgreskowiak@mckoolsmith.com
McKool Smith P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Telephone: (214) 978-4000
Telecopier: (214) 978-4044

Sam F. Baxter
Texas State Bar No. 01938000
E-mail: sbaxter@mckoolsmith.com
McKOOL SMITH P.C.
104 East Houston, Suite 300
Marshall, Texas 75670
Telephone: (903) 923-9000
Telecopier: (903) 923-9099

Robert M. Parker
Texas State Bar No. 15498000
E-mail: rmparker@pbatyler.com
Robert Christopher Bunt
Texas State Bar No. 00787165
E-mail: rcbunt@pbatyler.com
PARKER, BUNT & AINSWORTH, P.C.
100 East Ferguson, Suite 1114
Tyler, Texas 75702
Telephone: (903) 531-3535
Telecopier: (903) 533-9687

ATTORNEYS FOR PLAINTIFF VIRNETX, INC.

CERTIFICATE OF SERVICE

The undersigned certifies that, on November 4, 2011, the foregoing document was served via the Court's ECF system on all counsel who has filed notices of appearance in this case.

/s/ Austin Curry
John Austin Curry