1   **WO**

2

3

4

5

6   **IN THE UNITED STATES DISTRICT COURT**

7   **FOR THE DISTRICT OF ARIZONA**

8

9   GoDaddy.com, LLC,   No. CV-14-00126-PHX-JAT

10   Plaintiff,   **ORDER**

11   v.

12   RPost Communications Limited, et al.,

13   Defendants.

14

15   Before the Court is Defendants'[1] Opening Claim Construction Brief (Doc. 114),

16   Plaintiff GoDaddy.com, LLC ("GoDaddy")'s Responsive Claim Construction Brief

17   (Doc. 117), and Defendants' Reply Claim Construction Brief (Doc. 119). On October 22,

18   2015, the Court conducted a *Markman* Hearing pursuant to *Markman v. Westview*

19   *Instruments, Inc.*, 517 U.S. 370 (1996). Consistent with *Markman*, the Court now

20   construes the claims in the patents-at-issue: (1) U.S. Patent No. 8,161,104 (filed April 17,

21   2012) (the "'104 Patent"); (2) U.S. Patent No. 8,209,389 (filed June 26, 2012) (the "'389

22   Patent"); (3) U.S. Patent No. 8,224,913 (filed July 17, 2012) (the "'913 Patent"); (4) U.S.

23   Patent No. 8,468,198 (filed June 18, 2013) (the "'198 Patent"); (5) U.S. Patent

24   No. 8,468,199 (filed June 18, 2013) (the "'199 Patent"); and (6) U.S. Patent

25   No. 6,182,219 (filed January 30, 2001) (the "'219 Patent").[2]

26   _____

27   [1] Defendants are RPost Communications Ltd.; RPost Holdings, Inc.; RPost
     International Ltd.; and RMail Ltd. Defendants are collectively referred to as "RPost."

28   [2] The '104, '389, '913, '198, and '199 Patents are referred to herein as the
     "Tomkow Patents." The '219 Patent is referenced as the "Feldbau Patent."

Table of Contents

- 3 -

I.   Background

The Tomkow Patents and Feldbau Patent claim, in broad terms, various systems and methods for tracking, authenticating, and verifying the transmission, delivery or non-delivery, opening, forwarding, content, and time events associated with an electronic message.

The Tomkow Patents are all rooted in the same parent application, which issued as U.S. Patent No. 7,966,372 ("'372 Patent"). Because the Tomkow Patents stem from the '372 Patent, they all share a similar specification and file history. The Field of Invention for each Tomkow Patent is directed to "a system and method for verifying delivery and content of an electronic message and, more particularly, to a system and method of later providing proof regarding the delivery and content of an e-mail message." '199 Patent col. 1 ll. 22–26.

As a general overview of the individual Tomkow Patents, the '104 Patent describes a system and method of verifying the opening of an electronic message sent from a sender to a recipient through a server. The '389 Patent furnishes a system and method to verify the receipt of an electronic message sent from a sender to a recipient through a server. The '913 Patent sets forth a system and method of verifying the delivery or non-delivery of an electronic message from a sender to a recipient through a server. The '198 Patent—a continuation of the '104 Patent—claims a system and method of verifying the opening and delivery of an electronic message sent from a sender to a recipient through a server. Finally, the '199 Patent—a continuation of the '389 Patent—provides a system and method of verifying the failure to deliver an electronic message sent from a sender to a recipient through a server.

In a similar manner, the Feldbau Patent is disclosed as "a method and apparatus for authenticating the dispatch and the contents of dispatched information in general." '219 Patent col. 1 ll. 6–8. In other words, the Feldbau Patent provides an apparatus and method of proving that the sender of a dispatch sent it to a particular recipient at a particular time and that it had a particular content.

II.   Legal Standard

A patent includes two basic components: (1) a written description of the invention, which is referred to as the "specification" of the patent, and (2) the patent claims. The claims of a patent define the scope of the invention to which the patentee is entitled. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). "The purpose of claim construction is to 'determin[e] the meaning and scope of the patent claims asserted to be infringed.'" *See O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1360 (Fed. Cir. 2008) (citation omitted). Claim construction is a question of law exclusively within the province of the Court. *See Markman*, 517 U.S. at 372. The Court need only construe claims, however, when the parties raise a dispute about the proper scope of a claim. *O2 Micro*, 521 F.3d at 1362. Moreover, if a disputed claim term has a plain and ordinary meaning such that it needs no clarification or explanation, the Court need not adopt a construction beyond that plain meaning. *See U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997).

When construing claims, the Court "look[s] to the words of the claims themselves," giving them "their ordinary and customary meaning" unless clearly stated otherwise. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). Claims should be considered as a whole, and terms used in multiple claims should be construed consistently. *See Inverness Med. Switz. GmbH v. Princeton Biomeditech Corp.*, 309 F.3d 1365, 1371 (Fed. Cir. 2002). "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips*, 415 F.3d at 1313; *see also Tex. Dig. Sys., Inc. v. Telegenix, Inc.*, 308 F.3d 1193, 1202 (Fed. Cir. 2002) ("The terms used in the claims bear a 'heavy presumption' that they mean what they say and have the ordinary meaning that would be attributed to those words by persons skilled in the relevant art.").

"[T]here is no magic formula or catechism for conducting claim construction." *Phillips*, 415 F.3d at 1324. Rather, the Court "looks to those sources available to the public that show what a person of skill in the art would have understood disputed claim

1   language to mean." *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381

2   F.3d 1111, 1116 (Fed. Cir. 2004). "Those sources include the words of the claims

3   themselves, the remainder of the specification, the prosecution history, and extrinsic

4   evidence concerning relevant scientific principles, the meaning of technical terms, and

5   the state of the art." *Id.* The Court is not "required to analyze [these] sources in any

6   specific sequence," but may not use extrinsic evidence to contradict "claim meaning that

7   is unambiguous in light of the intrinsic evidence." *Phillips*, 415 F.3d at 1324 (refining the

8   holding of *Vitronics*).

9   The specification "is the single best guide to the meaning of a disputed term."

10   *Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 711 F.3d 1348, 1361

11   (Fed. Cir. 2013) (quoting *Vitronics*, 90 F.3d at 1582). The patentee may "act as its own

12   lexicographer," *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed.

13   Cir. 2012), by defining a claim term in the specification as having "a different meaning

14   than [it] would otherwise have to a person of ordinary skill in the art," *Innova/Pure*

15   *Water*, 381 F.3d at 1116. *See also Vitronics*, 90 F.3d at 1582 (a specification "acts as a

16   dictionary when it expressly defines terms used in the claims or when it defines terms by

17   implication"). However, the Court will find the patentee to have acted as its own

18   lexicographer only if the patentee "clearly express[es] an intent to redefine the term."

19   *Thorner*, 669 F.3d at 1365 (citation and internal quotation marks omitted).

20   Similarly, the specification may narrow the scope of a disputed claim term if the

21   patentee has "demonstrate[d] intent to deviate from the ordinary and accustomed

22   meaning of a claim term by including in the specification expressions of manifest

23   exclusion or restriction, representing a clear disavowal of claim scope." *Thorner*, 669

24   F.3d at 1365 (quoting *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed.

25   Cir. 2002)). In ascertaining whether the patentee has disavowed the full scope of a claim,

26   the Court must not read limitations from the specification into the claims. *See Teleflex*,

27   299 F.3d at 1326 (citing *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1186

28   (Fed. Cir. 1998)). In other words, the claims are not necessarily limited to the

1   embodiments disclosed in the specification and courts must not read limitations from the
2   specification into the claims. *See SRI Int'l v. Matsushita Elec. Corp. of Am.*, 775 F.2d
3   1107, 1121 n.14 (Fed. Cir. 1985) (en banc). To avoid importing limitations, the court
4   must consider the purposes of the specification, which are to teach and enable those of
5   skill in the art to make and use the invention and to provide the best way for doing so. *See*
6   *Phillips*, 415 F.3d at 1317–18.

7   In addition to the specification, the Court considers "the patent's prosecution
8   history, if it is in evidence." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 980
9   (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996). "The purpose . . . is to 'exclude
10   any interpretation that was disclaimed during prosecution.'" *Chimie v. PPG Indus., Inc.*,
11   402 F.3d 1371, 1384 (Fed. Cir. 2005) (citation omitted). The prosecution history may
12   reveal that the patentee "has unequivocally disavowed a certain meaning to obtain [its]
13   patent." *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003). Thus,
14   the Court examines both the specification and prosecution history to ascertain whether
15   the patentee has disavowed the full scope of a claim term.

16   The Court may also consider extrinsic evidence to aid in its construction of
17   disputed claim terms. *See Phillips*, 415 F.3d at 1317–18. For example, "[d]ictionaries are
18   always available to the court to aid in the task of determining meanings that would have
19   been attributed by those of skill in the relevant art to any disputed terms used by the
20   inventor in the claims." *Tex. Dig. Sys.*, 308 F.3d at 1202 (citing *Vitronics*, 90 F.3d at 1584
21   n.6). Technical dictionaries are worthy of special note and constitute evidence of
22   understanding of persons of skill in the relevant art. *See Linear Tech. Corp. v. Impala*
23   *Linear Corp.*, 379 F.3d 1311, 1320 (Fed. Cir. 2004). Dictionaries are particularly helpful
24   in claim construction because they "endeavor to collect the accepted meanings of terms,"
25   *Phillips*, 415 F.3d at 1318, but the Court should not elevate dictionaries to prominence
26   over the specification and claim language, *see id.* at 1319–24. If a term has more than one
27   plausible ordinary meaning, the court must consult the intrinsic record to identify which
28   of the possible meanings is most consistent with the use of the words by the inventor.

Stephen Key Design LLC., v. Lego Sys., Inc., 261 F. Supp. 2d 1196, 1199 (N.D. Cal. 2003). Other extrinsic evidence, such as expert testimony, is less helpful because it may suffer from bias, and the Court should "discount any expert testimony 'that is clearly at odds with the claim construction mandated by the claims themselves, the written description, and the prosecution history, in other words, with the written record of the patent.'" *Phillips*, 415 F.3d at 1318 (quoting *Key Pharm. v. Hercon Labs. Corp.*, 161 F.3d 709, 716 (Fed. Cir. 1998)).

Finally, dependent claims must be construed to "incorporate by reference all the limitations of the claim[s] to which [they] refer[]." 35 U.S.C. § 112(d).

III.   Table of Construed Terms for the Tomkow Patents

The following chart summarizes the disputed claim terms for the Tomkow Patents, each party's proposed construction, and the Court's construction.

Term No.	Disputed Claim Term	Tomkow Patent Claims[3]	RPost's Proposed Construction	GoDaddy's Proposed Construction	The Court's Construction
1	"message"	All asserted claims in all Tomkow Patents	"an electronic message"	"an electronic message that can be transmitted as a whole through an electronic network"	"an electronic message"

---

[3] The asserted Tomkow Patent claims are: '104 Patent Claims 1, 9, 23, and 27; '389 Patent Claims 1, 5, 7, 12, 13, 14, and 15; '913 Patent Claims 1 and 2; '198 Patent Claims 1, 6, 7, 10, 18, 23, 32, 35, and 40; and '199 Patent Claims 1, 2, 3, and 7.

2	"server"	All asserted claims in all Tomkow Patents	Ordinary meaning. Alternatively, "a computer(s), computer program(s), or computing device(s) that provide resources to other devices across a network"	"the outgoing server, separate from the sender, that creates an attachment, transmits the attachment and the message, and stores the portion of the mail transport dialog generated during transmission of the message"	"a server that is separate from the sender"
3	"A link"	'104 Patent Claims 1 and 27 and their dependent claims; all asserted claims for '198 Patent	"a set of instructions that directs one computing resource to another"	Ordinary meaning.	The Court does not construe this term.
4	"an indication that the message has been opened by (delivered to) a recipient"	'104 Patent Claims 1 and its dependent claims; '198 Patent Claims 1, 6, 18, and 32 and their dependent claims	"information that indicates that the message has been opened by (delivered to) the recipient"	"confirmation (at the server) that the message content was viewed by the recipient"	"verifiable information that indicates that the message has been opened by (opened at; delivered to) the recipient"

5	"an indication of receipt of the message by the recipient (recipient processor)"	All asserted claims for '389 Patent	"information that indicates that the message has been received by the recipient (recipient processor)"	"confirmation that the message content was received by the recipient"	"verifiable information that indicates that the message was received by the recipient (recipient processor)"
6	"an indication of the failure to deliver the message to the recipient"	'199 Patent Claim 1 and its dependent claims	"information that indicates that the message has failed to be delivered to the recipient"	"confirmation that the message content was not received by the recipient"	"verifiable information that indicates the failure to deliver the message to the recipient"
7	"executing the link when the message is opened at the recipient to control the server to provide an indication that the message has been opened at the recipient"	'104 Patent Claim 1 and its dependent claims	"executing the link when the message is opened at the recipient to cause the server to provide an indication that the message has been opened at the recipient"	"action by the recipient when the message is opened at the recipient to control the server to provide proof that the message has been opened at the recipient, the proof providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"the link executing on its own when the message is opened at the recipient to control the server to provide verifiable information that indicates that the message has been opened at the recipient"

8	"the link being configured to execute automatically when the message is opened at the recipient processor to control the server to provide an indication at the server that the message has been opened at the recipient processor"	'104 Patent Claim 27 and its dependent claims	"the link programmed to execute automatically when the message is opened at the recipient to cause the server to provide an indication at the server that the message has been opened at the recipient"	"[link configured to execute through] action by the recipient when the message is opened at the recipient to control the server to provide proof that the message has been opened at the recipient, the proof providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"the link being configured to execute automatically when the message is opened at the recipient to control the server to provide verifiable information that indicates at the server that the message has been opened at the recipient processor"
9	"the link configured to execute when the link is activated at the recipient to provide an indication that the message has been opened by (delivered to) the recipient"	'198 Patent Claims 1, 18, and 32 and their dependent claims	"the link programmed to execute when the link is activated at the recipient to provide an indication that the message has been opened by (delivered to) the recipient"	"[link configured to execute through] action by the recipient when the message is opened at the recipient to control the server to provide proof that the message has been opened at the recipient, the proof providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"the link configured to execute when the link is activated at the recipient to provide verifiable information that indicates that the message has been opened by (delivered to) the recipient"

10	"executing the link when the link is activated at the recipient to control the server to provide an indication that the message has been delivered to the recipient"	'198 Patent Claim 1 and its dependent claims	"executing the link when the link is called at the recipient to cause the server to provide an indication that the message has been delivered to the recipient"	"[executing the link through] action by the recipient when the message is opened at the recipient to control the server to provide proof that the message has been opened at the recipient, the proof providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"the link executing on its own when the link is activated at the recipient to control the server to provide verifiable information that indicates that the message has been delivered to the recipient"
11	"wherein the link is executed when the link is activated at the recipient to control the server to provide an indication that the message has been opened at (delivered to) the recipient"	'198 Patent Claims 18 and 32 and their dependent claims	"wherein the link is executed when the link is called at the recipient to cause the server to provide an indication that the message has been opened at (delivered to) the recipient"	"[link is executed through] action by the recipient when the message is opened at the recipient to control the server to provide proof that the message has been opened at the recipient, the proof providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"wherein the link is executed when the link is activated at the recipient to control the server to provide verifiable information that indicates that the message has been opened at (delivered to) the recipient"

12	"authenticatible information"	'104 Patent Claim 1 and its dependent claims; all asserted claims for '198 Patent	"information regarding the content or delivery of a message that can be verified"	"information unique to the message, the digital signature of the message, and the portion of the mail transport dialog generated during transmission of the message"	"information unique to the content or delivery of a message that can be verified"
13	"mail transport protocol dialog"	All asserted claims for '389 Patent	"mail transport data including a sequence of at least one command and at least one response"	"a list of commands and responses exchanged between servers during transmission of the message that is sufficient to prove delivery of the message to the recipient, providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"data including a sequence of at least one mail transport protocol command and at least one mail transport protocol response exchanged between devices during transmission of the message"

14	"at least a portion of a mail transport protocol dialog (data transport dialog) generated (by the electronic mail system) during transmission of the message from the server to the recipient (processor)"	All asserted claims for '389 Patent; '199 Patent Claim 1 and its dependent claims	No further construction necessary	"a list of commands and responses exchanged between servers during transmission of the message that is sufficient to prove delivery of the message to the recipient, providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"data including at least one mail transport protocol command or at least one mail transport protocol response exchanged between devices during transmission of the message"
15	"SMTP and ESMTP protocol dialog"	All asserted claims for '913 Patent	"SMTP or ESMTP data including a list of at least one command and at least one response generated by the electronic mail system during transmission of the message from the server to the recipient"	"a list of commands and responses exchanged between servers during transmission of the message that is sufficient to prove delivery of the message to the recipient, providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"SMTP or ESMTP data including a list of at least one protocol command and at least one protocol response exchanged between devices during transmission of the message"

16	"data transport dialog"	'199 Patent Claim 1 and its dependent claims	"transport data including a sequence of at least one command and at least one response"	"a list of commands and responses exchanged between servers during transmission of the message that is sufficient to prove delivery of the message to the recipient, providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"transport data including a list of at least one command and at least one response exchanged between devices during transmission of the message"
17	"before the message is authenticated (any authentication of the message) by the server"	'389 Patent claims 1, 12, 14, and 15 and their dependent claims; '199 Patent Claim 1 and its dependent claims	"before the content and delivery of the message is proved (proving the content and delivery of the message) by the server" The plain language of this phrase does not require that any authentication of the message be performed by the server.	"before proving the content and delivery of the message by comparing and matching authenticable information so as to provide a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"before the content and delivery of the message is proved (proving the content and delivery of the message) by the server"

18	"Mail Transport Agent"	All asserted claims for '913 Patent	"software that transfers electronic messages from one computer to another"	"software that resides on the server and that is dedicated to transferring and receiving electronic messages from one computer to or from another"	"software that resides on a server and that transfers and receives electronic messages from one computer to or from another"
19	"sender"	All asserted claims in all Tomkow Patents	Ordinary meaning. Alternatively: "originator of a message"	"the computer that originates the message"	"a combination of (1) the user that caused the computerized device to originate the message and (2) the computerized device itself"
20	"recipient"	All asserted claims in all Tomkow Patents	Ordinary meaning. Alternatively: "who the sender intends to receive the message"	"the computer that receives the message at its intended destination"	"a combination of (1) the user that the sender intends to receive the message and (2) the computerized device that receives the message"

21	"originating processor"	'104 Patent Claim 27 and its dependent claims; '389 Patent Claim 7 and its dependent claims	Ordinary meaning. Alternatively: "a computing device where the message originates"	"the computer that originates the message"	"the computerized device where the message originates"
22	"recipient processor"	'104 Patent Claim 27 and its dependent claims; '389 Patent Claim 7 and its dependent claims	Ordinary meaning. Alternatively: "a computing device where the recipient receives the message"	"the computer that receives the message at its intended destination"	"the computerized device that receives the message"
23	"providing proof of receipt of the message by the recipient processor"	'389 Patent Claim 7	This phrase appears in the preamble and is not limiting.	"providing evidence that confirms receipt of the message by the recipient, the evidence providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	"proving that the message was received by the recipient processor"

24	"the link configured to execute when the message is opened at the recipient"	'104 Patent Claims 1 and 27 and their dependent claims	"the link programmed to execute when the message is opened at the recipient"	"[link configured to execute through] action by the recipient when the message is opened at the recipient to control the server to provide proof that the message has been opened at the recipient, the proof providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail"	The Court does not construe this term.
25	"the server (being) displaced from the recipient (recipient processor)"	'104 Patent Claims 1 and 23 and their dependent claims; '389 Patent Claims 1, 7, 14, and 15 and their dependent claims; all asserted claims for '199 Patent; '198 Patent Claim 1 and its dependent claims	"the server (being) logically displaced from the recipient (recipient processor)"	Ordinary meaning	The Court does not construe this term.

26	"the server constructs authenticatible information related to the message"	'104 Patent Claim 27 and its dependent claims	"the server assembles authenticatible information related to the message"	"authenticatible information related to the message" should be construed as "information unique to the message, the digital signature of the message, and the portion of the mail transport dialog generated during transmission of the message"	The Court construes "authenticatible information" as set forth above and does not construe the remainder of the term.

IV. Table of Construed Terms for the Feldbau Patent

The following chart summarizes the disputed claim terms for the Feldbau Patent, each party's proposed construction, and the Court's construction.

Term No.	Disputed Claim Term	Feldbau Patent Claims[4]	RPost's Proposed Construction	GoDaddy's Proposed Construction	The Court's Construction
1	"authenticating the dispatch and contents of the dispatch"	All asserted claims	"provide evidence capable of being used to prove the contents of the dispatch"	"proving the contents and the receipt of a dispatch by using reliable evidence on par with that used to notarize documents or to admit as evidence in a court of law"	"providing evidence that is capable of being used to prove both the dispatch and the contents of the dispatch"

---

[4] The asserted Feldbau Patent claims are: 60, 62, 66, 69, 82, 86, and 88. On June 19, 2012, an Ex Parte Reexamination Certificate was issued for the Feldbau Patent. All disputed terms of the Feldbau Patent involve claims amended by the reexamination.

| 2 | "authentication data" | All asserted claims | "information that is associated with the contents of the dispatch by generating a representation of at least content data, an indicia of a time of successful transmission of the dispatch to the recipient, and an indicia relating to the destination of the dispatch, the representation comprising one or more elements" | "information that is associated with the contents of the dispatch by generating a representation of at least the elements a1, a2 and a3, the representation comprising one or more elements" | "information that is associated with the contents of the dispatch by generating a representation of at least (1) content data; (2) an indicia of a time of successful transmission of the dispatch to the recipient, said indicia being recorded by an authenticator and provided in a manner that is resistant to or indicative of tampering by either sender or recipient; and (3) an indicia relating to the destination of the dispatch; where the representation is comprised of one or more elements" |

3	"dispatch record data"	All asserted claims	"information relating to the dispatch"	"data recorded by the authenticator during the transmission of the dispatch, which includes at least the time related indicia and the indicia relating to the destination of the dispatch, and which does not include the content data representative of the contents of the dispatch"	"information relating to the dispatch but not relating to content data representative of the contents of the dispatch"
4	"an indicia of time of successful transmission of the dispatch to the recipient"	Claim 60 and its dependent claims	"data that represents the time at which the dispatcher forwarded the dispatch for delivery such that the recipient may later be able to receive the dispatch and where the data is obtained without any cooperation from the recipient"	"data that represents the actual time at which the dispatcher completed transmission of the dispatch for delivery, such that the recipient may later be able to receive the dispatch and where the data is obtained without any cooperation from the recipient"	"data that represents the time at which the dispatcher forwarded the dispatch for delivery such that the recipient may later be able to receive the dispatch and where the data is obtained without any cooperation from the recipient"

5	"sender"	All asserted claims	Ordinary meaning	"the computer that originates the dispatch"	"a combination of (1) the user that caused the computerized device to originate the dispatch and (2) the computerized device itself"
6	"recipient"	All asserted claims	Ordinary meaning	"the computer that receives the dispatch at its intended destination"	"a combination of (1) the user that the sender intends to receive the message and (2) the computerized device that receives the message"

| 7 | "processor for associating" | Claim 82 and its dependent claims | Ordinary meaning; claim term is not indefinite and is not subject to 35 U.S.C. §112(6) | Indefinite.

Function: associating the content data with dispatch record data and generating the authentication data

Structure: None. | Claim term is subject to 35 U.S.C. §112(6).

Function: Associating the content data with dispatch record data and generating the authentication data.

Structure: A function executor 102, which may be a Microchip Technology Inc.'s PIC16C5x series EPROM-based micro-controller, that associates a set of information elements ("A") by applying an association function ("F") to generate another set of information elements ("B"), i.e., $B=F(A)$; and its equivalents. |

| 8 | "means for providing an indicia of a time of successful transmission of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient" | Claim 82 and its dependent claims | **Function**: Providing an indicia of a time of successful transmission of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient

Structure: (1) Internal clock 50 (2) Communications network server (3) Secure time generator 104 (4) Digital Notary System (DNS); and their equivalents | **Function:** Agreed to by the parties.

Structure: A secure clock internal to the authenticator or a time stamping service such as the Digital Notary System (DNS) external to the authenticator that is secured from being set or modified by an interested party such as the sender. | **Function:** Providing an indicia of a time of successful transmission of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient.

Structure: Either a (1) securable clock 50 and equivalents thereof; (2) time generator 104 and equivalents thereof; (3) communications network server and equivalents thereof; or (4) Time Stamping Service, such as the Digital Notary System, and equivalents thereof; where structures (1) and (2) are internal to the authenticator, structures (3) and (4) are external to the authenticator, and structures (2), (3) and (4) are secured from being set or modified by an interested party such as the sender. |

| 9 | "means for securing at least part of the authentication data against tampering by the sender and the recipient; wherein the processor is combined with the means for securing" | Claim 82 and its dependent claims | **Function**: Securing at least part of the authentication data against tampering by either the sender or the recipient

Structure: Storage unit 54 or storage device 106, and their equivalents | **Function:** Agreed to by the parties.

Structure: Using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof, such as those employed by the widely used RSA encryption method, and by the PKZIIP(tm) program from PKWARE Inc., Glendale, Wis., U.S.A., and where the "securing" procedure, key or password are unknown to any interested party. | **Function:** Securing at least part of the authentication data against tampering by either the sender or the recipient.

Structure: Storing the data either (1) on a write-once read-many ("WORM") device such as an optical disk or a Programmable Read-Only Memory ("PROM") device; or (2) using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof, such as those employed by the widely used RSA encryption method, and by the PKZIIP(tm) program from PKWARE Inc., Glendale, Wis., U.S.A., and where the "securing" procedure, key or password are unknown to any interested party. |

| 10 | "source transmitting system" | Claim 82 and its dependent claims | "system for transmitting a dispatch for a sender" | "the computer that originates the dispatch" | "computerized system for transmitting a dispatch for a sender" |
| 11 | "destination receiving system" | Claim 82 and its dependent claims | "system for receiving a dispatch for a recipient" | "the computer that receives the dispatch at its intended destination" | "computerized system for receiving a dispatch for a recipient" |

V. Table of Construed Terms on Which the Parties Agree

The Court adopts the parties' stipulated constructions of the four Feldbau Patent claim terms as set forth in the box below.

Term No.	Claim Term	Feldbau Patent Claims	Stipulated Construction
1	"dispatch"	All asserted claims	"the transmission sent from a sender toward a recipient via a dispatcher"
2	"authenticator"	All asserted claims	"a sub-system that operates to authenticate a dispatch"
3	"non-interested third party"	All asserted claims	"a party who carries out the authentication function without bias and without the participation of the sender or the recipient"
4	"contents of the dispatch / content data"	All asserted claims	"the entire content the sender originates for sending to the recipient"

1   **VI.   Construction of Disputed Claim Terms in the Tomkow Patents**

2   **A.   "message" (Term No. 1)**

3   **1.   The Parties' Positions**

4   RPost argues that the claim term "message" should be construed as "an electronic

5   message." (Doc. 191-1 at 1). RPost explains that Judge Rodney Gilstrap of the Eastern

6   District of Texas ("EDTX") construed "message" as "an electronic message" and urges

7   the Court to adopt the same construction. (Doc. 114 at 7–8).[5]

8   In response, GoDaddy agrees that "message" should be construed as "electronic"

9   but disputes the adequacy of that description. (Doc. 117 at 6–7). Specifically, GoDaddy

10   maintains that "message" should also be limited by how the message is transmitted

11   ("through an electronic network") and by its singularity ("as a whole"). (*Id.*) To support

12

13   [5] Many of the disputed terms in this case were construed by Judge Gilstrap in
2013. *See RMail Ltd. v. Amazon.com, Inc.*, 2013 WL 968246 (E.D. Tex. Mar. 12, 2013).
14   At issue before Judge Gilstrap was the Feldbau Patent; the '372 Patent; and U.S. Patent
No. 7,865,557 ("'557 Patent"), which is a division of the '372 Patent. Several of the
15   Tomkow Patents ('104, '389, '198, and '199 Patents) are continuations of the '372
16   Patent, while the '913 Patent is a division of the '557 Patent.

17   One of the disputed terms in the Feldbau Patent was also construed by Judge
18   James Selna of the Central District of California in *Propat Int'l Corp. v. RPost Inc.*, 2005
WL 6287844 (C.D. Cal. Jan. 14, 2005) ("*Propat*"). All substantive rulings in *Propat* were
19   subsequently vacated, however, when the court determined that the plaintiff, Propat
20   International Corporation, lacked standing. *See Propat Int'l Corp. v. RPost Inc.,* 2005
WL 6233792 (C.D. Cal. Nov. 28, 2015).
21

22   For many of the thirty-seven disputed terms in this case, a party advocates that the
Court should adopt a construction as crafted by Judge Gilstrap or Judge Selna. Even if
23   these constructions were from this district, however, they would not be binding on the
Court. The cases before Judge Gilstrap and Judge Selna involved different defendants,
24   making issue preclusion inapplicable here. There is, nonetheless, an interest in *stare
25   decisis* and uniformity in treatment of the same patent. *See Markman*, 517 U.S. at 390–
91. Prior constructions may be used as persuasive precedent, but that does not foreclose
26   the Court from reaching a different conclusion. *See Verizon Cal. Inc. v. Ronald A. Katz
27   Licensing, L.P.*, 326 F. Supp. 2d 1060, 1069 (C.D. Cal. 2003); *Nilssen v. Motorola, Inc.*,
80 F. Supp. 2d 921, 924 n.4 (N.D. Ill. 2000). Consequently, the Court will consider the
28   prior constructions of Judge Gilstrap and Judge Selna but only for their persuasive value.

1 these added limitations, GoDaddy observes that the shared specification discloses that the

2 invention "may apply to any electronic message that can be transmitted through an

3 electronic message network." (*Id.* at 7 (quoting '199 Patent col. 27 ll. 26–32)). GoDaddy

4 further contends that a "message" must be sent "as a whole" because the term "message"

5 is always preceded in the claims by the articles "a" or "the." (*Id.*) GoDaddy therefore

6 proposes a construction of: "an electronic message that can be transmitted as a whole

7 through an electronic network." (Doc. 191-1 at 1).

8   RPost replies that GoDaddy's "as a whole" limitation is unsupported by the

9 intrinsic record and will confuse the jury. (Doc. 119 at 3). RPost also contends that

10 GoDaddy's "cherry-picked" limitation of "through an electronic network" does not

11 describe a feature of the message and also neglects to include a second transmission

12 method disclosed in the same sentence of the specification. (*Id.* at 4).

13   **2.   Analysis**

14   The term "message" is used in all asserted claims of the Tomkow Patents. For

15 example, the '199 Patent claims:

16   **1**. A method of transmitting a message from a sender to a recipient
   through a server displaced from the recipient, the steps at the server
17 comprising:

18   receiving the *message* at the server from the sender;

19   transmitting the *message* to the recipient

20   . . .

21   receiving at the server from the recipient an indication of the failure
   to deliver the *message* to the recipient . . . .
22
23 '199 Patent col. 27 ll. 58–65 (emphasis added). Another example is found in the '198

   Patent which claims:
24
       1. A method of transmitting a message from a sender to a recipient
25 and providing an indication that the message was opened by the recipient,
   comprising:
26
           receiving the *message* at a server from the sender, the server being
27 displaced from the recipient,

28

1   associating a link with the *message* by the server . . .

2   transmitting the *message* . . . from the server to the recipient . . . .

3 '198 Patent col. 28 ll. 6–16 (emphasis added).

4   Because the parties do not dispute that "message" should be construed as

5 "electronic," the Court will, at a minimum, adopt RPost's proposed construction of "an

6 electronic message." The remaining question is whether "an electronic message" should

7 be cloaked with the limitations proposed by GoDaddy.

8   Regarding GoDaddy's first proposed limitation "as a whole," the Court is not

9 persuaded by GoDaddy's argument that because certain articles precede "message" in the

10 claim language, there is somehow a requirement that the message must be sent "as a

11 whole." Beyond referencing the claims' use of "a" and "the," GoDaddy does not cite any

12 other portion of the intrinsic record to show that "a message" cannot be transmitted in

13 multiple components. Accordingly, the Court rejects this portion of GoDaddy's proposal

14 because it would ambiguously construe a readily understandable term.

15   As to GoDaddy's second proposed limitation "through an electronic network," the

16 Court finds that such a limitation is not supported by the intrinsic record. The asserted

17 claims of the Tomkow Patents do not require that messages be transmitted only through

18 electronic networks. In fact, the portion of the shared specification relied upon by

19 GoDaddy actually sets forth two means of transmitting a message. *See* '199 Patent col. 27

20 ll. 26–32 ("Although the above generally describes a system and method of verifying that

21 an e-mail was sent and/or received, the present invention may apply to any electronic

22 message that can be transmitted through an electronic message network *or through an*

23 *electronic gate*." (emphasis added)). GoDaddy, without explanation, severed the

24 "electronic gate" transmission method in its proposal. In any event, the Court finds that

25 appending this method of transmission limitation to "message" is needlessly redundant

26 considering the parties agree that "message" must be "electronic." Thus, the Court rejects

27 this portion of GoDaddy's proposed construction.

28

1   For these reasons, the Court adopts RPost's proposal and construes "message" as

2   "an electronic message."

3   **B.   "server" (Term No. 2)**

4   **1.   The Parties' Positions**

5   RPost recommends that the Court should shadow Judge Gilstrap and abstain from

6   construing the term "server." (Doc. 114 at 8–9). Judge Gilstrap concluded that defining

7   "server" was unnecessary because the term had been used by the asserted claim

8   according to its plain and ordinary meaning. *See RMail*, 2013 WL 968246, at *60. RPost

9   also advances an alternative construction: "a computer(s), computer program(s), or

10   computing device(s) that provides resources to other devices across a network."

11   (Doc. 191-1 at 1). This alternative construction closely tracks RMail's proposal that

12   Judge Gilstrap rejected as "not derived from intrinsic evidence." *RMail*, 2013 WL

13   968246, at *60.

14   GoDaddy responds that "server" must be interpreted because there is "no plain

15   meaning that resolves the parties' dispute." (Doc. 117 at 7–8). According to GoDaddy,

16   "server" must: 1) be "outgoing"; 2) be "separate from the sender"; 3) "create an

17   attachment"; 4) "transmit the attachment and message"; and 5) "store the portion of the

18   mail transport dialog generated during transmission of the message." (*Id.*)

19   RPost replies that GoDaddy's limitations are improper because they "cannot apply

20   to all of the claims." (Doc. 119 at 4). RPost also contends that GoDaddy's limitations are

21   ambiguous and unsupported by the intrinsic record. (Doc. 114 at 8–9).

22   **2.   Analysis**

23   The term "server" is used by all asserted claims of the Towkow Patents but is not

24   defined or explained within the intrinsic record. A few examples include:

25   **1**. A method of transmitting a message from a sender to a recipient

26   through a server displaced from the recipient, the steps at the server
     comprising:

27   receiving the message at the *server* from the sender

28   . . .

receiving at the *server* at least a portion of a mail transport protocol dialog generated during transmission of the message from the *server* to the recipient; and

receiving at the *server* from the recipient an indication of the receipt of the message by the recipient;

forming at the *server* a first information from the at least a portion of the mail transport protocol dialog and the indication of the receipt of the message by the recipient; and

transmitting, before any authentication of the message, a copy of the message and the first information to the sender from the *server*.

'389 Patent col. 27 ll. 58–col 28 ll. 7 (emphasis added).

7. A system for transmitting a message through an electronic mail system from an originating processor to a recipient processor and providing proof of receipt of the message by the recipient process, comprising:

a *server* displaced from the originating processor, the *server* capable of being configured by software commands . . . .

Id. col. 28 ll. 33–39 (emphasis added).

32. A system transmitting a message from a sender to a recipient and providing an indication that the message was opened by the recipient, comprising:

a *server* in electronic communication with the sender and receiver, the *server* programmed to receive a message from the sender, to associate a link with the message, the link configured to execute when the link is activated at the recipient to provide an indication that the message has been delivered to a recipient, to transmit the message and the link from the *server* to the recipient, wherein

the link is executed when the link is activated at the recipient to control the *server* to provide an indication that the message has been delivered to the recipient; and

wherein the *server* is programmed to form an authenticatible information related to the message, and to transmit the indication of the delivery of the message to the recipient and the authenticatible information from the *server* to the sender.

'198 Patent col. 30 ll. 7–25 (emphasis added).

1. A method of transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:

- 31 -

. . .

> Recording at the *server* some portion of the selected one of the SMTP and ESMTP protocol dialog between the *server* and the recipient through the *server* including those portions of the selected one of the SMTP and ESMTP protocol dialog between the *server* and the recipient in which the receiving Mail Transport Agent accepts or declines delivery of the transmitted message.

'913 Patent col. 27 ll. 41–54 (emphasis added).

Initially, despite GoDaddy's argument that no "plain meaning" of "server" resolves the parties' dispute, GoDaddy does not raise an actual dispute concerning the plain meaning of the term. Particularly, GoDaddy's proposed construction *includes* the word "server" and shrouds it with five limitations. For example, GoDaddy's proposal states that "server" must be an "outgoing server." While this construction limits "server" as "outgoing," it does not raise an actual dispute as to the "plain meaning" of the word "server." Likewise, the balance of GoDaddy's proposal affixes several limitations to "server" without challenging the plain meaning of the term. Accordingly, the question presented by GoDaddy is not whether the plain meaning of "server" is disputed, but whether the proposed limitations should be levied upon the term.

The Court will review each of GoDaddy's proposed limitations in turn.

a. "outgoing server"

GoDaddy proposes that "server" must be construed as "outgoing server" but does not cite to the intrinsic record for support. *See* (Doc. 117 at 3–4). The Tomkow Patents, however, consistently specify that the server can both receive and transmit messages. *See, e.g.*, '389 Patent col. 27 ll. 59–61 (claiming "steps at the server comprising: receiving the message at the server from the sender . . . ."). If GoDaddy intended to limit "server" to only servers that send messages and not ones that receive messages, such a construction violates the intrinsic record. In absence of more compelling evidence, the Court rejects GoDaddy's proposed limitation of "outgoing."

b. "separate from the sender"

GoDaddy also proposes that "server" should be limited as "separate from the sender." (Doc. 117 at 7–8). RPost's sole dispute with this limitation is that it is redundant because "server" and "sender" are "distinct claim elements." (Doc. 114 at 9). RPost observes that several courts have spurned—on "redundancy" grounds—constructions that incorporate language from the claim itself. (Doc. 119 at 4 (citing *Interdigital Commuc'ns., Inc. v. ZTE Corp.*, 2014 WL 3908771, at *1 (D. Del. Aug. 8, 2014); *Asetek Holdings, Inc. v. Coolit Sys.*, 2013 WL 6327691, at *4 (N.D. Cal. Dec. 3, 2013); *Ferring B.V. v. Watson Labs., Inc.*, 2013 WL 499158, at *7 (D. Nev. Feb. 6, 2013)). The Federal Circuit, however, rejected the robotic application of such a stringent rule. *See 01 Communique Lab., Inc. v. LogMeIn, Inc.*, 687 F.3d 1292, 1296 (Fed. Cir. 2012) ("[Plaintiff] argues that because those functions are set forth expressly in the claim, it would be 'redundant and unnecessary' to incorporate them into the construction of 'location facility.' However, [Plaintiff] has not cited, and we have not discovered, any authority for the proposition that construction of a particular claim term may not incorporate claim language circumscribing the meaning of the term. The claim language makes clear that the location facility in fact does perform the functions in question. The district court correctly incorporated those functions into its claim construction."). Thus, RPost's "redundancy" argument, while persuasive, is not binding on the Court.

RPost never disputes that the claimed "server" is, in fact, "separate from the sender," and on balance, the Court concludes that construing "server" with the limitation "separate from the sender" would be more helpful to the jury than a plain meaning construction. The Court therefore adopts this portion of GoDaddy's construction.

c. "creates an attachment, transmits the attachment and the message"

As a third limitation, GoDaddy argues that the server "creates an attachment [and] transmits the attachment and the message." (Doc. 117 at 8). GoDaddy, however, does not point to claim language that requires the server to "create" or "transmit" an "attachment."

1 The only claim language cited by GoDaddy concerns the role of the processor to

2 "associate a link with the message" or "add[] a link to the message," but these claims are

3 all dependent claims. (*Id.* (citing '198 Patent col. 28 ll. 6–25, col. 29 ll. 13–19; '104

4 Patent col. 27 ll. 66–col. 28 ll. 4, col. 31 ll. 24–37)). GoDaddy does not explain why the

5 Court should interpret "link" as "attachment" or how "associate" or "add" is analogous to

6 "creates." Without a more compelling reason for construing "server" with a limitation

7 found only in dependent claims, the Court rejects this portion of GoDaddy's proposal.

8 *See Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004) ("[T]he

9 presence of a dependent claim that adds a particular limitation raises a presumption that

10 the limitation in question is not found in the independent claim." (citing *Wenger Mfg.,*

11 *Inc. v. Coating Mach. Sys., Inc.*, 239 F.3d 1225, 1233 (Fed. Cir. 2001))).

12   Regarding the balance of this third limitation, the claim language is clear that the

13 server "transmits" the message. *See, e.g.*, '198 Patent col. 28 ll. 15–16, col. 29 ll. 13–19.

14 Accordingly, the Court rejects this part of GoDaddy's proposal as needlessly redundant.

15   **d.   "stores the portion of the mail transport dialog generated**
                               during transmission of the dispatch"
16

17   As a fourth limitation, GoDaddy insists that the construction must include that the

18 server "stores the portion of the mail transport dialog generated during transmission of

19 the dispatch." (Doc. 117 at 8). During the *Markman* Hearing, GoDaddy explained that the

20 server must store this information to later verify the message.

21   Only two asserted claims recite that the server stores any portion of the mail

22 transport dialog, and both are dependent claims found in only one Tomkow Patent. *See*

23 '389 Patent, Claims 12 and 14.[6] Had the inventor wanted to limit any of the asserted

24 independent claims in this manner, he certainly could have done so. As quoted above, the

25 Federal Circuit has held, "the presence of a dependent claim that adds a particular

26

27   [6] The "storing" function is also found in asserted claims of the '913 Patent and
'199 Patent, but neither relates to "mail transport dialog" and both are dependent claims.
28 *See* '913 Patent, Claim 2; '199 Patent, Claim 2.

- 34 -

1 limitation raises a presumption that the limitation in question is not found in the

2 independent claim." *Liebel-Flarsheim*, 358 F.3d at 910 (citing *Wenger Mfg.*, 239 F.3d at

3 1233). Further, "where the limitation that is sought to be 'read into' an independent claim

4 already appears in a dependent claim, the doctrine of claim differentiation is at its

5 strongest." *Id.*; *see SunRace Roots Enter. Co., Ltd. v. SRAM Corp.*, 336 F.3d 1298, 1302–

6 03 (Fed. Cir. 2003) (the presumption that an independent claim does not have a limitation

7 that is introduced for the first time in a dependent claim "is especially strong when the

8 limitation in dispute is the only meaningful difference between an independent and

9 dependent claim, and one party is urging that the limitation in the dependent claim should

10 be read into the independent claim"); *Wenger Mfg.*, 239 F.3d at 1233 ("Claim

11 differentiation . . . is clearly applicable when there is a dispute over whether a limitation

12 found in a dependent claim should be read into an independent claim, and that limitation

13 is the only meaningful difference between the two claims.").

14   A claim term should be construed in a manner that can be applied to all claims.

15 *See Inverness Med. Switz. GmbH*, 309 F.3d at 1371. Here, for all but two dependent

16 claims, "server" is not limited to "storing" mail transport dialog. Moreover, none of the

17 asserted claims from the '104 and '198 Patents even use the term "mail transport protocol

18 dialog." Accordingly, the Court rejects this portion of GoDaddy's proposal.

19   **3.**   **Conclusion**

20   For these reasons, the Court construes "server" as "a server that is separate from

21 the sender."

22   **C.**   **"a link" (Term No. 3)**

23   **1.**   **The Parties' Positions**

24   RPost argues that "a link" should be construed as "a set of instructions that directs

25 one computing resource to another." (Doc. 114 at 9–10). RPost claims that such an

26 interpretation is "fully supported by the intrinsic record." (*Id.*)

27

28

1   GoDaddy responds that no construction is necessary because "a link" is a readily

2   understandable term to a skilled artisan. (Doc. 117 at 8). GoDaddy further contends that

3   RPost's construction broadens the scope of "a link" contrary to the intrinsic record. (*Id.*)

4   RPost replies that GoDaddy "completely ignores that the Tomkow patents

5   describe links as akin to instructions." (Doc. 119 at 5). RPost also states that a "person of

6   ordinary skill in the art would understand that links, such as URLs, may contain

7   commands, or instructions, that direct one computing resource to another." (*Id.*)

8   **2.   Analysis**

9   The Court finds that a person of ordinary skill in the art would understand the

10   functions "a link" performs without additional construction. As RPost concedes: "[a]

11   person of ordinary skill in the art would understand that links, such as URLSs, may

12   contain commands, or instructions, that direct one computing resource to another."

13   (Doc. 119 at 5). The internal record also makes clear that "a link" is "added to the

14   message by the server," is "configured to execute when the message is opened" in order

15   to "provide an indication that the message has been opened." '104 Patent col. 28 ll. 1–4,

16   col. 31 ll. 25–31; '198 Patent col. 28 ll. 11–14, col. 29 ll. 14–19. If a disputed claim term

17   has a plain and ordinary meaning such that it needs no clarification or explanation, the

18   Court need not adopt a construction beyond that plain meaning. *See U.S. Surgical*, 103

19   F.3d at 1568. RPost failed to cite any portion of the intrinsic record to show that "a link"

20   was used in a way other than its plain meaning.

21   For these reasons, the Court does not construe this term.

22   **D.   "an indication that the message has been opened by (delivered to) a
         recipient" (Term No. 4)**

23

24   **1.   The Parties' Positions**

25   RPost argues that "indication" should be broadly interpreted as "information that

26   indicates" and supports its position by citing the Meriam Webster Dictionary. (Doc. 114

27   at 10). RPost thus proposes a construction of "information that indicates that the message

28   has been opened by (delivered to) a recipient." (Doc. 191-1 at 1).

1   GoDaddy responds that RPost's "circular" definition should be rejected. (Doc. 117

2   at 9). Instead, GoDaddy proposes a construction of "confirmation (at the server) that the

3   message content was viewed by the recipient." (Doc. 191-1 at 1). To buttress its

4   definition of "indication" as "confirmation," GoDaddy heavily relies on Figure 8 of the

5   '199 Patent and its corresponding description. (Doc. 117 at 9). Figure 8—a preferred

6   embodiment of the '199 Patent—depicts the invention as sending a "confirmation

7   message" to the sender, which provides "verifiable confirmation" that the message was

8   received at a certain time, by a certain network route, and with specific content. '199

9   Patent Fig. 8, col. 25 ll. 49–col. 26 ll. 5. GoDaddy insists that the claimed "indication"

10   must have "certainty of content and provenance." (Doc. 117 at 9). GoDaddy also defines

11   "opened" as "viewed" because, according to the specification, "the message is opened for

12   reading," and GoDaddy argues that a message cannot be read without at some point being

13   viewed. (*Id.* at 10).

14   RPost argues that GoDaddy's proposal is a shrewd and misguided attempt to

15   narrow the plain meaning of the claimed "indication." *See* (Docs. 114 at 10; 119 at 5–6).

16   According to RPost, the patentee intentionally claimed "indication" in a broad manner

17   and "[a]bsent a clear disavowal in the specification or the prosecution history, the

18   patentee is entitled to the full scope of its claim language." (Doc. 119 at 6 (citing *Home

19   Diagnostics, Inc. v. LifeScan, Inc.*, 381 F.3d 1352, 1358 (Fed. Cir. 2004))). RPost

20   contends that the patentee did not make a "clear disavowal" of the full meaning behind

21   "indication," and thus, GoDaddy's proposal improperly imports a limitation from the

22   specification into the claim. (Doc. 114 at 10). RPost further observes that Figure 8's

23   corresponding description "undermines" GoDaddy's argument because "confirmation

24   message 72" is an "optional message" that "may or may not include verifiable

25   information" and can merely be a "simple text message *indicating* that a message was

26   received." (Doc. 119 at 5). Finally, RPost complains that GoDaddy's construction of

27   "opened" as "viewed" is improper because it narrows the meaning of the term without

28   adequate intrinsic record support. (Doc. 114 at 10).

2. Legal Standard

A fundamental principle for discerning a term's usage is the ordinary and accustomed meaning of the words amongst artisans of ordinary skill in the relevant art at the time of invention. *See Rexnord Corp. v. Laitram Corp.*, 274 F.3d 1336, 1342 (Fed. Cir. 2001). Normal rules of usage suggest a "heavy presumption" that claim terms carry their accustomed meaning in the relevant community at the relevant time. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002) (citing *Johnson Worldwide Assocs. Inc. v. Zebco Corp.*, 175 F.3d 985, 989 (Fed. Cir.1999)). Of course, the Federal Circuit acknowledges that a patent applicant may overcome this presumption by clearly using the words in the specification, prosecution history, or both "in a manner inconsistent with its ordinary meaning." *Boehringer Ingelheim Vetmedica, Inc. v. Schering–Plough Corp.*, 320 F.3d 1339, 1347 (Fed. Cir. 2003) (citing *Teleflex*, 299 F.3d at 1325–26). In other words, an inventor may consistently and clearly use a term in a manner either more or less expansive than its general usage in the relevant community, and thus expand or limit the scope of the term in the context of the patent claims. *See Ballard Med. Prods. v. Allegiance Healthcare Corp.*, 268 F.3d 1352, 1361 (Fed. Cir. 2001) (noting that an applicant may disclaim claim scope during prosecution); *Cordis Corp. v. Medtronic Ave, Inc.*, 511 F.3d 1157, 1177 (Fed. Cir. 2008) ("In order to constitute binding surrenders of claim scope, the statements in question must be such that a competitor would reasonably believe that the applicant had surrendered the relevant subject matter." (quotation omitted)).

3. Analysis

This phrase is used in the '104 and '198 Patents as follows:

1. A method of transmitting a message from a sender to a recipient and providing an indication that the message was opened by the recipient, comprising:

. . .

adding a link to the message by the server, the link configured to execute when the message is opened at the recipient to provide *an indication that the message has been opened by the recipient*,

executing the link when the message is opened at the recipient to control the server to provide *an indication that the message has been opened at the recipient*,

providing an authenticatible information related to the message, including the *indication of the opening of the message at the recipient*, at the server,

transmitting the *indication of the opening of the message at the recipient*, and the authenticatible information from the server to the sender,

'104 Patent col. 27 ll. 63–col. 28 ll. 16 (emphasis added).

1. A method of transmitting a message from a sender to a recipient and providing an indication that the message was opened by the recipient, comprising:

. . .

associating a link to the message by the server, the link configured to execute when the message is opened at the recipient to provide *an indication that the message has been opened by the recipient*,

executing the link when the message is activated at the recipient to control the server to provide *an indication that the message has been delivered to the recipient*,

providing an authenticatible information related to the message, including *the indication of the delivery of the message at the recipient*, at the server,

transmitting *the indication of the delivery of the message at the recipient*, and the authenticatible information form the server to the sender,

'198 Patent col. 28 ll. 6–25 (emphasis added). The term "indication" is similarly used in independent Claims 18 and 32 and dependent Claim 6 of the '198 Patent. *See* '198 Patent col. 28 ll. 39–41, col. 29 ll. 11–28, col. 30 ll. 7–25.

The parties dispute the interpretation of three terms: "indication," "opened," and "message." The Court will analyze each in turn.

- 39 -

a. "indication"

GoDaddy maintains that to differentiate the invention from prior art, "indication" must be construed as "confirmation" because the specification states that the invention provides "proof" of the delivery and content of the message. (Doc. 117 at 10). According to GoDaddy, "RPost cites no authority for its bare proposition that the patentee 'chose to claim the invention' as covering something more than 'proof' of a message's delivery and content." (*Id.*) GoDaddy collaterally asserts that RPost's construction of "indication" defines the term by the term itself, thereby making the construction "circular" and altogether unhelpful to the jury. (*Id.*)[7]

Contrary to GoDaddy's argument, RPost cites the most significant authority of all: the claim language. The "appropriate starting point" for "proper claim construction" is "always the language of the asserted claim itself." *Comark Commc'ns*, 156 F.3d at 1186 (citations omitted). In the asserted claims here, the patentee claimed the invention to provide an "indication" not a "confirmation"—undisputedly a term with a narrower scope. Generally, an "indication" is a generic piece of information that tends to show (i.e., indicates) something else. *See* Random House Webster's College Dictionary 669 (1999) (defining "indication" as "something serving to indicate; sign; token" and "indicate" as "to be a sign of; betoken"). On the other hand, "confirmation" is verifying or establishing the "truth, accuracy, validity, or genuineness of" something. *See id.* 279 (defining "confirmation" as "the act of confirming" and "confirm" as "to establish the truth, accuracy, validity, or genuineness of; corroborate; verify"). The dispute here is whether the specification limits the claimed "indication" to the tapered boundaries of "confirmation."

---

[7] GoDaddy proposed similar "circular" constructions for "server" (Term No. 2) and "authenticator" (agreed upon Term No. 2, Feldbau Patent). *See* (Doc. 191-1 at 1, 14 (construing "server" as "the outgoing server . . ." and "authenticator" as "a sub-system that operates to authenticate a dispatch")).

1   To resolve this dispute, understanding the Tomkow Patents' two-step

2   "verification" or "proof" process is essential. As an example, the '104 Patent claims a

3   system and method for verifying, i.e., proving, the opening of a message and the

4   message's content. The first step commences when the sender originates the message and

5   transmits it to the recipient. Before the message reaches the recipient, however, it cyphers

6   through an RPost server whereupon certain information is recorded, such as a hashed

7   version of its contents. *See* '104 Patent col. 28 ll. 25–29. The RPost server also adds a

8   "link" to the message that executes when the message is opened by the recipient, *id.* col.

9   28 ll. 1–4, and creates and stores "authenticatible information" about the message, which

10 essentially identifies a particular message as unique, *id.* col. 28 ll. 10–12, col. 31 ll. 33–

11 34. The RPost server then forwards the message to the recipient. *See id.* col. 28 ll. 5–6.

12 When the recipient opens the message, the link executes and provides an "indication that

13 the message has been opened by the recipient." *See id.* col. 28 ll. 7–9. To conclude the

14 first step, the RPost server sends a receipt to the sender which includes the "indication"

15 that the message was opened and other "authenticatible information." *See id.* col. 28 ll.

16 13–15.

17   The second step involves the actual verification of the opening of the message and

18 its contents. This step is disclosed in the specification as follows:

19   Verification

20   In the event that the originator of a message requires evidence at a
        later date that an e-mail was sent, delivered, and/or read, the originator
21   presents the receipt(s) for the message to the operators of the system.

22   For example, in order to prove that a particular message was sent
        from sender **10** to recipient **18**, sender **10** sends to RPost a copy of receipt
23   **20** with a request to verify the information contained within the receipt.
        This could be done by sending the receipt to a predefined mailbox at RPost,
24   e.g., verify@RPost.com. RPost then determines whether or not the receipt
        is a valid receipt. A receipt is a valid receipt if the digital signature matches
25   the reminder of the receipt, and the message digests match the
26   corresponding respective portions of the original message. Specifically,
        RPost performs the hash function on the various portions of the message
27   including the message body, the attachments, and the overall message
28

- 41 -

including the SMTP dialog and DSN reports, to produce one or more message digest corresponding to the purposed message copy. RPost compares the message digests in the purported copy, including the overall message digest, with the message digests which RPost has computed from the purported message copy. The overall message digest can be compared by either decrypting the overall message digest received as the digital signature in the purported receipt, or by encrypting the overall message digest which was calculated from the purported message copy. If the message digests including the digital signature match, then the receipt is an authentic RPost-generated receipt. Assuming that a good hash function was used and that the keys used in the cryptographic hash function and the digital signature encryption algorithm have not been divulged to others, it is virtually impossible that the receipt has been 'forged' by the person presenting the receipt. That is, the receipt must have been a receipt that was generated by RPost, and therefore the message contained in the receipt, the to/from information, the date and time of delivery, the fact of successful delivery, the route by which the message traveled, and any DSN information contained within the receipt, must be a true copy of that information and is accurate. RPost can then provide authentication, verification, and confirmation of the information contained within the receipt. This confirmation can take the form of an e-mail confirmation, affidavit testimony from RPost employees familiar with the methods used by RPost, live sworn testimony in depositions and in court, and other forms of testimony. . . .

In sum, the system provides reliable evidence based on the testimony of a disinterested third party that a particular message having a particular content was sent, when it was sent, who sent it, who received it, when it was opened for reading, and when it was deleted. . . .

'104 Patent col. 16 ll. 63–col. 17 ll. 55.

As readily seen, the invention "verifies" the opening of a message and its contents during the second step of the process—not the first step. The first step merely provides an "indication" to the sender that the message was opened by the recipient. This two-step process was claimed by the inventor and explained through the specification. Because the intrinsic record is clear that the invention "confirms" nothing during the first step, GoDaddy's proposed construction of "confirmation" is internally inconsistent.

Furthermore, GoDaddy's adoption of Figure 8's terminology is misplaced. Figure 8 is merely "another embodiment of the invention." '104 Patent col. 25 ll. 14–15.

- 42 -

1   If the Court were to adopt GoDaddy's proposal, it would be reading a limitation from the

2   specification into the claim—a "cardinal sin" according to the Federal Circuit. *Teleflex*,

3   299 F.3d at 1326 (citing *Comark Commc'ns*, 156 F.3d at 1186); *see Tex. Instruments, Inc.*

4   *v. United States Int'l Trade Comm'n*, 805 F.2d 1558, 1563 (Fed. Cir. 1986) ("This court

5   has cautioned against limiting the claimed invention to preferred embodiments or specific

6   examples in the specification."). "To avoid importing limitations from the specification

7   into the claims, it is important to keep in mind that the purposes of the specification are to

8   teach and enable those of skill in the art to make and use the invention and to provide a

9   best mode for doing so." *Phillips*, 415 F.3d at 1323.

10   One of the best ways to teach a person of ordinary skill in the art how to
         make and use the invention is to provide an example of how to practice the
11   invention in a particular case. Much of the time, upon reading the
         specification in that context, it will become clear whether the patentee is
12   setting out specific examples of the invention to accomplish those goals, or
13   whether the patentee instead intends for the claims and the embodiments in
         the specification to be strictly coextensive. The manner in which the
14   patentee uses a term within the specification and claims usually will make
15   the distinction apparent.

16   *Id.* (internal citations omitted). Although "there is sometimes a fine line between reading

17   a claim in light of the specification, and reading a limitation into the claim from the

18   specification," *Comark Commc'ns*, 156 F.3d at 1187, the Court believes that GoDaddy is

19   pursuing the latter rather than the former. Figure 8 does not establish the patentee's "clear

20   disavowal" of "indication" to the narrower meaning of "confirmation." *See Thorner*, 669

21   F.3d at 1365 (quoting *Teleflex*, 299 F.3d at 1325).

22   In short, notwithstanding the internal flaws within GoDaddy's proposal, the Court

23   finds that if it were to construe "indication" as "confirmation," a limitation from the

24   specification would be read into the claim. By focusing solely on the specification,

25   GoDaddy improperly seeks to construe the claims as limited to a single embodiment,

26   which goes against bedrock claim construction principles. *See Comark Commc'ns*, 156

27   F.3d at 1187.

28

1   Nonetheless, the patentee did not merely claim "indication" as a nebulous

2   indication without concern of later verification. The intrinsic record conveys that the

3   primary purpose of the invention is to provide information regarding the delivery,

4   opening, and content of an electronic message that *can be* "verified." For example, Claim

5   1 of the '104 Patent states that the "indication of the opening of the message at the

6   recipient" is "includ[ed]" in the "authenticatible information" which is sent to the sender.

7   '104 Patent col. 28 ll. 10–13; *see also* '198 Patent col. 28 ll. 20–22 ("providing an

8   authenticatible information related to the message, including the indication of the

9   delivery of the message at the recipient, at the server . . . ."). As construed below,

10   "authenticatible information" is certain information that "can be verified." Accordingly,

11   because the "indication of the opening of the message" is an element of "authenticatible

12   information," the indication *itself* must be verifiable.

13   For these reasons, the Court construes "indication" as "verifiable information that

14   indicates."

15   **b.   "opened"**

16   The parties also dispute the meaning of the term "opened" as used by the asserted

17   claims. RPost argues that "opened" does not need to be construed because the words

18   "opened," "viewed," and "read" all embody different meanings and the inventor claimed

19   "opened." (Doc. 119 at 6). In response, GoDaddy defines "opened" as "viewed" because,

20   according to the specification, "the message is opened for reading," and it would be

21   impossible to read a message without at some point viewing it. (Doc. 117 at 10).

22   The Court finds that "opened" does not require further construction. In construing

23   claim terms, the Court need not clarify a term if it has a plain meaning that requires no

24   clarification. *See U.S. Surgical*, 103 F.3d at 1568. Here, "opened" is a generic term that is

25   readily understood within the context of the claims to connote that a message was

26   "opened" by the recipient. A jury will have no trouble understanding this concept and

27   GoDaddy has not raised an actual dispute as to the scope of the term. It would be illogical

28   for the Court to force the jury to consider convoluted semantics of whether the message

was "opened," "viewed," or "read" when the patentee already claimed the generic term "opened." Thus, this portion of GoDaddy's proposal is rejected.

c. "message"

The parties' final dispute is whether "message" should be interpreted as "message" or "message content." GoDaddy proposes "message content" but does not explain why such a construction is necessary. *See* (Doc. 117 at 9–10). In the absence of compelling evidence to the contrary, the Court elects not to construe this portion of the phrase. "Message" is a readily understandable term and GoDaddy has not brought to the Court's attention a valid dispute concerning the term's scope. Moreover, because the Court declined to define "opened" as "viewed," construing this phrase as "opened the message content" makes little sense. The Court therefore rejects this portion of GoDaddy's proposal.

4. Conclusion

For these reasons, the Court construes "an indication that the message has been opened by (delivered to) a recipient" as "verifiable information that indicates that the message has been opened by (opened at; delivered to) the recipient."[8]

E. "an indication of receipt of the message by the recipient (recipient processor)" (Term No. 5)

1. The Parties' Positions

As with Term No. 4, the parties' dispute centers on the term "indication." RPost proposes a construction of "information that indicates that the message has been received by the recipient (recipient processor)." (Doc. 191-1 at 1–2). GoDaddy responds by proposing: "confirmation that the message content was received by the recipient." (*Id.*)

2. Analysis

This phrase is used in the asserted claims of the '389 Patent as follows:

---

[8] The Court includes "opened at" in its construction because Claim 18 of the '198 Patent claims "opened at the recipient." *See* '198 Patent col. 29 ll. 23.

1   **1**. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:

. . .

receiving at the server from the recipient *an indication of the receipt of the message by the recipient*;

forming at the server a first information from the at least a portion of the mail transport protocol dialog and *the indication of the receipt of the message by the recipient . . . .*

'389 Patent col. 27 ll. 58–col 28 ll. 3 (emphasis added).

        7. A system for transmitting a message through an electronic mail system from an originating processor to a recipient processor and providing proof of receipt of the message by the recipient process, comprising:

a server displaced from the originating processor, the server capable of being configured by software commands to:

. . .

receive *an indication of receipt of the message from the recipient processor* and a mail transport protocol dialog generated by the electronic mail system during transmission of the message from the server to the recipient processor;

generate a first information including *the indication of receipt of the message from the recipient processor* and at least a portion of the mail transport protocol dialog generated by the electronic mail system during transmission of the message from the server to the recipient processor.

Id. col. 28 ll. 33–52 (emphasis added).

        14. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:

. . .

receiving at the server from the recipient a first information including *an indication of the receipt of the message by the recipient* and at least a portion of a mail transport protocol dialog generated during transmission of the first information from the server to the recipient . . . .

Id. col. 29 ll. 17–col. 30 ll. 5.

- 46 -

The Court adopts its analysis for the terms "indication" and "message" as set forth for Term No. 4 and therefore construes this phrase as "verifiable information that indicates that the message was received by the recipient (recipient processor)."

F. "an indication of the failure to deliver the message to the recipient" (Term No. 6)

1. The Parties' Positions

RPost proposes a construction of "information that indicates that the message has failed to be delivered to the recipient." (Doc. 191-1 at 2). GoDaddy responds that the phrase should be defined as "confirmation that the message content was not received by the recipient." (*Id.*)

2. Analysis

This phrase is found in the asserted claims of the '199 Patent as follows:

> **1**. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:
>
> . . .
>
> receiving at the server from the recipient *an indication of the failure to deliver the message to the recipient*;
>
> forming at the server a first information from the at least a portion of the data transport protocol dialog and *the indication of the failure to deliver the message by the recipient* . . . .

'199 Patent col. 27 ll. 58–65 (emphasis added).

The parties again dispute the claim terms "indication" and "message." The Court adopts its analysis as set forth in Term No. 4 and construes "indication" as "verifiable information that indicates" and does not construe "message."

The parties also proffer different constructions for the balance of the phrase. GoDaddy suggests a construction that interprets "failure to deliver" as "not receiv[ing]" the message. (Doc. 191-1 at 2). However, the '199 Patent does not speak in terms of "receipt" of the message but claims whether the message failed to be "delivered." The

- 47 -

1   Court finds that this portion of the claim uses plain language the jury will readily be able

2   to understand without further construction.

3   The Court therefore construes Term No. 6 as "verifiable information that indicates

4   the failure to deliver the message to the recipient."

5   **G.   "executing the link when the message is opened at the recipient to control the server to provide an indication that the message has been opened at the recipient" (Term No. 7)**

6

7   **1.   The Parties' Positions**

8   RPost proposes a construction that closely tracks the claim language: "executing

9   the link when the message is opened at the recipient to cause the server to provide an

10   indication that the message has been opened at the recipient." (Doc. 191-1 at 2).

11   GoDaddy responds by construing the phrase as: "action by the recipient when the

12   message is opened at the recipient to control the server to provide proof that the message

13   has been opened at the recipient, the proof providing a legal or other evidentiary status on

14   par with, if not superior to, that of registered United States mail." (*Id.*) GoDaddy argues

15   that the "structure" of the asserted claims "makes clear that—once the message is opened

16   at the recipient—it is the recipient (including the link at the recipient) that controls the

17   server to provide the attendant proof that the message has been opened at the recipient."

18   (Doc. 117 at 11). GoDaddy also maintains that the "core purpose of the claimed

19   inventions is to provide not merely an 'indication,' but 'proof regarding the delivery and

20   contents of an e-mail message.'" (*Id.* at 11–12). GoDaddy finally argues that RPost's

21   proposed change from "control" to "cause" is flawed because the two words are not

22   synonymous. (*Id.* at 12).

23   RPost criticizes GoDaddy's construction for three reasons. First, RPost argues that

24   GoDaddy's proposal improperly limits the claim to actions performed by the recipient.

25   (Doc. 114 at 10). RPost explains that the link is executed "at the recipient," not "by the

26   recipient" as GoDaddy contends. (Doc. 119 at 6). Second, RPost asserts that GoDaddy's

27   construction impermissibly narrows the claim's plain meaning by construing "indication"

28

as "proof." (Doc. 114 at 10). Third, RPost insists that GoDaddy's proposed limitation regarding "legal or other evidentiary status" is not supported by the claim language and violates the intrinsic record. (*Id.* at 10–11).

2. Analysis

This phrase is used in Claim 1 of the '104 Patent as follows:

> **1**. A method of transmitting a message from a sender to a recipient and providing an indication that the message was opened by the recipient, comprising:
>
> adding a link to the message by the server, the link configured to execute when the message is opened at the recipient to provide an indication that the message has been opened by the recipient,
>
> . . .
>
> *executing the link when the message is opened at the recipient to control the server to provide an indication that the message has been opened at the recipient . . . .*

'104 Patent col. 27 ll. 63–col. 28 ll. 9 (emphasis added). The Court will analyze the parties' proposals in turn.

a. "control"

The Court first reviews RPost's suggestion that "control" should be interpreted as "cause." GoDaddy complains that such a construction is improper because the two words have different meanings. (Doc. 117 at 12). To support its argument, GoDaddy cites to the American Heritage Dictionary which defines "control" as "[t]o exercise authoritative or dominating influence over; direct" and "cause" as "**1a**. The producer of an effect, result, or consequence. **b**. The one, such as a person, event, or condition, that is responsible for an action or result." (*Id.*)

It is apparent from the dictionary definitions that the two terms have entirely different meanings. While "cause" simply refers to one that is responsible for an action or result, "control" requires that one exercise some sort of dominion or authority over another. In other words, "cause" is broader than "control." This distinction is exemplified by the '198 Patent's usage of the two words in an unrelated claim. *See* '198 Patent col. 29

1 ll. 1–4 ("**16**. The method of claim **15**, wherein activating the link also *causes* information

2 to be displayed to the recipient and to *control* the server to make a record of the

3 information displayed." (emphasis added)). RPost does not point to evidence within the

4 intrinsic record to show that the inventor intended to claim "control" with a broader

5 meaning. Accordingly, this portion of RPost's proposed construction is rejected.

6 **b.   "executing the link"**

7 The Court next reviews GoDaddy's proposal that "executing the link" should be

8 construed as "action by the recipient." GoDaddy explains that the "structure" of the

9 asserted claims "makes clear that—once the message is opened at the recipient—it is the

10 recipient (including the link at the recipient) that controls the server to provide the

11 attendant proof that the message has been opened at the recipient." (Doc. 117 at 11).

12 GoDaddy further notes that "it is . . . the recipient (i.e., the link in the message) that

13 performs the claimed function." (*Id.*) RPost replies that even though the recipient

14 performs the opening of the message, that fact is irrelevant because "the disputed claim

15 function is executing, which the link does on its own." (Doc. 119 at 6).

16 The Court finds that "executing the link" does not require the recipient to

17 affirmatively act beyond opening the message. Rather, the function of the claim,

18 "executing," occurs by the link itself "when the message is opened." Furthermore,

19 GoDaddy's likening of the "recipient" to the "link" itself is baseless, as the two terms are

20 clearly distinct. Consequently, this portion of GoDaddy's proposal is rejected.

21 The Court adopts a slightly amended version of this portion of RPost's proposal:

22 "the link executing on its own when the message is opened at the recipient." This

23 construction clarifies for the jury that the link executes on its own when the message is

24 opened.

25 **c.   "an indication"**

26 Finally, the Court examines GoDaddy's argument that "an indication" should be

27 interpreted as "proof that the message has been opened at the recipient, the proof

28 providing a legal or other evidentiary status on par with, if not superior to, that of

1   registered United States mail." (Doc. 191-1 at 2).[9] While it is undisputed that the claim

2   language does not include this purported "evidentiary" limitation, GoDaddy argues that

3   the limitation emerges from the specification and is essential to differentiate the Tomkow

4   Patents from prior art. *See* (Doc. 117 at 11–12).

5   The portion of the shared specification from which GoDaddy plucks this limitation

6   is found in the Summary of the Present Invention which reads as follows:

7   A general object of the present invention is to provide a system and
method for reliably verifying via secure and tamper-proof documentation

8   the content and delivery of an electronic message such as an e-mail. Ideally,

9   the invention will give e-mail and other electronic messages a legal status
on par with, if not superior to, that of registered United States mail.

10   However, it is not necessary to the invention that any particular legal status
is accorded to messages sent according to the methods taught herein, as the

11   invention provides useful information and verification regardless.

12   '199 Patent col. 3 ll. 8–17; '389 Patent col. 3 ll. 6–15 (same); '104 Patent col. 3 ll. 6–15

13   (same); '198 Patent col. 3 ll. 9–18 (same); '913 Patent col. 3 ll. 8–17 (same). Based on

14   this language and references to prior art in the specification, GoDaddy maintains that the

15   "indication" provided by the invention must have some level of evidentiary status—legal

16   or otherwise—that is equal or superior to registered United States mail. (Doc. 117 at 11).

17   To begin, as the Court has already recounted, construing this term must be done in

18   light of the Federal Circuit's frequent admonition against reading limitations from the

19   specification into the claim. *See Comark Commc'ns*, 156 F.3d at 1187. In ascertaining

20   whether the patentee disavowed the full scope of a claim, the Court must refrain from

21   committing the "cardinal sin" of reading limitations from the specification into the

22   claims. *Teleflex*, 299 F.3d at 1326 (citing *Comark Commc'ns*, 156 F.3d at 1186). The

23   only way a specification may narrow the scope of a disputed claim term is if the patentee

24   "demonstrate[d] intent to deviate from the ordinary and accustomed meaning of a claim

25

26

27   [9] GoDaddy proposes this or a similar limitation for a dozen disputed claim terms
in the Tomkow Patents. *See* (Docs. 117, 191-1 (proposing this limitation for Term Nos. 7,

28   8, 9, 10, 11, 13, 14, 15, 16, 17, 23, and 24).

1 term by including in the specification expressions of manifest exclusion or restriction,

2 representing a clear disavowal of claim scope." *Thorner*, 669 F.3d at 1365 (quoting

3 *Teleflex*, 299 F.3d at 1325). Here, because the proposed evidentiary limitation

4 purportedly springs from the specification, GoDaddy must show that the inventor clearly

5 disavowed the claim scope.

6 In this regard, the Court is not persuaded that GoDaddy's proposed evidentiary

7 limitation exists. The specification flatly expresses that "it is not necessary to the

8 invention that any particular legal status is accorded to messages sent according to the

9 methods taught herein, as the invention provides useful information and verification

10 regardless." GoDaddy nonetheless attempts to circumvent this language by arguing that

11 its proposal affords two methods of attaining the evidentiary status of registered United

12 States mail: (1) "legal" or (2) "other evidentiary status." As the inventor clearly disclosed

13 that no "legal" status was required for the invention, the question becomes whether an

14 "indication" must have an "evidentiary status on par with, if not superior to, that of

15 registered United States mail."

16 In response to this question, the Court finds that GoDaddy's proposal misses the

17 mark. As discussed at length for Term No. 4, the "indication" provided by the invention

18 is not the "proof" that is discussed in the specification. The second step of the process—

19 the "verification" of a message—is when the invention arguably provides "proof" of

20 certain aspects of the message. Consequently, even if the Court were to sidestep the

21 "cardinal sin" of reading limitations from the specification into a claim and disregard the

22 invention's express disclaimer that no legal status is vital to the invention, the Court

23 would still reject this portion of GoDaddy's argument because the purported evidentiary

24 limitation does not even concern the invention's initial step of providing an "indication."

25 Accordingly, the Court adopts its construction of "indication" as explained in

26 Term No. 4.

27

28

3. **Conclusion**

For these reasons, the Court construes this phrase as: "the link executing on its own when the message is opened at the recipient to control the server to provide verifiable information that indicates that the message has been opened at the recipient."

H. **"the link being configured to execute automatically when the message is opened at the recipient processor to control the server to provide an indication at the server that the message has been opened at the recipient processor" (Term No. 8)**

1. **The Parties' Positions**

Similar to its proposed construction for Term No. 7, RPost advances the following construction of Term No. 8: "the link programmed to execute automatically when the message is opened at the recipient to cause the server to provide an indication at the server that the message has been opened at the recipient." (Doc. 191-1 at 2). As seen, RPost modifies the claim language in two ways: (1) defining "control" as "cause" and (2) construing "configured" as "programmed." RPost asserts that the minor linguistic change from "configured" to "programmed" clarifies for the jury that the term is "used in a computer programming sense." (Doc. 119 at 10).

In response, GoDaddy proposes a construction of: "[link configured to execute through] action by the recipient when the message is opened at the recipient to control the server to provide proof that the message has been opened at the recipient, the proof providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail." (Doc. 191-1 at 2).

2. **Analysis**

This phrase is used in Claim 27 of the '104 Patent as follows:

27. A system for transmitting a message from an originating processor to a recipient processor in an electronic mail system and providing an indication that the message was opened by the recipient processor, comprising:

a server in electronic communication in the electronic mail system, the server receiving the message from the originating processor and adding a link to the message before transmitting the message and link to the

1
2
3

recipient processor, *the link being configured to execute automatically when the message is opened at the recipient processor to control the server to provide an indication at the server that the message has been opened at the recipient processor . . . .*

4 '104 Patent col. 31 ll. 20–32 (emphasis added).

5 For the reasons set forth in Term No. 7, the Court rejects GoDaddy's evidentiary

6 proposal and its suggestion that the claim requires "action by the recipient." Likewise, the

7 Court also rejects the portion of RPost's proposal that construes "control" as "cause."

8 As to RPost's argument that "configured" should be defined as "programmed," the

9 Court finds that such a construction is unwarranted. The term "configured" has a plain

10 and ordinary meaning that the jury will be able to understand within the context of this

11 electronic messaging dispute. *See U.S. Surgical*, 103 F.3d at 1568. RPost has not shown

12 that the term is used in a manner that diverges from its plain meaning, and therefore the

13 Court rejects this portion of RPost's proposal.

14 For these reasons, the Court construes this phrase as: "the link being configured to

15 execute automatically when the message is opened at the recipient to control the server to

16 provide verifiable information that indicates at the server that the message has been

17 opened at the recipient processor."

18
19

I.   **"the link configured to execute when the link is activated at the recipient to provide an indication that the message has been opened by (delivered to) a recipient" (Term No. 9)**

20   **1.**   **The Parties' Positions**

21 Similar to its proposals for Term Nos. 7 and 8, RPost suggests that this phrase

22 should be interpreted as "the link programmed to execute when the link is activated at the

23 recipient to provide an indication that the message has been opened by (delivered to) a

24 recipient." (Doc. 191-1 at 3).

25 In response, GoDaddy argues that the claim should be construed as "[link

26 configured to execute through] action by the recipient when the message is opened at the

27 recipient to control the server to provide proof that the message has been opened at the

28

- 54 -

1   recipient, the proof providing a legal or other evidentiary status on par with, if not

2   superior to, that of registered United States mail." (*Id.*)

3   **2.   Analysis**

4   This phrase is found in Claims 1, 18, and 32 of the '198 Patent as follows:

5   **1**. A method of transmitting a message from a sender to a recipient
     and providing an indication that the message was opened by the recipient,
6   comprising:

7   associating a link with the message by the server*, the link configured
     to execute when the link is activated at the recipient to provide an*
8   *indication that the message has been opened by a recipient . . . .*

9   '198 Patent col. 28 ll. 6–14 (emphasis added).

10   **18**. A system transmitting a message from a sender to a recipient and
11   providing an indication that the message was opened by the recipient,
     comprising:
12
             a server in electronic communication with the sender and the
13   receiver, the server programmed to receive a message from the sender, to
     associate a link with the message, *the link configured to execute when the*
14   *link is activated at the recipient to provide an indication that the message*
15   *has been opened by a recipient*, to transmit the message and the link from
     the server to the recipient . . . .
16

17   *Id.* col. 29 ll. 11–20 (emphasis added); *see id.* col. 30 ll. 7–16 (same).

18   For the reasons set forth in Term No. 7, the Court rejects GoDaddy's evidentiary

19   proposal and its suggestion that the claim requires "action by the recipient." For the

20   reasons expressed in Term No. 8, the Court also rejects the portion of RPost's proposal

21   that construes "configured" as "programmed."

22   The remaining dispute is whether "activated" should be construed as "opened at

23   the recipient to control the server." The use of the term "activated" in the '198 Patent is

24   different than the prior two disputed terms from the '104 Patent which claim "opened at

25   the recipient." "Activated" is a readily-understandable term, and there is no evidence

26   before the Court showing that the inventor of the '198 Patent intended the link to be

27   activated only when the message is opened. While it could be argued that because the

28   activation of the link causes an indication of the opening of the message to be sent to the

1   recipient it is the opening of the message that activates the link, this is not necessarily

2   true. In fact, the dependent claims of Claim 1 suggest other ways of activating the link.

3   *See* '198 Patent col. 28 ll. 26–27. Thus, the Court rejects GoDaddy's proposal and does

4   not construe the generic term "activated."

5   For these reasons, the Court defines Term No. 9 as "the link configured to execute

6   when the link is activated at the recipient to provide verifiable information that indicates

7   that the message has been opened by (delivered to) the recipient."

8   **J.   "executing the link when the link is activated at the recipient to control
         the server to provide an indication that the message has been delivered
9   to the recipient" (Term No. 10)**

10   **1.   The Parties' Positions**

11   For Term No. 10, RPost asks the Court to adopt the following construction:

12   "executing the link when the link is called at the recipient to cause the server to provide

13   an indication that the message has been delivered to the recipient." (Doc. 191-1 at 3–4).

14   In response, GoDaddy proposes a construction of "[executing the link through]

15   action by the recipient when the message is opened at the recipient to control the server to

16   provide proof that the message has been opened at the recipient, the proof providing a

17   legal or other evidentiary status on par with, if not superior to, that of registered United

18   States mail." (*Id.*)

19   **2.   Analysis**

20   This phrase is used in Claim 1 of the '198 Patent as follows:

21   **1**. A method of transmitting a message from a sender to a recipient
         and providing an indication that the message was opened by the recipient,
22   comprising:

23   . . .

24   *executing the link when the message is activated at the recipient to*
         control the server to provide an indication that the message has been
25   *delivered to the recipient . . . .*

26   '198 Patent col. 28 ll. 6–19 (emphasis added).

27

28

1   Several of the modifications proposed by the parties have already been resolved in

2   prior terms. As to GoDaddy's "evidentiary" and "action by the recipient" proposals, the

3   Court adopts its reasoning for Term No. 7. Regarding GoDaddy's construction of the

4   claim term "activated," the Court adopts its analysis as set forth for Term No. 9. Finally,

5   the Court adopts its reasoning and rejection of RPost's construction of "control" as

6   explained in Term No. 7.

7   RPost additionally proposes that the term "activated" should be interpreted as

8   "called." RPost does not explain this construction in its briefing, and the Court is not

9   persuaded that construction of this term is necessary for the reasons set forth in Term

10   No. 9. Thus, the Court rejects this portion of RPost's proposal.

11   For these reasons, the Court construes Term No. 10 as "the link executing on its

12   own when the link is activated at the recipient to control the server to provide verifiable

13   information that indicates that the message has been delivered to the recipient."

14   **K.   "wherein the link is executed when the link is activated at the recipient
        to control the server to provide an indication that the message has been**
15   **opened at (delivered to) the recipient" (Term No. 11)**

16   **1.   The Parties' Positions**

17   RPost argues that Term No. 11 should be construed as "wherein the link executed

18   when the link is called at the recipient to cause the server to provide an indication that the

19   message has been opened at (delivered to) to the recipient." (Doc. 191-1 at 4).

20   In response, GoDaddy proposes a construction of "[executing the link through]

21   action by the recipient when the message is opened at the recipient to control the server to

22   provide proof that the message has been opened at the recipient, the proof providing a

23   legal or other evidentiary status on par with, if not superior to, that of registered United

24   States mail." (*Id.*)

25   **2.   Analysis**

26   This phrase is found in the '198 Patent as follows:

27

28

18. A system transmitting a message from a sender to a recipient and providing an indication that the message was opened by the recipient, comprising:

a server in electronic communication with the sender and the receiver, the sever programmed to receive a message from the sender, to associate a link with the message, the link configured to execute when the link is activated at the recipient to provide an indication that the message has been opened by a recipient, to transmit the message and the link from the server to the recipient, *wherein*

the link is executed when the link is activated at the recipient to control the server to provide an indication that the message has been opened at the recipient . . . .

'198 Patent col. 29 ll. 11–24 (emphasis added). Asserted Claim 32 incorporates the same language as Claim 18, but replaces "delivered to" with "opened at." *Id.* col. 30 ll. 7–20.

The Court has already settled all of the parties' disputes for prior terms and incorporates those analyses and constructions here. The Court therefore defines this phrase as "wherein the link is executed when the link is activated at the recipient to control the server to provide verifiable information that indicates that the message has been opened at (delivered to) the recipient."

L.   "authenticatible information" (Term No. 12)

1.   The Parties' Positions

RPost proposes that "authenticatible information" should be broadly construed as "information regarding the content or delivery of a message that can be verified." (Doc. 191-1 at 4–5). RPost argues this construction is "consistent with the intrinsic record, which repeatedly refers to authentication in the context of verifying the content and delivery of an electronic message." (Doc. 114 at 11).

GoDaddy, on the other hand, proposes the following itemized construction: "information unique to the message, the digital signature of the message, and the portion of the mail transport dialog generated during transmission of the message." (Doc. 191-1 at 4–5). GoDaddy contends that its construction is grounded in the specification's disclosure of "digital signature." (Doc. 117 at 13). Specifically, GoDaddy explains that

1 "authenticatible information" must include the message's digital signature, which it

2 defines as a "digital code that uniquely identifies the message and/or its attachments."

3 (*Id.*)[10] GoDaddy did not clarify in its briefing or during the *Markman* Hearing why the

4 balance of its proposal, "the portion of the mail transport dialog generated during

5 transmission of the message," is necessary.

6 RPost replies that GoDaddy's proposal is problematic because GoDaddy did not

7 cite any portion of the intrinsic record showing that the inventor intended to limit

8 "authenticatible information" to three enumerated elements. (Doc. 119 at 7). RPost also

9 points out that the term "digital signature" is not claimed in either the '104 or '198

10 Patents where "authenticatible information" is claimed. (*Id.*) RPost thus contends that

11 GoDaddy is attempting to limit "authenticatible information" by terms from the

12 specification. (Doc. 114 at 11).

13 ### 2. Analysis

14 The term "authenticatible information" is used by the '104 and '198 Patents. The

15 '104 Patent claims as follows:

16 **1**. A method of transmitting a message from a sender to a recipient

17 and providing an indication that the message was opened by the recipient,
comprising:

18 . . .

19 providing an *authenticatible information* related to the message,

20 including the indication of the opening of the message at the recipient, at
the server, and

21 transmitting the indication of the opening of the message at the

22 recipient, and the *authenticatible information* from the server to the sender.

23 '104 Patent col. 27 ll. 63–col. 28 ll. 16 (emphasis added). The term is also claimed by the

24 '198 Patent as follows:

25 _____

26 [10] As GoDaddy notes, RMail defined "digital signature" in this manner before

27 Judge Gilstrap. *See RMail*, 2013 WL 968246, at *55. However, "digital signature" is not
claimed by either of the asserted claims here, nor does GoDaddy suggest that this

28 definition should be included in the construction.

1. A method of transmitting a message from a sender to a recipient and providing an indication that the message was opened by the recipient, comprising:

. . .

providing an *authenticatible information* related to the message, including the indication of the delivery of the message at the recipient, at the server, and

transmitting the indication of the delivery of the message at the recipient, and the *authenticatible information* from the server to the sender.

'198 Patent col. 28. ll. 6–25 (emphasis added).

18. A system transmitting a message from a sender to a recipient and providing an indication that the message was opened at the recipient, comprising:

. . .

wherein the server is programmed to form an authenticatible information related to the message, and to transmit the indication of the opening of the message at the recipient and the authenticatible information from the server to the sender.

Id. col. 29 ll. 11–28 (emphasis added); *see id.* col. 30 ll. 7–25 (same).

GoDaddy argues that "digital signature" should be included within the construction of "authenticatible information." The term "digital signature" is disclosed in the specification as follows:

The present invention includes an electronic message system that creates and records a *digital signature* of each electronic message sent through the system. An originator may send a copy of the electronic message to the system or generate the electronic message within the system itself. The system then forwards and delivers the electronic message to all recipients (or to the designated message handlers associated with the recipients), including "to" addressees and "cc" addressees. Thereafter, the system returns a receipt of delivery to the originator of the electronic message. The receipt includes, among other things: the original message, the *digital signature* of the message, and a handshaking and delivery history including times of delivery to the recipients. To later verify and authenticate information contained in the receipt, the originator or user sends a copy of the receipt to the system. The system then verifies that the *digital signature* matches the original message and the rest of the receipt. If

the two match, then the system sends a letter or provides other confirmation of authenticity verifying that the electronic message has not been altered.

Id. col. 3 ll. 19–38 (emphasis added).

At the outset, the Court agrees with GoDaddy's argument that the information comprising "authenticatible information" must be "unique" to a particular message. If the information was not unique to a message, verification of the message would be infeasible thereby making the claims limitless. GoDaddy's proposed construction, however, is superfluous. Specifically, GoDaddy defines "digital signature" as a "digital code that *uniquely identifies* the message and/or its contents." (Doc. 117 at 13 (emphasis added)). GoDaddy then offers a construction that includes both "information unique to the message" and "the digital signature of the message." There is no need to use both phrases in the construction when the phrases purportedly mean the same thing. On balance, the Court finds that "unique" would be more helpful to the jury than "digital signature"—a term that is not in the claim language and that would require a separate definition.

GoDaddy also contends that authenticatible information must include "the portion of the mail transport dialog generated during transmission of the message." (Doc. 191-1 at 4–5). GoDaddy does not explain why this limitation is necessary, and the Court does not find it to be supported by the intrinsic record. In fact, the '104 and '198 Patents do not even recite the term "mail transport dialog." Thus, if the Court were to adopt this portion of GoDaddy's construction, it would be importing concepts from other Tomkow Patents into the '104 and '198 Patents.

Finally, the Court agrees with RPost that "authenticatible information" is information regarding either the "content or delivery" of a message that "can be verified." The information must be able to be verified due to the two-step verification process as explained in Term No. 4.

For these reasons, the Court adopts the following amalgam of the parties' proffered constructions for "authenticatible information": "information unique to the content or delivery of a message that can be verified."

M. "mail transport protocol dialog" (Term No. 13)

1. The Parties' Positions

RPost contends that Term No. 13 should be interpreted as "mail transport data including a sequence of at least one command and at least one response." (Doc. 191-1 at 5). RPost posits that this construction is "virtually identical" to Judge Gilstrap's construction of the same term. (Doc. 114 at 12).

In response, GoDaddy proposes a narrower definition: "a list of commands and responses exchanged between servers during transmission of the message that is sufficient to prove delivery of the message to the recipient, providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail." (Doc. 191-1 at 5). GoDaddy explains that its proposal "make[s] clear that the commands and responses exchanged during transmission of the message must be sufficient to prove delivery of the message to the recipient." (Doc. 117 at 14). GoDaddy further argues that the inclusion of the phrase "or other evidentiary status" in its construction overcomes RPost's argument that the invention need not confer a legal status upon its messages. (*Id.*)

RPost complains that GoDaddy's proposal is "completely at odds with the intrinsic record, which expressly states that it is not necessary to the invention that messages be accorded legal status." (Doc. 114 at 12). RPost also contends that GoDaddy's proposal conflicts with Judge Gilstrap's definition of "dialog" and improperly imports limitations from the specification into the claim. (*Id.*; Doc. 119 at 7).

2. Analysis

The term "mail transport protocol dialog" is used in the '389 Patent as follows:

> **1**. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:
>
> . . .
>
> receiving at the server at least a portion of a *mail transport protocol dialog* generated during transmission of the message from the server to the recipient . . .

forming at the server a first information that the at least a portion of the *mail transport protocol dialog* and the indication of the receipt of the message by the recipient . . .

'389 Patent col. 27 ll. 58–col. 28 ll. 3 (emphasis added).

7. A system for transmitting a message through an electronic mail system from an originating processor to a recipient processor and providing proof of receipt of the message by the recipient process, comprising:

. . .

receive an indication of receipt of the message from the recipient processor and a *mail transport protocol dialog* generated by the electronic mail system during transmission of the message from the server to the recipient processor;

generate a first information including the indication of receipt of the message from the recipient processor and at least a portion of the *mail transport protocol dialog* generated by the electronic mail system during transmission of the message from the server to the recipient processor.

Id. col. 28 ll. 33–52 (emphasis added).

14. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:

receiving at the server from the recipient a first information including an indication of the receipt of the message by the recipient and at least a portion of a *mail transport protocol dialog* generated during transmission of the first information from the server to the recipient . . . .

Id. col. 29 ll. 16–col. 30 ll. 5 (emphasis added).

As used in the '372 and '557 Patents, Judge Gilstrap construed "mail transport protocol dialog" as: "data including a list of at least one command and at least one response exchanged between devices during the transmission of a message." *RMail*, 2013 WL 968246, at *55. In doing so, Judge Gilstrap relied upon the patents' specification and prosecution history. *Id.* Specifically, Judge Gilstrap considered the following excerpt from the '372 Patent's specification:

Whether the connection is SMTP or ESMTP, the RPost server will record the entire protocol dialogue between the two servers. Typically this dialogue will include protocol messages in which, among other things, the destination server identifies itself, grants permission to upload a message

1
2
3

> for a named recipient, and acknowledges that the message was received. RPost will save the record of this transaction in such way that it may be later retrieved and included in or attached to the RPost Delivery Receipt for this message.

4   *Id.* at *54. The '389 Patent shares this portion of the specification. *See* '389 Patent col. 12

5   ll. 65–col. 13 ll. 6.

6   Judge Gilstrap further explained that during prosecution of the patent, the inventor

7   disclaimed that "a dialog, as that term is understood by one skilled in the relevant art, is a

8   list of commands and responses exchanged between an outgoing server and a destination

9   address or server to transmit a message." *RMail*, 2013 WL 968246, at *54. Judge Gilstrap

10 concluded that this statement rose "to the level of a 'reasonably clear' lexicography

11 defining 'dialog' in the context of 'mail transport dialog' as being data that includes a list

12 of command and responses exchanged during transmission of a message." *Id.* (citations

13 omitted).

14   The '389 Patent describes two primary mail transport protocols: SMTP and

15 ESMTP. The '389 Patent describes an (E)SMTP "dialogue" between the sender's Mail

16 Transport Agent ("MTA") and the recipient's MTA during which the message is

17 delivered. *See, e.g.*, '389 Patent col. 11 ll. 50–56, col. 12 ll. 65–67. A person of ordinary

18 skill in the art would understand "at least a portion of a mail transport protocol dialogue"

19 to include information from the dialogue between the MTAs (e.g., an SMTP command or

20 an SMTP response), not merely information from the message itself. Moreover, the Court

21 agrees with Judge Gilstrap's analysis and finds that the construction of this term should at

22 least incorporate "data including a sequence of at least one mail transport protocol

23 command and at least one mail transport protocol response exchanged between devices

24 during transmission of the message."[11]

25

26

27
28

---

[11] RPost's "virtually identical" proposed construction did not include the phrase "exchanged between devices during transmission of a message" from Judge Gilstrap's construction. *See* (Doc. 191-1 at 5). During the *Markman* Hearing, however, RPost

- 64 -

1   As has been the case for several terms, GoDaddy raises an issue regarding the use

2   of the invention. Specifically, GoDaddy insists that the data must be "sufficient to prove

3   delivery of the message to the recipient, providing a legal or other evidentiary status on

4   par with, if not superior to, that of registered United States mail." (Doc. 117 at 14). As

5   discussed for the "indication" terms above, however, even disregarding the "cardinal sin"

6   of reading limitations from the specification into the claim, the Court finds no

7   requirement that the invention bestow upon its messages an evidentiary status on par with

8   or superior to registered United States mail.

9   For these reasons, the Court adopts RPost's proposed construction with minor

10   changes. Term No. 13 means "data including at least one mail transport protocol

11   command and at least one mail transport protocol response exchanged between devices

12   during transmission of a message."

13   **N.   "at least a portion of a mail transport protocol dialog (data transport**
         dialog) generated (by the electronic mail system) during transmission
14   **of the message from the server to the recipient (processor)" (Term**
15   **No. 14)**

16   **1.   The Parties' Positions**

17   RPost contends that this phrase does not require further construction beyond

18   construing "mail transport protocol dialog." (Doc. 191-1 at 5). GoDaddy appears to

19   advance the same construction as it did for Term No. 13. *See* (Doc. 117 at 13).

20   **2.   Analysis**

21   This phrase is claimed in the '389 Patent as quoted in Term No. 13 and also in

22   Claim 1 of the '199 Patent. The '199 Patent claims:

23

24

25   argued that this phrase should be included in the construction. The Court finds this phrase
     would help the jury understand the meaning of the disputed term.
26

27   Additionally, GoDaddy's proposal substitutes "servers" for "devices." The Court
     finds that the claims' plain language does not require transmissions between servers and
28   rejects this proposal.

1. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:

. . .

receiving at the server *at least a portion of a data transport protocol dialog generated during transmission of the message from the server to the recipient*; and

. . .

forming at the server a first information from the at least a portion of the data transport protocol dialog and the indication of the failure to deliver the message by the recipient . . . .

'199 Patent col. 27 ll. 58–col. 28 ll. 4 (emphasis added).

In 2014, Symantec Corporation filed a petition with the Patent Trial and Appeal Board ("Board") requesting *inter partes* review of several claims of the '372 Patent, of which the '389 and '199 Patents are continuations. *See Symantec Corp. v. RPost Commc'ns Ltd.*, 2014 WL 3542162, at *1 (Patent Tr. & App. Bd. July 15, 2014). RPost, as patent owner, filed a response. *Id.* One of the claims before the Board for construction was "at least a portion of a mail transport protocol dialog." *Id.* at *6–7. RPost proposed Judge Gilstrap's construction: "data including a list of at least one command and at least one response exchanged between devices during the transmission of a message." *Id.* at *7. The Board rejected the conjunctive nature of RPost's proposal and construed the phrase as "at least one mail transport protocol command *or* at least one mail transport protocol reply." *Id.* (emphasis added).

Because the claim recites "at least a portion," the Court rejects RPost's proposal that no construction is necessary because the jury could mistakenly conclude—as RPost did before the Board—that at least one command *and* one response is needed. Instead, the Court adopts the substance of the Board's construction and interprets this phrase to mean "data including at least one mail transport protocol command or at least one mail transport protocol response exchanged between devices during transmission of the message."

O. "SMTP and ESMTP protocol dialog" (Term No. 15)

1. The Parties' Positions

RPost advances a construction that closely mirrors its proposals for the preceding dialog terms. Specifically, RPost argues that "SMTP and ESMTP protocol dialog" should be construed as "SMTP or ESMTP data including a list of at least one command and at least one response generated by the electronic mail system during transmission of the message from the server to the recipient." (Doc. 191-1 at 5–6).

GoDaddy proposes the same construction as it did for Term Nos. 13 and 14: "a list of commands and responses exchanged between servers during transmission of the message that is sufficient to prove delivery of the message to the recipient, providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail." (*Id.*)

2. Analysis

This phrase is claimed by the '913 Patent as follows:

> **1**. A method of transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:
>
> transmitting the message to the recipient's Mail Transport Agent in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols; and
>
> recording at the server some portion of the selected one of the *SMTP and ESMTP protocol dialog* between the server and the recipient through the server including those portions of the selected one of the *SMTP and ESMTP protocol dialog* between the server and the recipient in which the receiving Mail Transport Agent accepts or declines delivery of the transmitted message.

'913 Patent col. 27 ll. 41–54 (emphasis added).

For the reasons expressed for Term No. 13, the Court finds that the majority of RPost's construction would assist the jury in understanding the concepts of this term. Thus, the Court construes "SMTP and ESMTP protocol dialog" as "SMTP or ESMTP

1   data including a list of at least one protocol command and at least one protocol response

2   exchanged between devices during transmission of a message."

P. "data transport protocol dialog" (Term No. 16)

1. The Parties' Positions

For the final "dialog" term, RPost proposes a construction of "transport data including a list of at least one command and at least one response." (Doc. 191-1 at 6).

GoDaddy proffers the same construction as it did for Term Nos. 13, 14, and 15: "a list of commands and responses exchanged between servers during transmission of the message that is sufficient to prove delivery of the message to the recipient, providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail." (*Id.*)

2. Analysis

"Data transport protocol dialog" is used in Claim 1 of the '199 Patent as follows:

> **1**. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:
>
> . . .
>
> receiving at the server at least a portion of a *data transport protocol dialog* generated during transmission of the message from the server to the recipient; and
>
> . . .
>
> forming at the server a first information from the at least a portion of the *data transport protocol dialog* and the indication of the failure to deliver the message by the recipient . . . .

'199 Patent col. 27 ll. 58–col. 28 ll. 4 (emphasis added).

For the reasons set forth in Term No. 13, the Court finds that the majority of RPost's construction would be helpful to the jury. Thus, the Court construes this term as: "transport data including a list of at least one command and at least one response exchanged between devices during transmission of a message."

Q. **"before the message is authenticated (any authentication of the message) by the server" (Term No. 17)**

1. **The Parties' Positions**

RPost contends that Term No. 17 should be construed as "before the content and delivery of the message is proved (proving the content and delivery of the message) by the server. The plain language of this phrase does not require that any authentication of the message be performed by the server." (Doc. 191-1 at 6–7). To support the latter part of its construction, RPost notes that Judge Gilstrap came to a similar conclusion. (Doc. 114 at 12–13).

GoDaddy agrees that this phrase requires providing proof of the content and delivery of a message but contends that the construction should also include "how" and "why" such proof is generated. (Doc. 117 at 14). Thus, GoDaddy proposes the following construction: "before proving the content and delivery of the message by comparing and matching authenticable information so as to provide a legal or other evidentiary status on par with, if not superior to, that of registered United States mail." (*Id.*)

RPost replies that GoDaddy's proposal impermissibly imports limitations from the specification into the claim. (Doc. 119 at 8).

2. **Analysis**

This disputed phrase is found in several claims of the '389 Patent and Claim 1 of the '199 Patent. The '389 Patent claims as follows:

> **1**. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:
>
> . . .
>
> transmitting, *before any authentication of the message*, a copy of the message and the first information to the sender from the server.

'389 Patent col. 27 ll. 58–col. 28 ll. 7 (emphasis added).

> **14**. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:

storing a representation of the message and the first information received by the server from the recipient in a memory, *before any authentication of the message*.

15. The method of claim **14**, further comprising:

Transmitting the representation of the message and the first information received by the server from the recipient to the sender from the server, *before any authentication of the message*.

Id. col. 29 ll. 16–col. 30 ll. 13 (emphasis added). Similarly, the '199 Patent claims:

1. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:

. . .

transmitting, *before any authentication of the message*, a copy of the first information to the sender from the server.

'199 Patent col. 27 ll. 58–col. 28 ll. 7 (emphasis added). The general method of "authentication" is disclosed in the shared specification as follows:

A general object of the present invention is to provide a system and method for reliably verifying via secure and tamper-proof documentation the content and delivery of an electronic message such as an e-mail. . . .

. . . . To later verify and authenticate information contained in the receipt, the originator or user sends a copy of the receipt to the system. The system then verifies that the digital signature matches the original message and the rest of the receipt. If the two match, then the system sends a letter or provides other confirmation of authenticity verifying that the electronic message has not been altered.

. . . .

. . . . The encrypted message digest provides one type of message authentication or validation code, or secure documentation. Other message authentication and/or validation codes may also be generated and used.

'389 Patent col. 3 ll. 6–61.

Having performed this calculation for each file attached to the original message, the system prepares a report which reports on the authenticity of the receipt and each of its attached files (**710**) or which reports the failure of validation (**712**).

Id. col. 24 ll. 66–col. 25 ll. 3.

1

2

3

4

To begin, GoDaddy's "comparing and matching" proposal is comparable to that of the defendants before Judge Gilstrap who proposed "a comparison of two digital fingerprints (hashes) to determine that they match." *RMail*, 2013 WL 968246, at *59. Judge Gilstrap analyzed that proposal as follows:

5

6

7

8

9

10

> On balance, Defendants' proposal of "a comparison of two digital fingerprints (hashes) to determine that they match" is an aspect of a preferred embodiment that should not be imported into the construction of the comparatively generic term "authentication." *Electro Med. Sys., S.A. v. Cooper Life Scis., Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994) ("[A]lthough the specifications may well indicate that certain embodiments are preferred, particular embodiments appearing in a specification will not be read into the claims when the claim language is broader than such embodiments.")

11

12

13

14

15

16

17

Id. The Court agrees with Judge Gilstrap. While the specification of the invention does disclose that the server can compare and match certain information about the message to authenticate the message, the claim itself uses broad language not limited to comparing and matching. Thus, the Court refrains from reading limitations from the specification into the claim and rejects this portion of GoDaddy's proposal. *See Teleflex*, 299 F.3d at 1326 ("[L]imitations from the specification are not to be read into the claims[.]" (citing *Comark Commc'ns*, 156 F.3d at 1186)).

18

19

20

21

22

23

24

25

As to GoDaddy's proposed evidentiary limitation, the Court incorporates its analysis as set forth in Term No. 7 and rejects the proposal. Specifically, even though "authentication" is the second step of the "proof" process claimed by the Tomkow Patents, the Court does not agree with GoDaddy that the status of the message—even after authentication—must be tantamount to the evidentiary quality of registered United States mail. The specification explicitly eschews the notion that any legal status be afforded to a message, and the Court will not import any lingering evidentiary limitations from the specification into the claim, particularly when the limitations relate to the "use" of the invention.

26

27

28

Finally, RPost proposes that the jury be instructed that "the plain language of this phrase does not require that any authentication of the message be performed by the

1 server." (Doc. 191-1 at 6). The Court finds that including this sentence in the construction

2 is unnecessarily redundant as the phrase "before the message is authenticated" is readily-

3 understandable.

4 For these reasons, the Court construes "before the message is authenticated (any

5 authentication of the message) by the server" as "before the content and delivery of the

6 message is proved (proving the content and delivery of the message) by the server."

7 **R.   "Mail Transport Agent" (Term No. 18)**

8 **1.   The Parties' Positions**

9 RPost argues that MTA should be interpreted as "software that transfers electronic

10 messages from one computer to another." (Doc. 191-1 at 7). RPost explains that this

11 construction is consistent with "dictionary" definitions of MTA. (Doc. 114 at 13 (citing

12 http://en.wikipedia.org/wiki/Message_transfer_agent)).

13 GoDaddy proposes that MTA should be construed as "software that resides on the

14 server and that is dedicated to transferring and receiving electronic messages from one

15 computer to or from another." (Doc. 191-1 at 7). GoDaddy stresses that its definition

16 means that "the software, not the server" is "dedicated" to the transfer and receipt of

17 messages. (Doc. 117 at 15). GoDaddy also argues that the MTA must be installed on the

18 server "because the asserted claims are directed to servers that send and receive

19 messages." (*Id.*)

20 RPost denounces GoDaddy's proposal because "[a]lthough MTA software may be

21 installed on a server, the plain claim language and the intrinsic record do not require that

22 MTA software always be installed on a server or that the server be dedicated to

23 transferring electronic messages." (Doc. 114 at 13). RPost underscores that the server can

24 also "record[] some portion of the selected one of the SMTP and ESMTP protocol dialog

25 between the server and the recipient." (*Id.*) RPost further contends that construing MTA

26 as residing on "the server" is redundant and confusing because the jury will not know on

27 which server the MTA resides. (Doc. 119 at 8).

28

2.   Analysis

"Mail Transport Agent" is used in the '913 Patent as follows:

> **1**. A method of transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:
>
> transmitting the message to the recipient's *Mail Transport Agent* in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols; and
>
> recording at the server some portion of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient through the server including those portions of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient in which the receiving *Mail Transport Agent* accepts or declines delivery of the transmitted message.

'913 Patent col. 27 ll. 41–54 (emphasis added). While the parties agree that MTA is software that can transfer messages, their proposals diverge in three respects.

The first dispute concerns whether the construction should state where the MTA software is located. In this regard, the Court agrees with GoDaddy that the construction should include the MTA software's location, but also finds merit in RPost's concern that if the construction reads "the server," the jury could be confused as to which server contains the MTA. Thus, the Court adopts a modified version of GoDaddy's proposal: "resides on a server."

Second, because the MTA software is acting as an intermediary between the sender and recipient, the Court agrees with GoDaddy that the MTA must be able to "receive" electronic messages. *See* '913 Patent col. 27 ll. 48–54.

Finally, the Court rejects GoDaddy's contention that the MTA software must be "dedicated to" transferring and receiving electronic messages. "Dedicated to" imports unnecessary ambiguity into the construction.

For these reasons, the Court construes MTA as "software that resides on a server and that transfers and receives electronic messages from one computer to or from another."

S.   "sender" (Term No. 19) and "recipient" (Term No. 20)

1.   The Parties' Positions

RPost argues that the terms "sender" and "recipient" have plain and ordinary meanings that require no further construction from the Court. (Doc. 191-1 at 7). RPost emphasizes that Judge Gilstrap gave these terms plain meaning constructions and urges the Court to adopt a similar plain meaning construction. (Doc. 114 at 13).[12] Alternatively, RPost proposes that "sender" be construed as "originator of a message" and "recipient" as "who the sender intends to receive the message." (*Id.*)

GoDaddy responds that no plain meaning of the terms resolves the parties' dispute and criticizes RPost's alternative constructions as "impermissibly vague." (Doc. 117 at 15–16). Instead, GoDaddy proposes that "sender" be construed as "the computer that originates the message" and "recipient" as "the computer that receives the message at its intended destination." (Doc. 191-1 at 7). According to GoDaddy, the Tomkow Patents "provide" that the terms are "computers" because the shared specification recites that the "sender" "create[s] the original messages" and "has both a name and Internet address, and only computers have .com Internet addresses as recited in the patents." (Doc. 117 at 15–16).

RPost replies that because the Tomkow Patents "repeatedly equate a user (i.e., a person) with 'sender,'" GoDaddy's "computer" proposal violates the intrinsic record. (Doc. 119 at 8–9). RPost also protests that GoDaddy's construction violates the doctrine of claim differentiation because it defines "sender" and "recipient" in the same way as "originating processor" and "recipient processor." (Doc. 114 at 13–14). RPost contends that because the inventor used different words in the claims, there is a presumption that he intended the terms to have different meanings. (*Id.* (citing *Comark Commc'ns*, 156 F.3d at 1187)). For its part, GoDaddy argues that the claim differentiation doctrine should

---

[12] Judge Gilstrap analyzed these terms as used in the Feldbau Patent. *See RMail*, 2013 WL 968246, at *25–27.

not be applied here "in light of the patents' disclosure of the meaning of these terms."

(Doc. 117 at 16).

2.   Analysis

The claim terms "sender" and "recipient" are peppered throughout the Tomkow

Patents. A few examples include:

> **1**. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:
>
> receiving the message at the server from the *sender*
>
> . . .
>
> receiving at the server at least a portion of a mail transport protocol dialog generated during transmission of the message from the server to the *recipient*; and
>
> receiving at the server from the *recipient* an indication of the receipt of the message by the *recipient*;
>
> forming at the server a first information from the at least a portion of the mail transport protocol dialog and the indication of the receipt of the message by the *recipient*; and
>
> transmitting, before any authentication of the message, a copy of the message and the first information to the *sender* from the server.

'389 Patent col. 27 ll. 58–col 28 ll. 7 (emphasis added).

> **1**. A method of transmitting a message from a sender to a recipient and providing an indication that the message was opened by the recipient, comprising:
>
> . . .
>
> adding a link to the message by the server, the link configured to execute when the message is opened at the *recipient* to provide an indication that the message has been opened by the *recipient*,
>
> executing the link when the message is opened at the *recipient* to control the server to provide an indication that the message has been opened at the *recipient*,
>
> providing an authenticatible information related to the message, including the indication of the opening of the message at the *recipient*, at the server,

transmitting the indication of the opening of the message at the *recipient*, and the authenticatible information from the server to the *sender*,

'104 Patent col. 27 ll. 63–col. 28 ll. 16 (emphasis added).

To support its position that "sender" and "recipient" should be defined as "computers," GoDaddy cites to the following sentence of the shared specification: "[f]or example, where the original sender of the message is user John Smith with Internet address jsmith@adomain.com . . . ." '199 Patent col. 9 ll. 53–54. GoDaddy explains that "sender" and "recipient" must be construed to mean "computers" because only computers have Internet addresses. (Doc. 117 at 15–16).

In this regard, the Court finds that the presence of the phrase "user John Smith" forecloses construing "sender" strictly as "computer." While it may technically be true that only computers have Internet addresses, a "user"—disclosed here as the "original sender"—is not necessarily a computer. Auxiliary disclosures in the specification equate "sender" with "user" and "originator." *See* '199 Patent col. 18 ll. 37–39 ("To register an e-mail message, in step **201** an *originator/sender/user* creates an email message using any Internet Mail User Agent (MUA)."). While it is undisputed that the asserted claims involve electronic methods of transmitting information, "sender" is best understood as a combination of both the user causing the computerized device to originate the message and the computerized device itself. In fact, GoDaddy's own argument supports this conclusion. *See* (Doc. 117 at 15 ("The specification also provides that the 'sender' has *both a name and Internet address . . . .*" (emphasis added))).

Correspondingly, the specification also forecloses construing "recipient" as "computer." For example, the specification discloses that "[n]otifications will not be generated, if ever, until the *recipient* opens *his* MUA e-mail client and takes some action with respect to the received mail." *Id.* col. 15 ll. 46–49 (emphasis added). The specification further explains that "MUA notices may report, among other things, that a message has been read *by a recipient . . . .*" *Id.* col. 15 ll. 63–64 (emphasis added). Thus,

the intrinsic record compels defining "recipient" in a manner that includes both the user and the device.

Finally, GoDaddy proposes that "recipient" should be defined with the limitation "at its intended destination" but did not explain this modification in its briefing or during the *Markman* Hearing. *See* (Doc. 117 at 15–16). The Court finds this phrase to be ambiguous and therefore does not incorporate it in the construction.

For these reasons, the Court construes "sender" as "a combination of (1) the user that caused the computerized device to originate the message and (2) the computerized device itself" and "recipient" as "a combination of (1) the user that the sender intends to receive the message and (2) the computerized device that receives the message."

T. "originating processor" (Term No. 21) and "recipient processor" (Term No. 22)

1. The Parties' Positions

RPost argues that "originating processor" and "recipient processor" need not be construed because the terms are used according to their plain and ordinary meanings. (Doc. 191-1 at 7). Alternatively, RPost proffers that "originating processor" be construed as "a computing device where the message originates" and "recipient processor" as "a computing device where the recipient receives the message." (*Id.*) RPost explains that a skilled artisan would understand that electronic messages can be "sent and received using computing devices other than computers." (Doc. 119 at 9).

GoDaddy proposes the same respective constructions as it did for "sender" (Term No. 19) and "recipient" (Term No. 20). *See* (Doc. 191-1 at 7). Thus, GoDaddy defines "processor" as "computer." (*Id.*)

RPost attacks GoDaddy's proposal for "originating processor" as being "too narrow because it requires that the computer itself originate the message and excludes the [far] more . . . likely case of a user originating a message at a computer." (Docs. 114 at 14; 119 at 9). RPost also claims that GoDaddy's proposed language "at its intended

1   destination" is flawed because it is unclear what such a limitation actually connotes in the

2   electronic message context. (Docs. 114 at 14; 119 at 9).

3   **2.   Analysis**

4   These two terms are used in the '104 and '389 Patents as follows:

5   **27**. A system for transmitting a message from an originating
         processor to a recipient processor in an electronic mail system and
6   providing an indication that the message was opened by the recipient
7   processor, comprising:

8   a server in electronic communication in the electronic mail system,
         the server receiving the message from the *originating processor* and adding
9   a link to the message before transmitting the message and link to the
10   *recipient processor*, the link being configured to execute automatically
         when the message is opened at the *recipient processor* to control the server
11   to provide an indication at the server that the message has been opened at
         the *recipient processor* . . . .
12
13   '104 Patent col. 31 ll. 20–32 (emphasis added).

14   **7**. A system for transmitting a message through an electronic mail
         system from an originating processor to a recipient processor and providing
15   proof of receipt of the message by the recipient process[or], comprising:

16   a server displaced from the *originating processor*, the server capable
         of being configured by software commands to:
17
18   receive a message from the *originating processor* and to transmit the
         message to the *recipient processor*,

19   receive an indication of receipt of the message from the *recipient
         processor* and a mail transport protocol dialog generated by the electronic
20   mail system during transmission of the message from the server to the
21   *recipient processor*;

22   generate a first information including the indication of receipt of the
         message from the *recipient processor* and at least a portion of the mail
23   transport protocol dialog generated by the electronic mail system during
24   transmission of the message from the server to the *recipient process*or.

25   '389 Patent col. 28 ll. 33–52 (emphasis added).

26   To begin, the Court finds that the jury would be aided by defining these terms.

27   RPost's own argument proves construction is necessary. Namely, there is a semantical

28   dispute as to whether the "originating processor" is a device "that" originates the message

1   or if it is "where" the message originates. Likewise, there is a dispute whether the

2   "recipient processor" is "where" the message is received by the recipient or if it is a

3   device "that" receives the message. Absent construction, the jury could be confused on

4   these issues.

5   In light of the Court's construction of "sender," the Court concludes that

6   "originating processor" is "where" the message originates. A combination of the user

7   interfacing with the originating processor originates the message, and this occurs at the

8   originating processor. Thus, the Court adopts this portion of RPost's alternative proposal.

9   Conversely, the Court finds that "recipient processor" is best understood as the

10   device "that" receives the message for the recipient. Unlike when a message originates

11   through an interaction between the user and originating processor, when a message is

12   received, it is the processor—not the user—"that" receives the message. The user may

13   open the electronic message at the processor, but it is the processor that receives the

14   message.

15   Finally, the Court must resolve whether "processor" should be construed as

16   "computing device" or "computer." RPost complains that "computer" is too narrow,

17   while GoDaddy laments that "computing device" is too vague. To resolve this dispute,

18   the Court looks to how a skilled artisan would view the term "processor." On one hand, a

19   skilled artisan would recognize that "processor" means a "computer," a "central

20   processing unit" ("CPU"), or a "program that translates another program into a form

21   acceptable by the computer being used." *See* Am. Heritage Dictionary of the English

22   Language 1398 (4th ed. 2006). On the other hand, a skilled artisan would also appreciate

23   "CPU" to mean "the *device* that interprets and executes instructions." Microsoft

24   Computer Dictionary 92 (5th ed. 2002) (emphasis added).

25   On balance, the Court finds that because the plain meaning of "processor"

26   includes "computer," the word "computer" should be assimilated in the construction.

27   However, it appears that a skilled artisan would understand that other types of devices

28   with processors could send and receive messages. The Court, therefore, construes

- 79 -

"originating processor" as "the computerized device where the message originates" and "recipient processor" as "the computerized device that receives the message."

U. "providing proof of receipt of the message by the recipient processor" (Term No. 23)

1. The Parties' Positions

The crux of the parties' disagreement over Term No. 23 is whether the phrase is limiting upon the claim. Because the phrase is found only in the preamble of Claim 7 of the '389 Patent, RPost contends that it is not limiting because it does not give life, meaning, and vitality to the claim. (Doc. 114 at 14). RPost argues that the inventor simply used the phrase to "state the purpose or intended use of the claimed system" and that the body of the claim is "structurally complete." (*Id.*)

In contrast, GoDaddy proffers a construction of "providing evidence that confirms receipt of the message by the recipient, the evidence providing a legal or other evidentiary status on par with, if not superior to, that of registered United States mail." (Doc. 117 at 10).[13] Because Claim 7 does not include any "authentication" terms, GoDaddy insists that construction is necessary to provide an "essential limitation" to the claim. (*Id.* at 11). GoDaddy further defends its construction by remarking that the preamble must be construed in order to "capture the purported invention's core concept of providing proof regarding the delivery and content of an e-mail message and to differentiate claim 7 from prior art." (*Id.* (citation omitted)).

2. Legal Standard

Whether a preamble limits a claimed invention is a question of law and is "resolved only on review of the entire patent to gain an understanding of what the inventors actually invented and intended to encompass by the claim." *Catalina Mktg.,*

---

[13] GoDaddy's proposed construction as recorded in its briefing does not correlate with the parties' Amended Joint Claim Construction Statement. *See* (Docs. 117 at 10; 191-1 at 8). In the Amended Joint Claim Construction Statement, GoDaddy's proposal is listed as "providing proof of receipt of the message by the recipient processor." (Doc. 191-1 at 8). The Court will analyze GoDaddy's proposal as outlined in its briefing.

1 *Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 807–08 (Fed. Cir. 2002) (quotation

2 omitted). A preamble may limit the invention if it "recites essential structure or steps, or

3 if it is 'necessary to give life, meaning and vitality' to the claim." *Id.* (quoting *Pitney*

4 *Bowes, Inc. v. Hewlett–Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999)). "When the

5 preamble is essential to understand limitations or terms in the claim body, the preamble

6 limits claim scope." *Id.* (citing *Pitney Bowes*, 182 F.3d at 1306).

7 Conversely, a preamble is not limiting "where a patentee defines a structurally

8 complete invention in the claim body and uses the preamble only to state a purpose or

9 intended use for the invention." *Id.* (citing *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir.

10 1997)). Furthermore, "preamble language merely extolling benefits or features of the

11 claimed invention does not limit the claim scope without clear reliance on those benefits

12 or features as patentably significant." *Id.* at 809 (citations omitted).

13 Finally, "preambles describing the use of an invention generally do not limit the

14 claims because the patentability of apparatus or composition claims depends on the

15 claimed structure, not on the use or purpose of that structure." *Id.* (citation omitted).

16 Indeed, "[t]he inventor of a machine is entitled to the benefit of all the uses to which it

17 can be put, no matter whether he had conceived the idea of the use or not." *Id.* (quotation

18 omitted). "Again, statements of intended use or asserted benefits in the preamble may, in

19 rare instances, limit apparatus claims, but only if the applicant clearly and unmistakably

20 relied on those uses or benefits to distinguish prior art." *Id.*

21 **3. Analysis**

22 Term No. 23 appears only in the preamble of Claim 7 of the '389 Patent. Claim 7,

23 in its entirety, reads:

24 **7**. A system for transmitting a message through an electronic mail
25 system from an originating processor to a recipient processor and *providing*
proof of receipt of the message by the recipient process, comprising:

26 a server displaced from the originating processor, the server capable
27 of being configured by software commands to:

28

receive a message from the originating processor and to transmit the message to the recipient processor,

        receive an indication of receipt of the message from the recipient processor and a mail transport protocol dialog generated by the electronic mail system during transmission of the message from the server to the recipient processor;

        generate a first information including the indication of receipt of the message from the recipient processor and at least a portion of the mail transport protocol dialog generated by the electronic mail system during transmission of the message from the server to the recipient processor.

'389 Patent col. 28 ll. 33–52 (emphasis added). The question before the Court is whether "providing proof of receipt of the message by the recipient processor" is necessary to give life, meaning and vitality to Claim 7 or else recites essential steps or structure.

As GoDaddy observes, unlike the rest of the asserted claims in the Tomkow Patents, Claim 7 does not include any "authentication" terminology. The invention's ability to authenticate, i.e., verify or prove, a certain aspect of a message—such as delivery or non-delivery—is necessary to differentiate the invention from prior art. In this regard, RPost argues that Claim 7 expresses "several proofs of receipt of the message, including 'an indication of receipt of the message' and 'a mail transport protocol dialog generated during transmission of the message.'" (Doc. 114 at 14–15).[14] As discussed for Term No. 4, however, providing an "indication" is merely the first step in the two-step "proof" process. The "proof of receipt" emerges not from the "indication" or "dialog" but from "authentication"—the second step which is absent from the body of Claim 7.

_____

[14] GoDaddy contends that this argument is internally inconsistent. (Doc. 117 at 10–11). The Court agrees. RPost argues that there are several "proofs of receipt" recited in the body of Claim 7 but only points to the "indication" and "dialog" language. *See* (Doc. 114 at 14–15). RPost concedes, however, that the "proof" of receipt occurs when the message is "authenticated"—not when an "indication" or "dialog" is generated. *See* (Doc. 191-1 at 6 (construing "before the message is authenticated" as "before the content and delivery of the message is proved")). As explained in Term No. 4, the Tomkow Patents integrate a two-step process to prove the delivery and content of a particular message. It is inconsistent for RPost to construe "indication" merely as "information that indicates" but then turn around and argue that an "indication" is also "proof of receipt."

Accordingly, the Court finds that "providing proof of receipt of the message" is a necessary limitation upon Claim 7 and must be construed.[15]

As to the construction of Term No. 23, GoDaddy's proposal again requires the invention to provide proof with a "legal or other evidentiary status on par with, if not superior to, that of registered United States mail." (Doc. 191-1 at 8). As explained for Term Nos. 7 and 17, however, the Tomkow Patents do not impose that evidentiary limitation on its messages.[16] Instead, because the term "authenticated" from Term No. 17 is analogous to the disputed claim term here, the Court finds that a similar construction is appropriate.

For these reasons, the Court concludes that Term No. 23 limits Claim 7 of the '389 Patent and adopts a construction of: "proving that the message was received by the recipient processor."

---

[15] The Court notes that the specification is riddled with references to "proving," "authenticating," or "verifying" some aspect of the message, underscoring the importance of the feature to the claimed invention. *See Rotatable Techs. LLC v. Motorola Mobility LLC*, 567 F. App'x 941, 943 (Fed. Cir. 2014). For example, the '389 Patent's Title, Abstract, Background of Invention, Summary of the Invention, Brief Description of the Drawings, and Detailed Description of the Preferred Embodiments all recite either "authentication, "verification," or "proving." *See* '389 Patent (54), (57), col. 1 ll. 21, col. 3 ll. 7, col. 5 ll. 60, col. 17 ll. 1–65.

[16] Notably, "proving" an aspect of the message is not, as RPost contends, merely a "use" of the invention. Instead, it is a distinguishing function of the invention requiring adequate structure. On the other hand, the "evidentiary" limitation GoDaddy repeatedly proposes *is* a "use" of the invention. Namely, whether the "proof" that the invention provides equates to "a legal or other evidentiary status on par with, or superior to registered United States mail" speaks to the ability to "use" the invention for a specific purpose. The function of "proving" is not so narrow and "[t]he inventor of a machine is entitled to the benefit of all the uses to which it can be put, no matter whether he had conceived the idea of the use or not." *Catalina Mktg.*, 289 F.3d at 809 (quotation omitted).

V. "the link configured to execute when the message is opened at the recipient" (Term No. 24)

1. The Parties' Positions

RPost argues that "the link configured to execute when the message is opened at the recipient" should be construed as "the link programmed to execute when the message is opened at the recipient." (Doc. 191-1 at 8). RPost insists this slight modification is necessary to clarify for the jury that the term is "used in a computer programming sense." (Doc. 119 at 10).

GoDaddy responds that RPost has not shown that "configured" is synonymous with "programmed" and complains that RPost's proposal changes the scope of the claim term. (Doc. 117 at 16). Instead, GoDaddy contends that the phrase is "plain on its face" and needs no construction. (*Id.*)

2. Analysis

As explained for Term Nos. 8 and 9, "configured" is a term that has a plain meaning that the jury will be able to understand. RPost has not shown that the term is used in a manner that is contrary to that plain meaning. Consequently, the Court does not construe Term No. 24.

W. "the server (being) displaced from the recipient (recipient processor)" (Term No. 25)

1. The Parties' Positions

For the twenty-fifth disputed term of the Tomkow Patents, RPost recommends a construction of "the server (being) logically displaced from the recipient (recipient processor)." (Doc. 191-1 at 8). RPost contends this construction will "clarify the meaning of the plain language of the claim[] for the benefit of the jury [and does] not otherwise change the meaning of the claim[]." (Doc. 114 at 15).

GoDaddy responds that RPost's proposed construction is not synonymous with the claim language and "changes the meaning and scope of the term." (Doc. 117 at 16).

1   Instead, GoDaddy argues that no construction is needed because the term is used

2   according to its plain and ordinary meaning. (*Id.*)

3   RPost replies that construing the term "displaced" as "logically displaced" would

4   simplify for the jury that the server and recipient are separated "in a computer

5   architecture sense but not necessarily physically separate." (Doc. 119 at 10).

6   **2.   Analysis**

7   This phrase is used in Claims 1 and 23 of the '104 Patent; Claims 1, 7, 14, and 15

8   of the '389 Patent; all asserted claims for the '199 Patent; and Claim 1 of the '198 Patent.

9   For example, the '104 and '198 Patents claim:

10   **1**. A method of transmitting a message from a sender to a recipient
         and providing an indication that the message was opened by the recipient,
11   comprising:

12   receiving the message at a server from the sender, *the server being*
         displaced from the recipient . . . .
13

14   '104 Patent col. 27 ll. 63–67 (emphasis added); *see* '198 Patent col. 28 ll. 6–10 (same).[17]

15   RPost's proposal injects "logically" before the claim term "displaced." Contrary to

16   RPost's argument, such a construction adds ambiguity to a readily understandable term.

17   RPost has not shown that the jury would be confused as to the meaning of the generic

18   term "displaced." Accordingly, the Court will not construe Term No. 25 and adopts

19   GoDaddy's proposal of ordinary meaning.

20   **X.   "the server constructs authenticatible information related to the**
                message" (Term No. 26)

21   **1.   The Parties' Positions**

22   RPost argues that the claim term "constructs" should be construed as "assembles"

23   because such a construction would "clarify the meaning of the plain language of the

24   claim[] for the benefit of the jury [and does] not otherwise change the meaning of the

25

26   [17] No asserted claim uses the term "recipient processor." Thus, the Court rejects
27   this portion of RPost's proposed construction.

28

1   claim[]." (Doc. 114 at 15). Thus, RPost proffers a construction of: "the server assembles

2   authenticatible information related to the message." (Doc. 191-1 at 8).

3   GoDaddy responds that RPost has not shown that "assembles" is synonymous

4   with "constructs" and asks the Court to reject RPost's proposal. (Doc. 117 at 16).

5   According to GoDaddy, "constructs" is a "readily-understood" term that the jury will be

6   able to apply without further construction. (*Id.*)

7   RPost replies that its construction is necessary because it clarifies for the jury that

8   "constructs" means the "assembling of information, such as described in the creation of a

9   delivery receipt." (Doc. 119 at 10). At the *Markman* Hearing, RPost further explained its

10   position by noting that the jury could misinterpret "constructs" as creating from new or

11   from scratch, versus taking and assembling information that already exists. According to

12   RPost, "constructs" as used in the '104 Patent does not require the server to create new

13   information.

14   **2.   Analysis**

15   This disputed phrase is used in Claim 27 of the '104 Patent as follows:

16   **27**. A system for transmitting a message from an originating
             processor to a recipient processor in an electronic mail system and
17   providing an indication that the message was opened by the recipient
             processor, comprising:
18

19   a server in electronic communication in the electronic mail system,
             the server receiving the message from the originating processor and adding a
20   link to the message before transmitting the message and link to the recipient
             processor . . .
21

22   wherein *the server constructs authentication information related to
             the message . . . .*

23   '104 Patent col. 31 ll. 20–34 (emphasis added).

24   The Court agrees with GoDaddy that RPost failed to show that "constructs" should

25   be construed as "assembles." The Meriam-Webster Dictionary defines "construct" as "to

26   make or form by combining or arranging parts or elements." The Merriam-Webster

27   Dictionary, http://www.merriam-webster.com/dictionary/construct (last visited January

28

19, 2016). On the other hand, "assemble" is defined as "to bring together" or "to fit together the parts of." *Id.*, http://www.merriam-webster.com/dictionary/assemble (last visited January 19, 2016). As readily seen, these two words have different meanings.

As used in Claim 27, "constructs" requires that the server take certain information and "construct" something else, namely, "authenticatible information." The server does not merely "assemble" the pre-existing information to form the authenticatible information. A simple example makes this distinction clear. When a builder "constructs" a backyard patio, he combines various pre-existing items—such as wood, paint, and nails—in a way that creates a new item comprised of the pre-existing items: the patio. If the builder simply were to "assemble" the wood, paint, and nails by gathering them into one place, without more, he would have "constructed" nothing.

Here, Claim 27 does not merely state that the server "assembles" together various forms of pre-existing information, but claims that the server "constructs authenticatible information." Because RPost has not shown that the inventor unequivocally chose to define "constructs" in a manner different from the term's plain meaning, the Court rejects RPost's proposed construction and does not construe the term. *See Omega Eng'g*, 334 F.3d at 1324.

VII. Claim Construction of Disputed Claim Terms in the Feldbau Patent

A. "authenticating a dispatch and contents of the dispatch" (Term No. 1)

1. The Parties' Positions

RPost urges the Court to adopt the construction of this phrase as crafted by Judge Gilstrap. (Doc. 114 at 13). Judge Gilstrap reasoned that the claim and specification language make clear that the patent's objective is to provide "evidence" that "can" be used by the sender to later prove aspects related to the dispatch. *See RMail*, 2013 WL 968246, at *7–8. Espousing this reasoning, RPost contends that "authenticating a dispatch and contents of the dispatch" should be construed as "provide evidence capable of being used to prove the contents of the dispatch." (Doc. 114 at 13).

1   GoDaddy responds that RPost's proposed construction is flawed in multiple

2   respects. (Doc. 117 at 17). First, GoDaddy explains that RPost's construction forsakes the

3   "conjunctive structure" of the phrase. (*Id.*) Namely, by providing evidence concerning

4   only the contents of the dispatch, GoDaddy argues that RPost's construction reads out

5   claim language requiring proof that the message was dispatched. (*Id.*) Second, GoDaddy

6   contends that RPost's construction is "too loose" a standard for the higher level of

7   "proof" purportedly embodied in the Feldbau Patent. (*Id.*) GoDaddy therefore proposes a

8   construction of "proving the contents and the receipt of a dispatch by using reliable

9   evidence on par with that used to notarize documents or to admit as evidence in a court of

10   law." (*Id.*)

11   RPost replies that GoDaddy's proposed construction improperly incorporates

12   limitations from the specification into the claim. (Doc. 119 at 10).

13   **2.   Analysis**

14   The phrase "authenticating a dispatch and contents of the dispatch" is disclosed in

15   Claims 60 and 82 of the Feldbau Patent. Claim 60 discloses:

16   **60**. A method of authenticating a dispatch and contents of the
17   dispatch <u>successfully</u> transmitted from a sender to a recipient . . .

18   . . .

19   Associating, by **[an]** the authenticator functioning as a non-
     interested third party with respect to the sender and the recipient, the
20   content data with dispatch record data which includes at least said time
     related indicia and an indicia related to the destination of the dispatch, to
21   generate authentication data which *authenticate the dispatch and the*
     contents of the dispatch . . . .
22

23   '219 Patent col. 2 ll. 56–col. 3 ll. 7 (amended version) (amendments by Ex Parte

24   Reexamination Certificate are shown with additions underlined; deletions in bolded

25   square brackets; italics added for emphasis). Similarly, Claim 82 discloses:

26   **82**. An information dispatch system in an electronic communication
     network comprising:

27   . . .

28

- 88 -

1
2
3

    an authenticator functioning as a non-interested third party with respect to the sender and the recipient for *authenticating the dispatch and contents of the dispatch* transmitted from the source transmitting system to the destination receiving system . . . .

4

Id. col. 4 ll. 4–18 (emphasis added).

5

6

7

8

9

    Initially, the Court agrees with Judge Gilstrap that the specification makes clear that "authenticating"—as the term is used by the Feldbau Patent—merely means storing evidence of the dispatch and its content without simultaneous verification or validation of the dispatch and its content. For example, the specification describes the Feldbau Patent's objective as providing "evidence" that "can" be used by the sender:

10

11

12

    It is therefore the object of the present invention to improve the capacity of conventional systems and methods for dispatching documents and transmitting information *to provide the sender with evidence he can use to prove both the dispatch and its contents*.

13

'219 Patent col. 2 ll. 57–61 (emphasis added). The specification also discloses:

14

15

16

17

18

19

    When it is desired to authenticate the dispatch of the original documents (and possibly also their receipt at the destination 30), either the sender or the document dispatching service provides the associated authentication-information, for example the envelope 32, unopened, to the party which required the authentication. When the envelope 32 is opened, it has associated therewith copies of both the dispatched documents and the dispatch information. *The envelope 32 therefore, provides reliable proof that the original documents 12 were dispatched on the date and to the destination listed on or in envelope 32.*

20

21

Id. col. 5 ll. 63–col. 6 ll. 6 (emphasis added). The Court therefore rejects GoDaddy's argument that "authenticating" should be construed as "proving."

22

23

24

25

26

    Moreover, as Judge Gilstrap explained, to "authenticate" a message, the invention does not speak in terms of the recipient's "receipt" of the message. *See RMail*, 2013 WL 968246, at *7–9. Rather, the claim relates only to the "dispatch" of the information while "receipt" is part of the later optional aspect of "verification." *Id.* Thus, the Court rejects GoDaddy's proposal of "proving the . . . receipt of a dispatch."

27

28

    On the other hand, the Court gives credence to GoDaddy's argument that the phrase "authenticating the dispatch and contents of the dispatch" is facially conjunctive.

1   The specification emphasizes the conjunctive nature of the claim by disclosing that the

2   invention will "provide the sender with evidence he can use to prove *both* the dispatch

3   *and* its contents." '219 Patent col. 2 ll. 60–61 (emphasis added); *see id.* col. 3 ll. 22–24

4   ("Thus, the present invention provides a sender with the capability to prove *both* the

5   dispatch *and* the contents of the dispatched materials." (emphasis added)). Providing

6   evidence capable of proving both the dispatch and its contents is plainly the objective of

7   the Feldbau Patent and distinguishes the invention from prior art. *See id.* col. 2 ll. 30–42;

8   *id.* col. 2 ll. 50–53. Accordingly, the Court's construction requires that the invention

9   provide evidence that "can" be used to prove both (1) the dispatch itself and (2) the

10   contents of the dispatch.

11   GoDaddy also contends that, as embodied by the Feldbau Patent, the quality of

12   evidence provided by the invention must rise to a higher level of "proof" than mere

13   "evidence." (Doc. 117 at 17). To supports its argument, GoDaddy references the entirety

14   of the specification's Background of the Invention and Summary of the Present

15   Invention. (*Id.* (citing '219 Patent col. 1 ll. 30–col. 2 ll. 17; *id.* col. 2 ll. 50–col. 4 ll. 39)).

16   RPost responds that such a construction would improperly read limitations from the

17   specification into the claim, and, in any event, rejects the contention that GoDaddy's

18   proposed limitation language is even disclosed in the specification. (Doc. 119 at 10).

19   The Court agrees with RPost that GoDaddy's proposal requiring the claimed

20   "evidence" to be "reliable evidence on par with that used to notarize documents or to

21   admit as evidence in the court of law" would improperly import limitations from the

22   specification into the claim. Throughout the claims, the inventor chose merely to claim

23   "evidence" or "proof," not the higher level of proof that GoDaddy contends is embodied

24   in the specification. For example, the specification discloses:

25   It is therefore an object of the present invention to improve the capacity of
        conventional systems and methods for dispatching documents and
26   transmitting information to provide the sender *with evidence* he can use to
        prove both the dispatch and its contents.
27

28

'219 Patent col. 2 ll. 57–61 (emphasis added). The section of the specification upon which GoDaddy so heavily relies does not convince the Court that the inventor chose to forego the broader meaning of the term "evidence" by limiting the term to "reliable evidence on par with that used to notarize documents or to admit as evidence in the court of law." Specifically, the Background of the Invention merely provides the reader with context as to the state of the present art, see *id.* col. 1 ll. 30–col. 2 ll. 17, while the Summary of the Present Invention is best understood as offering an example of how the evidence might be used, see *id.* col. 2 ll. 50–col. 4 ll. 39. *See Phillips*, 415 F.3d at 1323 ("To avoid importing limitations from the specification into the claims, it is important to keep in mind that the purposes of the specification are to teach and enable those of skill in the art to make and use the invention and to provide a best mode for doing so."). These disclosures do not evidence the inventor's "clear disavowal" of claim scope. *See Thorner*, 669 F.3d at 1365 (quoting *Teleflex*, 299 F.3d at 1325).

In fact, these portions of the specification provide additional support that the inventor intended only to claim the term "evidence." *See id.* col. 2 ll. 50–56 ("The literature does not provide a comprehensive solution that directly addresses the problem in question: what information has been sent to whom and when. Accordingly, there is a need for a method and system to provide the sender with a convenient means for authenticating both the dispatch and the contents of the documents, electronic information and other information during the normal flow of daily activities."); *id.* col. 3 ll. 22–24 ("Thus, the present invention provides a sender with the capability to prove both the dispatch and the contents of the dispatched materials."). The distinguishing feature of the invention concerns not—as GoDaddy asserts—the quality of the evidence, but the combination of providing evidence capable of being used to prove both the dispatch and its contents.

For these reasons, the Court construes "authenticating a dispatch and contents of the dispatch" as "providing evidence that is capable of being used to prove both the dispatch and the contents of the dispatch."

B.   "authentication data" (Term No. 2)

1.   The Parties' Positions

The parties agree that the majority of Judge Gilstrap's construction of "authentication data" should be adopted, but RPost proposes a modified construction due to a difference in the asserted claims. RPost argues that the term should be construed as "information that is associated with the contents of the dispatch by generating a representation of at least content data, an indicia of a time of successful transmission of the dispatch to the recipient, and an indicia relating to the destination of the dispatch, the representation comprising one or more elements." (Doc. 114 at 16). In contrast, GoDaddy parrots Judge Gilstrap's construction of "information that is associated with the contents of the dispatch by generating a representation of at least a1, a2, and a3, the representation comprising one or more elements." (Doc. 117 at 17).

RPost replies that GoDaddy's construction is flawed because Claim 30—where a1, a2, and a3 are defined—was being asserted in the dispute before Judge Gilstrap but has not been asserted against GoDaddy here. (Doc. 119 at 11). Because a1, a2, and a3 have not been defined by an asserted claim, RPost argues that construing this term with "a1, a2, and a3" would only confuse the jury. (*Id.*) RPost therefore proposes a construction that replaces the a1, a2, and a3 language with the elements as listed in the asserted claims. (*Id.*)

2.   Analysis

The term "authentication data" is used in Claims 60 and 82 of the Feldbau Patent. Claim 60 states as follows:

> **60**. A method of authenticating a dispatch and contents of the dispatch <u>successfully</u> transmitted from a sender to a recipient, comprising the steps of:
>
> receiving content data representative of the contents of the dispatch originated from the sender and being electrically transmitted to said recipient, and a destination of the dispatch;
>
> providing an indicia **[relating to]** <u>of</u> a time of <u>successful</u> transmission of the dispatch <u>to the recipient</u>, said time related indicia being

recorded by an authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

associating by **[an]** the authenticator functioning as a non-interested third party with respect to the sender and the recipient, the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate *authentication data* which authenticate the dispatch and the contents of the dispatch; and

securing by said authenticator, at least part of the *authentication data* against tampering of the sender and the recipient . . . .

'219 Patent col. 2 ll. 56–col. 3 ll. 13 (amended version) (amendments by Ex Parte Reexamination Certificate are shown with additions underlined and deletions in bolded square brackets; italics added for emphasis). The term is also used in Claim 82 as follows:

82. An information dispatch system in an electronic communication network comprising:

. . .

(3) a processor for associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate *authentication data* which authenticate the dispatch and the contents of the dispatch; and

(4) means for securing at least part of the *authentication data* against tampering of the sender and the recipient . . . .

Id. col. 4 ll. 4–39 (emphasis added).

While GoDaddy proposes Judge Gilstrap's exact construction, it goes without saying that "a1, a2, and a3" do not appear in either Claim 60 or 82. GoDaddy insists, nonetheless, that because the specification discloses a1, a2, and a3, the jury will understand that together these three elements compose "authentication data." (Doc. 117 at 18). The only portion of the specification that GoDaddy cites for its argument is the Abstract, which states:

Apparatus and method for authenticating that a sender has sent certain information via a dispatcher to a recipient is disclosed. The method includes the steps of: (a) providing a set A comprising a plurality of information elements a1, . . . an, said information element a1 comprising

the contents of said dispatched information, and said one or more information elements, a2, . . . an comprising dispatch-related information and comprise at least the following elements: a2—a time indication associated with said dispatch; and a3—information describing the destination of the dispatch, and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender, (b) associating said dispatch-related information with said element at by generating authentication-information, in particular comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A . . . .

'219 Patent (57). Two other portions of the specification disclose elements a1, a2, and a3, but both expressly relate to other claims. *See id.* col. 2 ll. 62–col. 3 ll. 20 (relating to Claim 1); *id.* col. 3 ll. 37–49 (relating to Claim 27). Two other claims—Claim 1 and Claim 30—include elements a1, a2, and a3 with accompanying definitions, but RPost does not assert either claim here. *See* '219 Patent col. 1 ll. 26–45, col. 2 ll. 11–27 (amended version).

When interpreting a term, the Court begins with the particular claim language used in the patent. *See Interactive Gift Express, Inc. v. Compuserve, Inc.*, 256 F.3d 1323, 1331 (Fed. Cir. 2001). Here, Claims 60 and 82 expressly disclose the types of information that are "associated" together to "generate authentication data." *Id.* col. 3 ll. 1–7, col. 4 ll. 31–36. In generalized terms, this information includes content data and certain indicia related to transmission of the dispatch. *Id.* Claims 60 and 82 do not, however, mention or refer to elements a1, a2, and a3.[18] Clearly, had the inventor wanted to include the a1, a2, and a3 language in either Claim 60 or 82 he could have done so.

The Court's next step is to review the specification. *See Compuserve*, 256 F.3d at 1331. The only reference in the specification to the a1, a2, and a3 terms is found in the Abstract. Beyond remaining faithful to Judge Gilstrap's construction, GoDaddy provides

---

[18] RPost is not asserting Claim 30 as it did before Judge Gilstrap, nor is RPost asserting Claim 1. Thus, the jury's only plausible reference point to the a1, a2, and a3 terminology is the Abstract.

- 94 -

1   no other reason for the Court to stray from the express limitation language used in Claims

2   60 and 82 in order to introduce "a1, a2, and a3"—terminology that is not incorporated in

3   either asserted claim and is referenced only once in the specification—into the

4   construction. The Court finds that, in the context of this case, using elements "a1, a2, and

5   a3" to define "authentication data" would be confusing and overall unhelpful to the jury.

6   Thus, the Court rejects GoDaddy's proposed construction.

7   At the *Markman* Hearing, GoDaddy argued that RPost's proposed construction is

8   "broader" than Judge Gilstrap's construction because it would allow "authentication

9   data" to include information not authorized by the Patent. Regarding RPost's proposed

10   construction elements of "content data" and "indicia relating to the destination of the

11   dispatch," the Court finds no merit in GoDaddy's argument because both elements are

12   appropriated verbatim from Claims 60 and 82.[19]

13   Claims 60 and 82 do, however, expressly limit "indicia of a time of successful

14   transmission of the dispatch to the recipient." Specifically, the "time related indicia *must*

15   *be* recorded by an authenticator *and* provided in a manner resistant to or indicative of

16   tampering by either of the sender and the recipient." '219 Patent col. 2 ll. 64–67, col. 4 ll.

17   27–30 (amended version) (emphasis added). The Court agrees with GoDaddy that this

18   element as currently listed in RPost's proposal is too broad because it does not account

19   for these limitations.

20   For these reasons, the Court construes "authentication data" as "information that is

21   associated with the contents of the dispatch by generating a representation of at least (1)

22   content data; (2) an indicia of a time of successful transmission of the dispatch to the

23   recipient, said indicia being recorded by an authenticator and provided in a manner that is

24   resistant to or indicative of tampering by either sender or recipient; and (3) an indicia

---

[19] The parties' stipulated construction of "content data" will apply here. *See infra* at 26; (Doc. 191-1 at 14).

1 relating to the destination of the dispatch; where the representation is comprised of one or

2 more elements."[20]

3   **C.   "dispatch record data" (Term No. 3)**

4   **1.   The Parties' Positions**

5   The parties' primary dispute over the term "dispatch record data" concerns the

6 breadth of the term. RPost asserts that the term should be broadly interpreted as

7 "information relating to the dispatch." (Doc. 114 at 16). GoDaddy, on the other hand,

8 proposes a narrower construction: "data recorded by the authenticator during the

9 transmission of the dispatch, which includes at least the time related indicia and the

10 indicia relating to the destination of the dispatch, and which does not include the content

11 data representative of the contents of the dispatch." (Doc. 117 at 18).

12   In reply, RPost argues that because the four limitations in GoDaddy's construction

13 are already recited in the claim, incorporating them in the construction would be

14 redundant and unnecessary. (Doc. 119 at 11 (citing various cases)).

15   **2.   Analysis**

16   The term "dispatch record data" is disclosed in Claims 60 and 82 and their

17 dependent claims. Claim 60 states as follows:

18   **60**. A method of authenticating a dispatch and contents of the
    dispatch <u>successfully</u> transmitted from a sender to a recipient, comprising
19 the steps of:

20   . . .

21   associating, by **[an]** <u>the</u> authenticator functioning as a non-interested
    third party with respect to the sender and the recipient, the content data with
22 *dispatch record data* which includes at least said time related indicia and an

23

24 _____

25   [20] The Court notes that the fourth claim dispute of the Feldbau Patent is "an indicia
    of a time of successful transmission of the dispatch to the recipient." (Docs. 114 at 16–
26 17; 117 at 18–19). As set forth below, the Court construes this phrase as "data that
    represents the time at which the dispatcher forwarded the dispatch for delivery such that
27 the recipient may later be able to receive the dispatch and where the data is obtained
    without any cooperation from the recipient."
28

indicia relating to the destination of the dispatch, to generate authentication data which authenticate[s] the dispatch and the contents of the dispatch . . . .

'219 Patent col. 2 ll. 56–col. 3 ll. 7 (amended version) (amendments by Ex Parte Reexamination Certificate are shown with additions underlined and deletions in bolded square brackets; italics added for emphasis). Similarly, Claim 82 discloses:

82. An information dispatch system in an electronic communication network comprising;

. . .

an authenticator functioning as a non-interested third party with respect to the sender and the recipient for authenticating the dispatch and contents of the dispatch transmitted from the source transmitting system to the destination receiving system, including;

. . .

(2) means for providing an indicia **[relating to]** of a time of successful transmission of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

(3) a processor for associating the content data with *dispatch record data* which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate[s] the dispatch and the contents of the dispatch.

Id. col. 4 ll. 4–36 (amendments by Ex Parte Reexamination Certificate are shown with additions underlined and deletions in bolded square brackets; italics added for emphasis).

GoDaddy's proposed construction includes four limitations, requiring dispatch record data to: (1) be recorded by the authenticator during the transmission of the dispatch, include both (2) time related indicia and (3) indicia relating to the destination of the dispatch, and (4) not include the content data representative of the contents of the dispatch. (Doc. 117 at 18). It is clear that the claim language already limits "dispatch record data" by GoDaddy's second, third, and fourth proposed limitations. On this point, RPost observes that several courts have spurned—on "redundancy" grounds—constructions that incorporate language from the claim itself. (Doc. 119 at 11 (citing

1   *Interdigital Commuc'ns., Inc. v. ZTE Corp.*, 2014 WL 3908771, at *1 (D. Del. Aug. 8,

2   2014); *Asetek Holdings, Inc. v. Coolit Sys.*, 2013 WL 6327691, at *4 (N.D. Cal. Dec. 3,

3   2013); *Ferring B.V. v. Watson Labs., Inc.*, 2013 WL 499158, at *7 (D. Nev. Feb. 6,

4   2013)). As noted above, however, the Federal Circuit rejected the robotic application of

5   such a stringent rule. *See 01 Communique Lab., Inc. v. LogMeIn, Inc.*, 687 F.3d 1292,

6   1296 (Fed. Cir. 2012) ("[Plaintiff] argues that because those functions are set forth

7   expressly in the claim, it would be 'redundant and unnecessary' to incorporate them into

8   the construction of 'location facility.' However, [Plaintiff] has not cited, and we have not

9   discovered, any authority for the proposition that construction of a particular claim term

10 may not incorporate claim language circumscribing the meaning of the term. The claim

11 language makes clear that the location facility in fact does perform the functions in

12 question. The district court correctly incorporated those functions into its claim

13 construction."). Thus, RPost's "redundancy" argument, while persuasive, is not binding

14 on the Court.

15   Regarding GoDaddy's first limitation that dispatch record data must be "recorded

16 by the authenticator during the transmission of the dispatch," the Court finds that such a

17 limitation is not warranted given the claim language. Specifically, the claim requires only

18 that "time related indicia" be recorded by the authenticator during the transmission of the

19 dispatch. *See* '219 Patent col. 2 ll. 63–67 (amended version). The "recorded by the

20 authenticator" limitation does not relate to *all* forms of "dispatch record data," which, as

21 GoDaddy points out, is comprised of *at least* "time related indicia" *and* "an indicia

22 relating to the destination of the dispatch." *See id.* col. 3 ll. 3–5, col. 4 ll. 31–34. In other

23 words, Claims 60 and 82 do not require that "indicia relating to the destination of the

24 dispatch" be recorded by the authenticator. Consequently, the Court rejects this portion of

25 GoDaddy's proposed construction.

26   As to GoDaddy's second and third proposed limitations, the Court concludes that

27 it unnecessary to construe "dispatch record data" as including at least indicia relating to

28 the time and destination of the dispatch. The sentence from which GoDaddy lifts this

1   unambiguous language follows *immediately* behind the term "dispatch record data" in the

2   claims. *See id.* col. 3 ll. 3–5, col. 4 ll. 27–30. It is therefore apparent from the claim

3   language that "dispatch record data" must include both indicia.

4   Regarding GoDaddy's fourth proposed limitation, however, the Court finds that

5   the claim language does not clearly articulate that "dispatch data" and "content data" are

6   distinct types of data. Further, RPost's proposal is vague because it fails to distinguish

7   between (1) data that concerns the event of the dispatch and (2) data that relates to the

8   contents of the dispatch. The jury would be aided by including this portion of GoDaddy's

9   proposal in the construction.

10   For these reasons, the Court construes "dispatch record data" as "information

11   relating to the dispatch but not relating to content data representative of the contents of

12   the dispatch."[21]

13   **D.   "an indicia of time of successful transmission of the dispatch to the recipient" (Term No. 4)**

14

15   **1.   The Parties' Positions**

16   The parties' proposed constructions for the next phrase are again quite similar.

17   RPost urges the Court to adopt Judge Gilstrap's construction of "data that represents the

18   time at which the dispatcher forwarded the dispatch for delivery such that the recipient

19   may later be able to receive the dispatch and where the data is obtained without any

20   cooperation from the recipient." (Doc. 114 at 16–17).

21   GoDaddy responds that while the majority of Judge Gilstrap's construction is

22   correct, two slight modifications should be incorporated: "data that represents the *actual

23   time* at which the dispatcher *completed transmission* of the dispatch for delivery, such

24   that the recipient may later be able to receive the dispatch and where the data is obtained

25   without any cooperation from the recipient." (Doc. 117 at 18–19) (emphasis added).

26   [21] During the *Markman* Hearing, GoDaddy expressed its concern that "information

27   relating to the dispatch" is too broad and could include information that it was cloudy at

28   the time of dispatch. The Court is skeptical that a jury could interpret "information *relating to the* dispatch" in a way that yields information about atmospheric conditions.

1   RPost replies that Judge Gilstrap expressly rejected both of GoDaddy's proposed

2   revisions and asks this Court to do the same. (Doc. 119 at 11).

3   **2.   Analysis**

4   This phrase is disclosed in Claim 60 as follows:

5   **60**. A method of authenticating a dispatch and contents of the
dispatch <u>successfully</u> transmitted from a sender to a recipient, comprising

6   the steps of:

7

. . .

8   providing *an indicia* **[relating to]** <u>*of*</u> *a time of <u>successful</u>*

9   *transmission of the dispatch <u>to the recipient</u>*, said time related indicia being
<u>recorded by an authenticator and</u> provided in a manner resistant to or

10   indicative of tampering by either of the sender and the recipient . . . .

11   '219 Patent, col. 2 ll. 56–67 (amended version) (amendments by Ex Parte Reexamination

12   Certificate are shown with additions underlined and deletions in bolded square brackets;

13   italics added for emphasis).

14   While both of the parties' proposed constructions are substantially based on Judge

15   Gilstrap's construction, GoDaddy proposes two alterations. First, GoDaddy argues that

16   the "indicia" must indicate the "actual time" at which the dispatch was forwarded, not

17   merely the "time." (Doc. 117 at 18–19). Second, GoDaddy asserts that the "indicia" must

18   express when the dispatcher "completed transmission of the dispatch for delivery," rather

19   than when the dispatcher "forwarded the dispatch for delivery." (*Id.*)

20   Judge Gilstrap expressly rejected GoDaddy's proposed construction of "actual

21   time" and so does this Court. *See RMail*, 2013 WL 968246, at *21. The Court agrees with

22   Judge Gilstrap that if "time" were construed as "actual time," such a construction could

23   be read too narrowly by the finder of fact as requiring absolute proof. *Id.*

24   Moreover, the Court agrees with Judge Gilstrap's construction of "forwarded the

25   dispatch for delivery." As Judge Gilstrap explained, the claim language of "successful

26   transmission" is focused on the relevant time at which the "dispatch was released from

27   the control of the non-interested third party." *Id.* GoDaddy proposes that "successful

28   transmission" should be construed as "completed transmission," but offers no compelling

1   reason to justify this revision of Judge Gilstrap's construction. In any event, the Court

2   finds that construing "successful transmission" as "completed transmission" does little to

3   aid the jury's understanding of the term.

4   For these reasons, the Court adopts Judge Gilstrap's construction and construes

5   "an indicia of time of successful transmission of the dispatch to the recipient" to mean

6   "data that represents the time at which the dispatcher forwarded the dispatch for delivery

7   such that the recipient may later be able to receive the dispatch and where the data is

8   obtained without any cooperation from the recipient."

9   **E.   "sender" (Term No. 5) and "recipient" (Term No. 6)**

10   **1.   The Parties' Positions**

11   RPost requests that the Court adopt Judge Gilstrap's conclusion that "sender" and

12 "recipient" are readily understandable terms requiring no construction. (Doc. 114 at 17).

13   GoDaddy responds that the terms should be defined as "the computer that

14 originates the message" and "the computer that receives the dispatch at its intended

15 destination," respectively. (Doc. 117 at 19).

16   In reply, RPost complains that GoDaddy's arguments conflict with the intrinsic

17 record because such constructions would improperly define the terms with the "same

18 meaning as originating processor and recipient processor from the Tomkow Patents"

19 without justification. (Doc. 119 at 11–12).

20   **2.   Analysis**

21   The terms "sender" and "recipient" are found in all asserted claims of the Feldbau

22 Patent. A few examples include:

23   **60**. A method of authenticating a dispatch and contents of the
            dispatch <u>successfully</u> transmitted from a sender to a recipient . . .
24
                . . .
25
                securing by said authenticator, at least part of the authentication data
26   against tampering of the *sender* and the *recipient* . . . .

27   . . . .

28

- 101 -

82. An information dispatch system in an electronic communication network comprising:

a source transmitting system coupled to the electronic communication network for sending a dispatch from a *sender* to a *recipient*;

a destination receiving system coupled to the electronic communication network for receiving the dispatch for the *recipient* . . .

'219 Patent col. 2 ll. 56–col. 4 ll. 12 (amended version) (amendments by Ex Parte Reexamination Certificate are shown with additions underlined; italics added for emphasis).

The Court finds that the terms "sender" and "recipient" have "plain and ordinary meanings." However, "[a] determination that a claim term 'needs no construction' or has a 'plain and ordinary meaning' may be inadequate when a term has more than one 'ordinary' meaning or when reliance on a term's 'ordinary' meaning does not resolve the parties' dispute." *O2 Micro*, 521 F.3d at 1361. GoDaddy correctly posits that "sender" and "recipient" have "ordinary" meanings that include natural persons—a method of transmission not asserted against GoDaddy. (Doc. 117 at 19). For this reason, the Court agrees that construction is necessary because the "plain and ordinary meanings" of these terms "do not resolve the parties' dispute." *See O2 Micro*, 521 F.3d at 1361.

The Court now turns to defining the terms. GoDaddy proffers constructions that define "sender" and "recipient" as "computers." (*Id.*) RPost replies that such constructions would be unduly narrow as the asserted claims do not limit "sender" and "recipient" to only "computers," but allow for other types of computerized devices. (Doc. 119 at 11–12). In this regard, the Court agrees with RPost. The asserted claims are not limited to "computers" *per se* but leave available the use of other forms of computerized devices. *See, e.g.*, '219 Patent col. 4 ll. 4–8 (**82**. An information dispatch system *in an electronic communications network* comprising: a source transmitting system coupled to the electronic communicating network for sending a dispatch from a sender to a recipient . . . . (amended version) (emphasis added)); *id.* col. 2 ll. 56–62 (**60**. A method of authenticating a dispatch and contents of the dispatch successfully

- 102 -

1   transmitted from a sender to a recipient, comprising the steps of: receiving content data

2   representative of the contents of the dispatch originated from the sender and being

3   *electrically transmitted* to said recipient . . . ." (emphasis added)); '219 Patent col. 4 ll. 1–

4   6 ("The present invention encompasses . . . *all types of dispatch methods, such as*

5   *transmission via facsimile machines, modems, computer networks, electronic mail*

6   *systems and so forth . . . .*" (emphasis added)). Thus, the Court rejects GoDaddy's

7   "computer" proposal.

8   Furthermore, the Court is not persuaded that limiting "sender" as *the* computerized

9   device that "originates" the dispatch is appropriate. GoDaddy's proposed construction

10   requires that the "computer" *itself* "originate" the dispatch, possibly leading to the

11   conclusion that the user interfacing with the computer does not create the message. Thus,

12   the Court's construction will clarify that "sender" incorporates some level of user

13   intervention to originate a message.

14   Finally, the Court finds that GoDaddy's proposed limitation "at its intended

15   destination" regarding the "recipient" is vague and requires the jury to engage in

16   unnecessary additional inquiry.

17   For these reasons, the Court construes "sender" as "a combination of (1) the user

18   that caused the computerized device to originate the dispatch and (2) the computerized

19   device itself" and "recipient" as "a combination of (1) the user that the sender intends to

20   receive the message and (2) the computerized device that receives the message."

21   **F.**   **"processor for associating" (Term No. 7)**

22   **1.**   **The Parties' Positions**

23   The parties' next dispute centers on whether "processor for associating" is subject

24   to means-plus-function ("MPF") claim construction pursuant to 35 U.S.C. § 112(6).

25   RPost argues that "processor for associating" need not be construed because the term has

26   a plain and ordinary meaning that the jury will be able to understand and apply.

27   (Doc. 114 at 17–18). RPost additionally contends that because the disputed phrase does

28   not include the term "means," there is a presumption that the patentee did not engage in

1 MPF claiming. (*Id.*) RPost explains that the phrase recites sufficient structure—a

2 processor—that "is a well-known reference in the electrical arts to a microprocessor or

3 microcontroller and connotes structure." (*Id.*) If the Court were to determine that

4 "processor" does require MPF claim construction, RPost asserts that the specification

5 discloses corresponding structures—controller 56 and function executor 102—and

6 algorithms that make the term definite. (*Id.*; Doc. 119 at 12).

7   GoDaddy responds that despite the absence of the word "means" in the claim,

8 "processor for associating" is still subject to MPF claim construction because it "fails to

9 recite sufficiently definite structure or else recites function without reciting sufficient

10 structure for performing that function." (Doc. 117 at 19–20). Pursuant to the two-step

11 approach to MPF claim construction, GoDaddy proposes that the claim's function is

12 "associating the content data with dispatch record data and generating the authentication

13 data." (Doc. 117 at 15). As to corresponding structure, however, GoDaddy argues the

14 claim is indefinite because if fails to disclose adequate corresponding structure for the

15 claimed functions via an algorithm. (*Id.*)

16 ## 2.   Legal Standard for Invoking 35 U.S.C. § 112(6)

17   MPF claim construction is necessary when a patent claim term is drafted in a

18 manner that invokes 35 U.S.C. § 112(6),[22] which states as follows:

19
20   An element in a claim for a combination may be expressed as a *means or step for* performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be
21 construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.
22

23 35 U.S.C. § 112(6) (emphasis added). By enacting this statute, "Congress struck a

24 balance between allowing patentees to express a claim limitation by reciting a function to

25
26   [22] 35 U.S.C. § 112(6) was amended in 2012 to become 35 U.S.C. § 112(f). However, section f is only applicable to patents issued after September 16, 2012. The
27 Feldbau Patent was originally filed in 1997, issued in 2001, and was issued an Ex Parte Reexamination Certificate on June 19, 2012. All asserted claims were modified by the
28 reexamination in 2012.

1   be performed rather than by reciting structure for performing that function, while placing

2   specific constraints on how such a limitation is to be construed." *Williamson v. Citrix*

3   *Online, LCC*, 792 F.3d 1339, 1347 (Fed. Cir. 2015). Namely, scope of coverage of the

4   claimed functions is limited only to the corresponding structure, materials, or acts

5   described in the specification and equivalents thereof. *See Northrop Grumman Corp. v.*

6   *Intel Corp.*, 325 F.3d 1346, 1350 (Fed. Cir. 2004).

7   The Federal Circuit has long held that use of the word "means" within a claim is

8   significant in the analysis of whether a claim limitation should be interpreted in

9   accordance with § 112(6). Specifically, there is a "rebuttable presumption" that § 112(6)

10   applies when the claim language includes the word "means," and a similar "rebuttable

11   presumption" that § 112(6) does not apply when "means" is absent from the claim term.

12   *Williamson*, 792 F.3d at 1347–49.[23] "When a claim term lacks the word 'means,' the

13   presumption can be overcome and § 112, para. 6 will apply if the challenger demonstrates

14   that the claim term fails to 'recite sufficiently definite structure' or else recites 'function

15   without reciting sufficient structure for performing that function.'" *Id.* (quoting *Watts v.*

16   *XL Sys., Inc.*, 232 F.3d 877, 880 (Fed. Cir. 2000)). The standard to determine "definite

17   structure" is "whether the words of the claim are understood by persons of ordinary skill

18   in the art to have sufficiently definite meaning as the name for structure." *Id.* (citing

19   *Greenberg v. Ethicon Endo-Surgery, Inc.*, 91 F.3d 1580, 1583 (Fed. Cir. 1996)).

20   To determine whether the presumption has been rebutted, the Court must consult

21   relevant intrinsic and extrinsic evidence. *See Inventio AG v. ThyssenKrupp Elevator Ams.*

22   *Corp.*, 649 F.3d 1350, 1357 (Fed. Cir. 2011) ("In cases where the claims do not recite the

23   term 'means,' considering intrinsic and extrinsic evidence is usually helpful, as the

24   litigated issue often reduces to whether skilled artisans, after reading the patent, would

25   conclude that a claim limitation is so devoid of structure that the drafter constructively

26

27
     [23] After years of application, *Williamson* expressly overruled the "strong"
28   presumption that § 112(6) only applied to claims that included the term "means."

1   engaged in [MPF] claiming."); *Media Rights Techs., Inc. v. Capital One Fin. Corp.*, 800

2   F.3d 1366, 1372 n.2 (Fed. Cir. 2015) (noting that courts must consider the entire intrinsic

3   record when assessing whether a claim term invokes § 112(6)).

4   ### 3.   § 112(6) Analysis

5   The term "processor for associating" is disclosed in Claim 82 as follows:

6   **82**. An information dispatch system in an electronic communication
     network comprising;

7

          . . .

8
     An authenticator functioning as a non-interested third party with
9   respect to the sender and the recipient for authenticating the dispatch and
     contents of the dispatch transmitted from the source transmitting system to
10   the destination receiving system, including;

11   (1) an input unit coupled to the communication network or to the
     source transmitting system for receiving content data representative of the
12   contents of the dispatch being electronically transmitted to said destination
13   receiving system, and a destination of the dispatch;

14   (2) means for providing an indicia **[relating to]** of a time of
15   successful transmission of the dispatch to the destination receiving system,
     said time related indicia being recorded by the authenticator and provided
16   in a manner resistant to or indicative of tampering by either of the sender
17   and the recipient;

18   (3) a *processor for associating* the content data with dispatch record
     data which includes at least said time related indicia and an indicia relating
19   to the destination of the dispatch, to generate authentication data which
     authenticate[s] the dispatch and the contents of the dispatch; and
20
     (4) means for securing at least part of the authentication data against
21   tampering of the sender and the recipient;

22   wherein the *processor* is combined with the means for securing.

23   '219 Patent col. 4 ll. 4–41 (amended version) (amendments by Ex Parte Reexamination

24   Certificate are shown with additions underlined and deletions in bolded square brackets;

25   italics added for emphasis).

26   To begin, the term "processor for associating" does not include the word "means."

27   Therefore, there is a rebuttable presumption that the term is not subject to § 112(6). The

28   question before the Court is whether that presumption has been overcome. Specifically,

- 106 -

the Court must determine whether the term "processor" (1) fails to "recite sufficiently definite structure" or (2) recites "function without reciting sufficient structure for performing that function." *Williamson*, 792 F.3d at 1349 (citations omitted).

a. Whether "Processor for Associating" Recites Sufficiently Definite Structure

RPost argues that "processor" has a sufficiently definite meaning because the term "is a well-known reference in the electrical arts to a microprocessor or microcontroller and connotes structure." (Doc. 114 at 17–18). GoDaddy's argument concentrates not on the initial inquiry of whether the term itself recites sufficient structure to avert § 112(6), but assumes that § 112(6) applies and explains that computer-related claim limitations "must include the algorithm needed to transform the general purpose computer or processor disclosed in the specification into the special purpose computer programmed to perform the disclosed algorithm—or else be indefinite." (Doc. 117 at 19–20).

In support of its argument, GoDaddy relies on *Aristocrat Techs. Austl. Pty Ltd. v. Int'l Game Tech.*, 521 F.3d 1328 (Fed. Cir. 2008). In *Aristocrat*, however, the disputed claim included the term "control means," which both parties agreed invoked § 112(6). 521 F.3d at 1331. The court applied traditional MPF claim construction principals, requiring the scope of the claim limitation to be defined by the structure disclosed in the specification plus any equivalents of that structure. *See id.* The patent-holder argued the structure corresponding to the recited functions was a standard microprocessor-based gaming machine with appropriate programming. *See id.* The Federal Circuit held,

> In cases involving a computer-implemented invention *in which the inventor has invoked means-plus-function claiming*, this court has consistently required that the structure disclosed in the specification be more than simply a general purpose computer or microprocessor. . . . For a patentee to *claim a means for* performing a particular function and then to disclose only a general purpose computer as the structure designed to perform that function amounts to pure functional claiming.

Id. at 1333 (emphasis added). GoDaddy's argument is based on the reverse legal theory, arguing that if "processor" is an insufficient structure to define the scope of an MPF

1   limitation, it cannot describe sufficient structure when recited directly in a claim

2   limitation itself. *See* (Doc. 117 at 19–20).

3   The Court is not persuaded that *Aristocrat* is applicable or binding in this case.

4   Initially, *Aristocrat* analyzed claim language that expressly used the term "means," and as

5   such, there was a presumption that MPF claim limitations were at issue. In fact, the

6   parties stipulated that the term invoked § 112(6). The *Aristocrat* rule that GoDaddy

7   argues should apply here was therefore derived from a determination as to whether

8   sufficient structure was disclosed in the specification so as to avoid a finding of

9   indefiniteness. GoDaddy is effectively treating as equivalent the standard used to prove

10   sufficient structure to avoid MPF treatment initially, with the standard used to identify

11   corresponding structure in the specification when MPF construction is necessary.

12   GoDaddy does not cite any cases that apply *Aristocrat* in this manner, and other courts

13   have declined to do so. *See eWinWin, Inc. v. Groupon, Inc.*, 2011 WL 6012194, at *14–

14   15 (M.D. Fla. Sept. 5, 2011) (declining to apply *Aristocrat* to find that "computer code"

15   was written as an MPF limitation, and noting that "the law on this issue goes both ways,

16   and the Federal Circuit has not had an opportunity to take a clear stance on facts similar

17   to those in the instant case"); *Markem–Imaje Corp. v. Zipher Ltd.*, 2011 WL 5837087, at

18   *4 n.7 (D.N.H. Nov. 21, 2011) ("The structural disclosure required in the specification

19   when a party chooses to employ [MPF] claiming is not the same structural disclosure

20   required to avoid [MPF] treatment."); *Chamberlain Grp., Inc. v. Lear Corp.*, 756 F. Supp.

21   2d 938, 977 (N.D. Ill. 2010) (noting that *Aristocrat* only applies when § 112(6) has been

22   invoked).

23   For the first inquiry of the *Williamson* analysis, the Federal Circuit only requires—

24   contrary to GoDaddy's argument—that the claim recite some structure to avoid § 112(6)

25   and has repeatedly rejected as "unduly restrictive" the argument that "specific structure"

26   is necessary. *See Lighting World*, 382 F.3d 1354, 1359–60 (Fed. Cir. 2004), *overruled on*

27   *other grounds by Williamson*, 792 F.3d 1339. For example, the Federal Circuit explained:

28

Implicit in [expert witness's] statement is the premise that in order to be regarded as structural for purposes of section 112 ¶ 6, a claim limitation must identify a specific structure and not use a generic term that includes a wide variety of structures. The district court adopted that view explicitly when it held that the claim language "connector assembly being pivotally connected to said pair of adjacent support members" was not structural because "it would cover every conceivable structure that could connect two elements and pivot."

That approach is unduly restrictive. In considering whether a claim term recites sufficient structure to avoid application of section 112 ¶ 6, we have not required the claim term to denote a specific structure. *Instead, we have held that it is sufficient if the claim term is used in common parlance or by persons of skill in the pertinent art to designate structure, even if the term covers a broad class of structures and even if the term identifies the structures by their function.*

Id. (citing *Greenberg v. Ethicon Endo–Surgery, Inc.*, 91 F.3d 1580, 1583 (Fed. Cir. 1996); *Apex Inc. v. Raritan Comput., Inc.*, 325 F.3d 1364, 1372 (Fed. Cir. 2003); *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1369 (Fed. Cir. 2002); *Watts*, 232 F.3d at 880; *Personalized Media Commc'ns, LLC v. Int'l Trade Comm'n*, 161 F.3d 696, 704–05 (Fed. Cir. 1998)) (emphasis added). While the term "processor" may not bring to mind a specific structure, that point is not dispositive for this first inquiry. *See Personalized Media Commc'ns*, 161 F.3d at 704 ("[N]either the fact that a 'detector' is defined in terms of its function, nor the fact that the term 'detector' does not connote a precise physical structure in the minds of those of skill in the art detracts from the definiteness of structure."). What is important is whether "processor" is a term that is understood to describe structure, as opposed to a term that is simply a nonce word not recognized as the name of structure and merely substitutes for "means for." *Id.*

In this case, the Court finds that "processor," albeit a term that might cover a broad class of structures, designates at least some structure. For example, one technical dictionary defines "processor" as "a device that (a) executes instructions, usually automatically and under computer program control, and (b) consists of at least an instruction control unit and an arithmetic unit." Martin H. Weik, *Fiber Optics Standard*

- 109 -

Dictionary 789 (3d ed. 1997); *see also* American Heritage Dictionary of the English Language 1398 (4th ed. 2006) (defining "processor" as "2. *Computer Science* **a.** A computer. **b.** A central processing unit. **c.** A program that translates another program into a form acceptable by the computer being used."); Philip E. Margolis, *Random House Webster's Computer & Internet Dictionary* 448 (3d ed. 1999) (defining "processor" as "Short for microprocessor or CPU"); *Lighting World*, 382 F.3d at 1361 (consulting dictionary definitions to determine whether "connector" has a reasonably well-understood meaning as a name for structure); *Linear Tech.*, 379 F.3d at 1320 (finding that technical dictionary definitions aid determination of whether a claim term is structural). This conclusion is buttressed by the intrinsic record which discloses structural features of the processor. *See* '219 Patent col. 13 ll. 19–27.

The Court agrees with RPost that one of ordinary skill in the art would understand that "processor" encompasses a microprocessor or microcontroller—structural terms. While "processor" "does not connote a precise physical structure in the minds of those of skill in the art[, that does not] detract[] from the definiteness of structure." *Personalized Media Commc'ns*, 161 F.3d at 704 (citing *Greenberg*, 91 F.3d at 1583).

> **b.** **Whether "Processor for Associating" Recites Function without Sufficient Structure for Performing that Function**

Although the Court concludes that the term "processor" connotes at least some structure, this does not end the *Williamson* analysis. The Federal Circuit also allows a challenger to overcome the presumption against application of § 112(6) if the claim recites "function without reciting sufficient structure for performing that function." *Williamson*, 792 F.3d at 1349 (quoting *Watts*, 232 F.3d at 880). Here, Claim 82 provides that the "processor" is "for associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data." '219 Patent col. 4 ll. 31–36 (amended version).

1   Thus, the Court must determine whether "processor" connotes "sufficient structure for

2   performing" the claimed associating and generating functions.

3   The Court first reviews how one skilled in the art would understand "processor" as

4   used in Claim 82. Based on a review of dictionary definitions, the Court concludes that a

5   skilled artisan would not recognize "processor" as a name of a sufficiently definite

6   structure for "associating" two distinct types of data in order to "generate" a third class of

7   data. Rather, one skilled in the art would understand "processor" to mean a general

8   purpose computer, a central processing unit ("CPU"), or a program that translates another

9   program into a form acceptable by the computer being used. *See* American Heritage

10   Dictionary of the English Language 1398.

11   Of course, if the functions performed by the processor are functions typically

12   found in a commercially available off-the-shelf processor, then a skilled artisan might

13   understand the term "processor" to provide sufficient structure for performing those

14   functions. *See In re Katz Interactive Call Processing Patent Litig.* ("*Katz*"), 639 F.3d

15   1303, 1316 (Fed. Cir. 2011) (holding that functions such as "processing," "receiving,"

16   and "storing" that can be achieved by any general purpose computer without special

17   programming do not require disclosure of more structure than the general purpose

18   processor that performs those functions). In this case, however, the Court concludes that

19   "associating" two sets of data in order to "generate" a third set of data is not a typical

20   function found in a general purpose processor and requires additional programming of the

21   processor to implement. Accordingly, the claimed "processor" alone is not sufficient

22   structure to perform the functions in Claim 82.

23   Finally, the term "processor" is different from claim terms "circuit" and

24   "circuitry," which the Federal Circuit has found to denote sufficiently definite structure to

25   avoid application of § 112(6). *See Mass. Inst. of Tech. & Elec. for Imaging, Inc. v.*

26   *Abacus Software ("MIT")*, 462 F.3d 1344, 1354–56 (Fed. Cir. 2006); *Linear Tech.*, 379

27   F.3d at 1320–21; *Apex*, 325 F.3d at 1374. These decisions hold that the term "circuit"

28   coupled with a description in the claims of the circuit's operation generally conveys the

1   structural arrangement of the circuit's components. *See MIT*, 462 F.3d at 1355; *Linear*
2   *Tech.*, 379 F.3d at 1320; *Apex*, 325 F.3d at 1373. In this case, however, the claimed
3   "processor" and other claim language does not convey to a skilled artisan anything about
4   the internal components, structure, or specific operation of the processor.

5   For these reasons, the Court concludes that the term "processor" as used in Claim
6   82 is a term that would not be understood by an ordinarily skilled artisan as having
7   sufficient structure for performing the recited functions of "associating the content data
8   with dispatch record data . . . to generate the authentication data" and therefore invokes
9   the   application   of   §   112(6).   *See   Ex   parte*   Smith,   No.   2012-007631,
10   http://www.uspto.gov/sites/default/files/ip/boards/bpai/decisions/inform/ex_parte_smith_
11   fd2012007631.pdf (P.T.A.B. Mar. 14, 2013) (holding that the claim "a processor . . .
12   programmed to . . . generate an opinion timeline" invoked § 112(6) because the claim
13   recited function without sufficient structure to perform the function).

14   **4.   Legal Standard for MPF Claim Construction**

15   When § 112(6) applies to a claim, the Court follows a two-step construction
16   approach. First, the Court identifies the particular claimed functions using traditional
17   tools of claim construction. *See Med. Instrumentation & Diagnostics Corp. v. Elekta AB*,
18   344 F.3d 1205, 1210 (Fed. Cir. 2003); *Omega Eng'g*, 334 F.3d at 1330. The Court may
19   not adopt functions that are different from those explicitly recited in the claim language.
20   *See Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.*, 296 F.3d 1106, 1113 (Fed. Cir.
21   2002).

22   Second, the Court reviews the specification and identifies the corresponding
23   structure that performs those functions. *See Elekta*, 344 F.3d at 1210. A disclosed
24   structure is "'corresponding' . . . only if the specification or prosecution history clearly
25   links or associates that structure to the function recited in the claim," *id.* (quotation
26   omitted), and only if the structure can perform the claimed function, see *Cardiac*
27   *Pacemakers*, 296 F.3d at 1113. These inquiries are made from the perspective of a person
28   of ordinary skill in the art. *See Cardiac Pacemakers*, 296 F.3d at 1113.

- 112 -

To avoid purely functional claiming in cases involving computer-implemented inventions, the Federal Circuit has "consistently required that the structure disclosed in the specification be more than simply a general purpose computer or microprocessor." *Aristocrat*, 521 F.3d at 1333. "Because general purpose computers can be programmed to perform very different tasks in very different ways, simply disclosing a computer as the structure designated to perform a particular function does not limit the scope of the claim to 'the corresponding structure, material, or acts' that perform the function, as required by section 112 paragraph 6." *Id.* Thus, for a computer or processor-implemented claim limitation interpreted under § 112(6), the corresponding structure must disclose the algorithm needed to transform the disclosed general purpose computer or processor into the special purpose computer. *Id.* Failure to disclose the corresponding algorithm for a computer-implemented MPF term renders the claim indefinite. *Id.* at 1337–38.

An algorithm is a "sequence of computational steps to follow." *Ibormeith IP, LLC v. Mercedes-Benz USA, LLC*, 732 F.3d 1376, 1379 (Fed. Cir. 2013) (citations omitted). "For a claim to be definite, a recited algorithm . . . need not be so particularized as to eliminate the need for any implementation choices by a skilled artisan; but it must be sufficiently defined to render the bounds of the claim—declared by section 112(6) to cover the particular structure and its equivalents—understandable by the implementer." *Id.* (citing *AllVoice Computing PLC v. Nuance Commc'ns, Inc.*, 504 F.3d 1236, 1245–46 (Fed. Cir. 2007)). An algorithm may be expressed as a mathematical formula, in prose, as a flow chart, or in any other manner that provides sufficient structure. *Noah Sys., Inc. v. Intuit Inc.*, 675 F.3d 1302, 1312 (Fed. Cir. 2012) (citing *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1340 (Fed. Cir. 2008)). Nonetheless, the purported algorithm cannot "merely provide[] functional language" and must provide a "step-by-step procedure" for accomplishing the claimed function. *Ergo Licensing*, 673 F.3d at 1365. Further, "[i]t is well settled that simply disclosing software, however, without providing some detail about the means to accomplish the function, is not enough." *Function Media, L.L.C. v. Google, Inc.*, 708 F.3d 1310, 1318 (Fed. Cir. 2013) (quotations omitted).

1   Finally, in a means-plus-function claim "in which the disclosed structure is a

2   computer, or microprocessor, programmed to carry out an algorithm, the disclosed

3   structure is not the general purpose computer, but rather the special purpose computer

4   programmed to perform the disclosed algorithm." *WMS Gaming*, 184 F.3d at 1349. Thus,

5   "the corresponding structure for a § 112 ¶ 6 claim for a computer-implemented function

6   is the algorithm disclosed in the specification." *Harris Corp. v. Ericsson Inc.*, 417 F.3d

7   1241, 1249 (Fed Cir. 2005).

8   **5.   MPF Claim Construction**

9   **a.   Function**

10   The Court finds that GoDaddy's functionality proposal is supported by the claim

11 language and accurately recites the function of the processor. *See* '219 Patent col. 4 ll.

12 31–36 (amended version). Thus, the Court construes the claim's function as "associating

13 the content data with dispatch record data and generating the authentication data."

14   **b.   Corresponding Structure**

15   In its Opening Brief, RPost argues that the specification discloses two

16 corresponding structures: "controller 56" and "function executor 102, which may be a

17 Microchip Technology Inc.'s PIC16C5x series EPROM-based micro-controller."

18 (Doc. 114 at 18). GoDaddy responds that the specification does not disclose a

19 corresponding structure because no algorithm is provided that transforms the general

20 purpose processor into a special purpose processor that can perform the claimed

21 functions. (Doc. 117 at 19–20). Thus, GoDaddy contends that the claim is indefinite. (*Id.*)

22   RPost replies that the specification "discloses numerous mathematical formulas

23 that may be used by function generator 102 to perform the claimed 'associating.'"

24 (Doc. 119 at 12 (citing '219 Patent col. 10 ll. 13–col. 13 ll. 7)).

25   Initially, the Court concludes that an algorithm must be disclosed in the

26 specification. The processor's claimed functions are to "associate" data to "generate"

27 authentication data. '219 Patent col. 4 ll. 31–36 (amended version). As discussed above,

28 these functions cannot be performed solely by a general purpose computer or processor,

1   but require a special purpose computer. *See EON Corp. IP Holdings LLC v. AT&T*

2   *Mobility LLC*, 785 F.3d 616, 623 (Fed. Cir. 2015) ("A microprocessor or general purpose

3   computer lends sufficient structure only to basic functions of a microprocessor. All other

4   computer-implemented functions require disclosure of an algorithm."). Accordingly, the

5   algorithm that transforms the general purpose processor into a special purpose processor

6   that performs the claimed function is required. *See Aristocrat*, 521 F.3d at 1333.

7   The relevant portions of the specification disclose:

8   The controller **56** associates the information **60** and the dispatch
9   information, by storing them in storage unit **54** and by associating link
             information with the stored authentication-information, for example, in the
10   form of a unique dispatch identifier such as a sequential dispatch number.

11   '219 Patent col. 7 ll. 59–64.

12   An efficient method for associating a plurality of information
             elements is by associating a digital representation thereof using a method
13   referred to herein as "*mathematical association*". A digital representation of
             an information element can be considered as a number, for example as the
14   element's standard binary, hexadecimal or other base representation. Using
15   mathematical association, rather than maintaining the information elements
             (numbers) themselves, it is sufficient to maintain the results (also numbers)
16   of one or more functions which are applied to one or more of these
17   information elements. (These results are sometimes referred to as
             "message-digests", "hash-values" or "digital-signatures"). *More formally, if*
18   *A is a set of information elements, and F is the mathematical association*
             function, then the set B of information elements is obtained as the result of
19   *applying the function F to the set A of information elements, i.e. B=F(A).*
20
                   Preferably, the function F is selected such that a fraudulent attempt
21   to change the elements of the set A, or an attempt to claim that a set A'
             which comprises different elements is the original set, can be readily
22   detected by comparing the result B' obtained by applying the function F to
23   the set A', to the original result B, i.e., by checking if F(A')=F(A).

24   It would be advantageous to select the function according to a
             cryptographic schemes. Encryption and digital envelope functions can
25   provide for secure data interchange. Digital signatures can provide for
26   accurate and reliable verification of both the signature generator and the
             data. One-way hash functions provides for security, and can reduce the size
27   of the generated signatures while still enable verification of the original

28

- 115 -

data used to generate these signatures. Utilizing combinations of cryptographic schemes can optimize particular implementations.

Various function classes of various degrees of complexity can be used for mathematical association purposes in accordance with various embodiments of the present invention. Furthermore, the function F and/or the result B can be kept secret and unknown in general, and to interested parties such as the sender or the recipient in particular. However, even if the function F and/or the result B are known, the task of finding a meaningful different set A' such that $B=F(A')$ is mostly very difficult even for relatively simple functions, not to mention for more complex ones.

A special class of functions most suitable for the purposes of the present invention is the class of functions having the property that given the result $B=F(A)$, it is exceptionally difficult to find a second set A' such that applying the function F to the second set A' will yield the same result B. The term "exceptionally difficult" refers herein to the fact that although many different such sets A' may exist, it is so difficult to find even one of them (sometimes even to find the set A itself) that it is practically infeasible. In fact, the functions of this class "hide" the elements they are applied to, (and sometimes the elements even cannot be reconstructed) and therefore this class is referred to herein as "the Hiding Class".

. . . .

Few well known and widely used functions of the Hiding class are encryption functions (e.g., the RSA [1.06] or the DES [1.01] algorithms) and Cyclic-Redundancy-Check [3] (C.R.C.) functions (e.g., the C.R.C-32 function). While C.R.C functions are generally used in applications requiring verification as to the integrity of an arbitrarily long block of data, encryption is used to maintain the original data elements, though in different, cryptic representation. Encryption functions convert the information elements into one or more cryptic data blocks using one key, while enabling their reconstruction by providing a matching (same or different) key. Other well known members of this class of functions in the prior art are compression functions (e.g., the Lempel-Ziv 1977 [5] and 1978 algorithms), one-way hash functions [1.03] (e.g., the MD4 [4], and MD5 [1.04] algorithms), and MACs [1.13].

Since for authentication purposes there is no need to maintain the original information elements, the use of encryption functions (which normally maintain the information though in a cryptic representation) may be inefficient. One-way hash functions (and other functions of the Hiding Class), on the other hand, maintain a small sized result value, but the information elements from which the result has been produced are secured,

- 116 -

i.e., cannot be reconstructed therefrom. It would be more advantageous, for example, to apply a one-way hash function to the union of all the information elements, i.e., to a bit-string, where the leftmost bit is the leftmost bit of the first element, and the rightmost bit is the rightmost bit of the last element. This produces a cryptic and secure result, as described hereinabove. Furthermore, one-way hash functions can be computed relatively quickly and easily.

Generally and more formally, the result B is a set of one or more information elements b1, . . . , bm, where each element bi (which itself can comprise one or more information elements) is the result of applying a (possibly different) function Fi to a subset Si of a set A which comprises one or more information elements a1, . . . , an, where the various subsets Si are not necessarily disjoint or different, each subset Si includes at least a portion of one or more (or even all) of the electronic information elements of the set A, and where each function Fi can comprise one or more functions (i.e., Fi can be the composition of functions). Preferably, the functions Fi are members of the Hiding Class. The elements of such a subset Si are considered to be mathematically associated.

Assuming that the set A comprises five information elements a1, a2, a3, a4, a5, a few examples of mathematical association function Fi and their result set B follow: (the UNION function is denoted as U(x1, . . . , xk), Which is an information element comprising a bit-string, where the left most bit is the leftmost bit of the element x1, and the rightmost bit is the rightmost bit of the element xk.)

(a) single element result set B

$b1=F1(S1)=F1(a1,a4,a5)=a1/(a4+a5+1)$

$b1=F1(S1)=F1(a1,a3,a4)=ENCRYPT(U(a1,a3,a4))$

$b1=F1(S1)=F1(a1,a2,a3,a4,a5)=MD5(U(a1,a2,a3,a4,a5))*$
$C.R.C.(a3)mod5933333$

$b1=F1(S1)=F1(a1,a2,a3,a4,a5)=C.R.C.(ENCRYPT(U(a1,a2)),$
$COMPRESS(U(a2,a3,a4)),a1,a5)$

$b1=F1(S1)=F1(a1,a2,a3,a4,a5)=U(a1,a2,a3,a4,a5)mod p$ (where
p is a large Prime number)

$b1=F1(S1)=F1(a1,a2,a3,a4,a5)=ENCRYPT(MD5(U(a1,a2,$
$a3,a4,a5)))$

(b) multi-element result set B

$B=[C.R.C.(U(a1,a3)),a2/(a1+1),ENCRYPT(a5)]$

$$b1=F1(S1)=F1(a1,a3)=C.R.C.(a1,a3)$$

$$b2=F2(S2)=F2(a1,a2)=a2/(a1+1)$$

$$b3=F3(S3)=F3(a5)=\text{ENCRYPT}(a5)$$

The elements of two or more (not necessarily disjoint) subsets of set A can be associated with each other by associating the elements of the result set B which correspond to these subsets, either mathematically, or by non-mathematical methods, as described hereinabove. Furthermore, if there is a subset of elements of set A to which no function has been applied, these elements may be associated with the elements of the result set B, again either mathematically or by non-mathematical methods.

Moreover, the elements of two or more subsets of the set A can be associated with each other by associating the elements of each of these subsets with a common subset comprising one or more elements of the set A, where this common subset uniquely relates to the specific dispatch. This type of association is referred to herein as "indirect association", and the elements of this common subset are referred to herein as "link elements". A link element can be for example a unique dispatch number, or the subset comprising the time indication and a machine serial number, etc.

For example, assuming that the element a2 of the above set A uniquely relates to the dispatch, the following function generates a multi-element result set B:

$$B=[b1,b2,b3]=[\text{ENCRYPT}(a1,a2),\ \text{COMPRESS}(a2,a3,a4),\ a2+a5]$$

where the subsets Si include the following elements: S1=[a1,a2], S2=[a2,a3,a4] and S3=[a2,a5]. The elements of each subset are mathematically associated. Since all of these subsets include the common link-element a2, all their elements (in this case all the elements of the set A) are associated with each other.

Id. col. 10 ll. 13–col. 13 ll. 7 (brackets in original; italics added for emphasis).

Reference is now made to FIG. **4** which is a block diagram that illustrates an authenticator **100**, constructed and operative in accordance with a preferred embodiment of the present invention. The authenticator **100** comprises a secure time generator **104**, a storage device **106** and a function executor **102** which has means for inputting the following information elements: the transmitted information, the destination address, a time indication generated by the secure time generator **104**, and a dispatch completion indication. Optionally, additional information elements can be provided as well.

- 118 -

1
2
3
4
5
6

*The function executor **102** can be for example a Microchip Technology Inc.'s PIC16C5x series EPROM-based micro-controller, and the input means can be for example an I/O port, a serial, parallel or disk interface. The function executor **102** is capable of executing a function F on at least one, and preferably on the union of all of the input elements, and of generating a result information element which is provided to a storage device **106**, and optionally to an output device **108**, such as a printing device.*

7
8
9
10
11
12
13

Preferably, the function F is a member of the Hiding Class, and is kept unknown at least to any interested party, by the function executor **102**. This can be achieved for example by enabling the code protection feature of the PIC16C5x series microcontroller. Alternatively, a MAC [1.13] such as a one-way hash function MAC can be used where secret codes, keys and data relating to the function can be for example stored in a shielded memory device which is automatically erased if the authenticator **100** is tampered with. Also, preferably the storage device **106** is a WORM device, such as a PROM. Preferably, a different function is used for each device employing the function F. This can be achieved for example by using different keys or codes with each function.

14 *Id.* col. 13 ll. 8–41 (brackets in original; italics added for emphasis). RPost argues that the

15 specification discloses two embodiments that perform the claimed functions:

16 (1) controller 56 and (2) function executor 102, which may be a Microchip Technology

17 Inc.'s PIC16C5x series EPROM-based micro-controller. (Doc. 114 at 17–18).

18 Regarding controller 56, the Court concludes that the specification does not

19 disclose a sufficient algorithm for this embodiment. While an algorithm to perform the

20 claimed function of "associating" has likely been disclosed for this embodiment, no

21 algorithm has been disclosed for the second function of "generating." *See* '219 Patent col.

22 7 ll. 59–64. Specifically, the portion of the specification discussing controller 56 only

23 speaks to "associating" data, but never discusses how controller 56 is to "generate" data.

24 Nor does the specification relate controller 56 to the algorithms that function

25 executor 102 has the capacity to perform. Because the algorithm must disclose how

26 controller 56 performs *all* claimed functions, this embodiment does not disclose sufficient

27 corresponding structure. *See Media Rights*, 800 F.3d at 1374 ("Where there are multiple

28

1 claimed functions . . . the patentee must disclose adequate corresponding structure to
2 perform all of the claimed functions." (citing *Noah*, 675 F.3d at 1318–19)).

3 As to function executor 102, however, the Court finds that the two methods of
4 associating and generating data disclosed in the specification—"mathematical
5 association" and "indirect association"—adequately set forth mathematical algorithms
6 that perform the claim's functions of "associating" and "generating." *See Noah*, 675 F.3d
7 at 1312 ("The specification can express the algorithm 'in any understandable terms
8 including as a mathematical formula, in prose, or as a flow chart, or in any other manner
9 that provides sufficient structure.'" (quoting *Finisar*, 523 F.3d at 1340)). Although the
10 specification describes the associating and generating processes in lengthy detail, the
11 algorithm for performing the two functions can be boiled down to the following section
12 of the specification:

13
14 > More formally, if A is a set of information elements, and F is the
     > mathematical association function, then the set B of information elements is
     > obtained as the result of applying the function F to the set A of information
15   > elements, i.e. B=F(A).

16 '219 Patent col. 10 ll. 25–29.

17 Specifically to Claim 82, the processor "associates" the content data with dispatch
18 record data (set A) by applying mathematical association function (F) to "generate"
19 authentication data (set B). The same foundational equation (i.e., B=F(A)) is used by both
20 "mathematical association" and "indirect association," and both methods expound on the
21 algorithm *See id.* col. 10 ll. 13–29; *id.* col. 12 ll. 55–col. 13 ll. 7. The specification also
22 discloses various association functions, such as encryption and C.R.C. functions, which
23 need not be recited in full here. Rather, for purposes of providing a "step-by-step
24 procedure" that a skilled artisan would understand constitutes sufficient structure to
25 perform the claimed functions, the recited mathematical algorithm satisfies that
26 requirement. *See EON Corp. IP Holdings*, 785 F.3d at 624 (citing *Noah*, 675 F.3d at
27 1313); *Ibormeith*, 732 F.3d at 1379 ("For a claim to be definite, a recited algorithm . . .
28 need not be so particularized as to eliminate the need for any implementation choices by

1 a skilled artisan; but it must be sufficiently defined to render the bounds of the claim—

2 declared by section 112(6) to cover the particular structure and its equivalents—

3 understandable by the implementer." (citation omitted)).[24]

4   Consequently, the Court rejects GoDaddy's argument that the claim is indefinite

5 for lack of corresponding structure, see *Cardiac Pacemakers*, 296 F.3d at 1113–14 (Fed.

6 Cir. 2002) ("Alternative embodiments may disclose different corresponding structure,

7 and the claim is valid even if only one embodiment discloses corresponding structure."

8 (citation omitted)), and construes the corresponding structure for this claim term as "a

9 function executor 102, which may be a Microchip Technology Inc.'s PIC16C5x series

10 EPROM-based micro-controller, that associates a set of information elements ("A") by

11 applying an association function ("F") to generate another set of information elements

12 ("B"), i.e., B=F(A); and its equivalents." *See Ericsson*, 417 F.3d at 1249 ("[T]he

13 corresponding structure for a § 112 ¶ 6 claim for a computer-implemented function is the

14 algorithm disclosed in the specification.").

15   **6.**   **Conclusion**

16   For the reasons set forth above, the Court finds that "processor for associating" is

17 subject to § 112(6) thereby compelling MPF claim construction. The Court construes the

18 claim's function to be: "associating the content data with dispatch record data and

19 generating the authentication data." As to structure, the Court construes the claim's

20 corresponding structure as: "a function executor 102, which may be a Microchip

21 Technology Inc.'s PIC16C5x series EPROM-based micro-controller, that associates a set

22 of information elements ("A") by applying an association function ("F") to generate

23 another set of information elements ("B"), i.e., B=F(A); and its equivalents."

24

25

26
27
28
    [24] GoDaddy argued during the *Markman* Hearing that the equation B=F(A) is merely a generic math function taught in first year calculus. That argument—whether true or not—is inconsequential. The Federal Circuit only requires the inventor to disclose an algorithm that can perform the claimed functions. The algorithm as set forth in the Feldbau Patent's specification satisfies that requirement.

G. **"means for providing an indicia of a time of successful transmission of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient" (Term No. 8)**

1. The Parties' Positions

The parties agree that this phrase is subject to MPF claim construction pursuant to § 112(6) and stipulate as to the claim's functionality but dispute the corresponding structure. Namely, RPost asks the Court to adopt the corresponding structure as found by Judge Gilstrap: "(1) internal clock 50 (2) communications network server (3) Secure time generator 104 (4) Digital Notary System (DNS); and their equivalents." (Doc. 114 at 18).

GoDaddy contends the corresponding structure should be "a secure clock internal to the authenticator or a time stamping service such as the Digital Notary System (DNS) external to the authenticator that is secured from being set or modified by an interested party such as the sender." (Doc. 117 at 20). GoDaddy explains that "it agrees with RPost's construction with one exception: the time generator must be secured from being set or modified by an interested party such as the sender." (*Id.*) GoDaddy argues this limitation is "expressly recited" in the specification as part of the structure for providing the time source indicia. (*Id.*)

RPost replies that GoDaddy's construction excludes two express corresponding structures from the specification: communications network server and secure time generator 104. (Doc. 119 at 12). RPost further argues that GoDaddy's proposal limiting the time generator as "secured from being set or modified by an interested party such as the sender" is flawed because that limitation is "only mentioned in the specification describing the communication network server, not the other three structures." (*Id.*)

2. Legal Standard

Because this claim is subject to § 112(6), the Court will apply the two step approach for MPF claim construction as set forth in Term No. 7.

- 122 -

3. Analysis

This disputed phrase is found in Claim 82 as follows:

> **82**. An information dispatch system in an electronic communication network comprising;
>
> . . .
>
> an authenticator functioning as a non-interested third party with respect to the sender and the recipient for authenticating the dispatch and contents of the dispatch transmitted from the source transmitting system to the destination receiving system, including;
>
> . . .
>
> (2) *means for providing an indicia* **[relating to]** *of a time of successful transmission* of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient . . . .

'219 Patent col. 4 ll. 4–30 (amended version) (amendments by Ex Parte Reexamination Certificate are shown with additions underlined and deletions in bolded square brackets; italics added for emphasis).

a. Function

Because the parties do not dispute the functionality of this claim, the Court adopts the stipulated construction of "providing an indicia of a time of successful transmission of the dispatch to the destination receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient."

b. Corresponding Structure

The Court has identified the following passages from the specification as disclosing corresponding structure for the claimed function:

> The authenticator **70** also *comprises* . . . an *internal clock **50*** for generating a time indication **66** . . . .

'219 Patent col. 6 ll. 66–col. 7 ll. 3 (emphasis added).

> The *internal clock **50*** provides an indication **66** of the current time, and is utilized to provide a time indication for the transmission. *Internal*

- 123 -

clock 50 is securable (to ensure the veracity of the produced time indication **66**), and preferably provides time indications according to a non-changing time standard, such as Greenwich–Mean–Time (G.M.T.) or UTC. Alternatively, *the time indication 66 can be externally obtained, for example from a communication network server, as long as the source is secured from being set or modified by an interested party such as the sender.* The security of the time indication can be provided in a number of ways, such as by factory pre-setting the *clock 50* and disabling or password securing the Set Date/Time function of the *internal clock 50*. Alternatively, the *clock 50* can maintain a "true offset" with the true preset date/time, that reflects the offset of the user set date/time from the genuine preset one.

Id. col. 7 ll. 12–28 (emphasis added).

Reference is now made to FIG. **4** which is a block diagram that illustrates an authenticator **100**, constructed and operative in accordance with a preferred embodiment of the present invention. The authenticator **100** *comprises* a *secure time generator 104*, a storage device **106** and a function executor **102** which has means for inputting the following information elements: the transmitted information, the destination address, *a time indication generated by the secure time generator 104*, and a dispatch completion indication. Optionally, additional information elements can be provided as well.

Id. col. 13 ll. 8–18 (emphasis added).

A related embodiment can utilize a *Time Stamping Service (TSS) such as the Digital Notary System (DNS)* provided by Surety Technologies Inc. [1.10], which has been proposed by Haber et al. in their U.S. patent documents [2]. The certificate **740** or any portion thereof (such as the signature **742**) can be sent to the DNS to be time stamped. Alternatively, an embodiment of the present invention could internally implement the DNS scheme. The DNS generates a certificate authenticating the certificate **740**. Utilizing such time stamping schemes is of great advantage, since the DNS generated certificates are virtually unforgeable, and there is no need to deposit copies of the certificates with trustees. Since in this case the DNS time stamps the certificate **740** anyway, the service **750** itself optionally need not add the time indication **720**.

Id. col. 16 ll. 60–col. 17 ll. 7 (brackets in original; italics added for emphasis).

As found by Judge Gilstrap, the specification discloses the following corresponding structures: internal clock 50, a communication network server, secure time

generator 104, and a Time Stamping Service such as the Digital Notary System. GoDaddy does not dispute that an internal clock and a time stamping device should be incorporated in the corresponding structure, and states that it "agrees with RPost's construction with one exception: the time generator must be secured from being set or modified by an interested party such as the sender." (Doc. 117 at 20). GoDaddy's proposed construction, however, appears to exclude both "communications network server" and "secure time generator 104." *See* (*id.*) Based on the express language of the specifications, these two methods of producing an "indicia" of time are preferred embodiments, and the Court agrees with Judge Gilstrap that all of "[t]hese structures should be included in the Court's construction as alternatives." *RMail*, 2013 WL 968246, at *30 (citing *Ishida Co., Ltd. v. Taylor*, 221 F.3d 1310, 1316 (Fed. Cir. 2000)).

On the other hand, the Court concludes that RPost's proposed construction is deficient in four areas. First, the specification expressly discloses that clock 50 "is *securable* (to ensure the veracity of the produced time indication 66)." '219 Patent col. 7 ll. 14 (emphasis added). The specification also discloses how clock 50 is securable:

> The security of the time indication can be provided in a number of ways, such as by factory pre-setting the clock 50 and disabling or password securing the Set Date/Time function of the internal clock 50. Alternatively, the clock 50 can maintain a "true offset" with the true preset date/time, that reflects the offset of the user set date/time from the genuine preset one.

Id. col. 7 ll. 21–28. Implicit in RPost's argument that "communications network server" is the only structure with a "secured" limitation is that the express "securable" limitation does not apply to clock 50. *See* (Doc. 114 at 18). While the inventor did not use the term "secured" to limit clock 50—which he readily could have done—the specification does disclose that clock 50 is at least "secur*able*." By doing so, the inventor chose to limit the nature of clock 50 as *able to be* secured. Accordingly, the Court's construction includes "securable" as a limitation for clock 50.

Second, as expressly set forth in the specification, "communications network server" is limited as "secured from being set or modified by an interested party such as

- 125 -

the sender." '219 Patent col. 7 ll. 18–21. RPost does not dispute this limitation applies and notes that it is "amenable to a construction that adds this limitation to the communication network server." (Doc. 119 at 12–13). Accordingly, the Court incorporates this limitation in its construction.

Third, the Court finds that the jury would be better served by defining the four corresponding structures by their location in relation to the authenticator, i.e., internal or external. As GoDaddy argues here and as RPost argued before Judge Gilstrap, the location of the time generator with respect to the authenticator is determinative of whether the generator must be "secured from being set by an interested party such as the sender."[25] Based on the specification language and the preferred embodiments, the Court finds that two corresponding structures are internal to the authenticator and two are external. Specifically, clock 50 and time generator 104 are internal to the authenticator, see '219 Patent col. 6 ll. 66–col. 7 ll. 3, Fig. 2, col. 13 ll. 11–12, Fig. 4, while the Time Stamping Service and communication network server are both external to the authenticator, see *id.* col. 7 ll. 17–21, col. 16 ll. 60–col. 17 ll. 7. As a result, the specification mandates that the Time Stamping Service and communication network server be "secured from being set or modified by an interested party such as the sender" as they are both "external" structures. *Id.* col. 7 ll. 18–21.

Finally, the specification discloses that time generator 104 is "secure." The Court finds that the jury would be aided by a construction that defines "secure." The specification defines a "secure" external time generating structure as one that is "secured

---

[25] In the case before Judge Gilstrap, RPost proposed a similar corresponding structure as the one now adopted by the Court. Specifically, RPost proposed "the corresponding structures disclosed in the specification are an internal clock 50 located within the authenticator *or an externally obtained time source that is secured from being set by an interested party such as the sender*." *RMail*, 2013 WL 968246, at *27 (emphasis added). Thus, RPost recognizes that if the time source is obtained from an external structure, the specification requires that the external structure must be secured from being set by an interested party. Although RPost did not propose a similar construction here, the Court incorporates this express limitation in its construction.

1   from being set or modified by an interested party such as the sender." *Id.* Because the

2   specification discloses that time generator 104 is "secure," the Court finds that the

3   "secure" limitation applicable to "external" structures equally applies to time generator

4   104.

5   For these reasons, the Court concludes that the corresponding structure for "means

6   for providing an indicia of a time of successful transmission" is "either a (1) securable

7   clock 50 and equivalents thereof; (2) time generator 104 and equivalents thereof;

8   (3) communications network server and equivalents thereof; or (4) Time Stamping

9   Service, such as the Digital Notary System, and equivalents thereof; where structures

10   (1) and (2) are internal to the authenticator, structures (3) and (4) are external to the

11   authenticator, and structures (2), (3) and (4) are secured from being set or modified by an

12   interested party such as the sender."

13   **H.   "means for securing at least part of the authentication data against
          tampering of the sender and the recipient; wherein the processor is
14   combined with the means for securing" (Term No. 9)**

15   **1.   The Parties' Positions**

16   Like Term No. 8, the parties agree that this claim is subject to MPF construction,

17   stipulate as to the claim's functionality, but dispute the corresponding structure. As to

18   structure, RPost contends that the Court should adopt Judge Gilstrap's construction of

19   "storage unit 54 or storage device 106, and their equivalents." (Doc. 114 at 18–19).

20   GoDaddy responds that the corresponding structure should be "using a

21   compression, private or public key encryption or scrambling technique, a password, or a

22   combination thereof, such as those employed by the widely used RSA encryption

23   method, and by the PKZIIP(tm) program from PKWARE Inc., Glendale, Wis., U.S.A.,

24   and where the 'securing' procedure, key or password are unknown to any interested

25   party." (Doc. 117 at 20–21). During the *Markman* Hearing, GoDaddy argued that RPost's

26   proposal should be rejected because "storage unit 54" and "storage device 106" are nonce

27   terms that disclose no structure. GoDaddy also asserted that an algorithm is necessary for

28

1   a processor to perform the claimed function and that its proposed structure is the only

2   algorithm disclosed in the specification.

3   RPost replies that GoDaddy's proposed structure is merely an alternative to

4   storage unit 54 in the claim specification and not the only structure providing a means for

5   securing the information. (Doc. 119 at 13). By excluding storage unit 54 and storage

6   device 106 from the corresponding structure, RPost contends that GoDaddy's proposal

7   should be rejected for conflicting with the intrinsic record. (*Id.*)

8   **2.   Legal Standard**

9   Because this claim is subject to § 112(6), the Court will apply the two step

10   approach for MPF claim construction as set forth in Term No. 7.

11   **3.   Analysis**

12   This disputed phrase is found in Claim 82 as follows:

13   **82**. An information dispatch system in an electronic communication
     network comprising;
14

15   . . .

16   an authenticator functioning as a non-interested third party with
     respect to the sender and the recipient for authenticating the dispatch and
17   contents of the dispatch transmitted from the source transmitting system to
     the destination receiving system, including;
18
           . . .
19
           (3) a processor for associating the content data with dispatch record
20   data which includes at least said time related indicia and an indicia relating
     to the destination of the dispatch, to generate authentication data which
21   authenticate[s] the dispatch and the contents of the dispatch.

22   (4) *means for securing at least part of the authentication data
     against tampering of the sender and the recipient*;
23
           wherein the processor is combined with the means for securing.
24

25

26

27

28

'219 Patent col. 4 ll. 4–41 (amended version) (emphasis added)

a. Function

Because the parties do not dispute the functionality of this claim, the Court adopts the stipulated construction of "securing at least part of the authentication data against tampering by either the sender or the recipient."

b. Corresponding Structure

The parties have identified the following passages from the specification as disclosing corresponding structure:

> The authenticator **70** also comprises an optional *storage unit 54* such as a tape, disk or memory device and so forth for storing the information **60** and related dispatch information . . . .

'219 Patent col. 6 ll. 66–col. 7 ll. 2 (emphasis added).

> The *storage unit 54* is used for storing the information **60** and/or the dispatch information, including the address **62**, the time indication **66**, and optionally the transmission completion indication **64**. Typically, the *storage unit 54* is relatively secure, such that the authentication-information contained therein is assumed unchangeable. For example it may be a Write–Once–Read–Many (WORM) device such as an optical disk or a Programmable Read–Only Memory (PROM) device, it may be enclosed within a securable device, or it may be provided with read-only access privilege. Alternatively, the authentication-information is stored in a secure manner, for example using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof, such as those employed by the widely used RSA encryption method, and by the PKZIP(tm) program from PKWARE Inc., Glendale Wis., U.S.A., and where the "securing" procedure, key or password are unknown to any interested party.
>
> The controller **56** associates the information **60** and the dispatch information, by storing them in *storage unit 54* and by associating link information with the stored authentication-information . . . .
>
> To provide the authentication-information for the transmission, the dispatch identifier is provided to the controller **56** through the user interface **48**. The controller **56**, in turn, retrieves the various stored authentication-information elements from *storage unit 54*. If the stored information is also secured (i.e., by compression, password, etc.), the controller **56** "unsecures" them, and then provides them to the output unit **58**.

- 129 -

Id. col. 7 ll. 41–col. 8 ll. 5 (emphasis added).

Similarly, information transmitted in a computer network or electronic mail system can be authenticated, for example, by having a file server or mail manager (whose time generator is considered secure) store the transmitted information together with its associated dispatch information in a secure manner. One embodiment of secure storage is that which has *read-only privileges*. Alternatively, such read-only effect can also be obtained by having the authentication-information encrypted with the authenticator's private key: everybody can decrypt it using the authenticator's public key, but no interested party can change it without such action being detectable.

Id. col. 9 ll. 56–67 (emphasis added).

Reference is now made to FIG. 4 which is a block diagram that illustrates an authenticator **100**, constructed and operative in accordance with a preferred embodiment of the present invention. The authenticator 100 comprises a secure time generator **104**, *a storage device 106*, and a function executor **102** . . . .

. . . .

. . . . Also, preferably the *storage device 106* is a WORM device, such as a PROM. Preferably, a different function is used for each device employing the function F. This can be achieved for example by using different keys or codes with each function.

Id. col. 13 ll. 8–41 (emphasis added).

Judge Gilstrap construed the corresponding structure of the claimed function as "storage unit 54 or storage device 106, and equivalents thereof." *RMail*, 2013 WL 968246, at *35. During the *Markman* Hearing, GoDaddy argued that the specification is required to disclose an algorithm because the claimed function of "securing" cannot be performed by a general purpose computer, but requires a special purpose computer. Although Judge Gilstrap did not analyze whether the Feldbau Patent needed to disclose an algorithm to perform the claimed function, the Court finds that such an analysis is necessary because the claims asserted against GoDaddy involve computer-implemented functions. *See Aristocrat*, 521 F.3d at 1333.

i.   Applicability of *Aristocrat*

In this case, there is no dispute that the claimed function of "securing" is disclosed as part of a computer-implemented invention. The question before the Court, therefore, is whether "securing" can be performed by a general purpose computer.

As set forth in the Court's analysis for Term No. 7, *Aristocrat* requires that for computer or processor-implemented claim terms interpreted under § 112(6), the corresponding structure must disclose the algorithm needed to transform the general purpose computer or processor into the special purpose computer. 521 F.3d at 1333. The *Aristocrat* requirement is limited, however, to cases where an inventor has claimed "a specific function performed by a special purpose computer." *Katz*, 639 F.3d at 1316. Where the inventor has merely recited general computer functions such as "processing," "receiving," or "storing," he need not "disclose more structure than the general purpose processor that performs those functions." *Id.*

As employed by the Feldbau Patent, RPost's proposed corresponding structures of "storage device 54" and "storage unit 106" do not—despite their labels—merely perform the general computer function of "storing." Rather, the claim language requires that the devices "secure" data from tampering by interested parties. *See* '219 Patent col. 4 ll. 37–38.[26] The Court must therefore determine whether "securing" data is a "general computer function" or a "specific function performed by a special purpose computer."

The Federal Circuit recently provided guidance on this particular issue. In *Spa Syspatronic AG v. United States*, the disputed claim involved a means for producing a secret microcode or access code for communications between a control unit and specific data. 117 Fed. Cl. 375, 390 (2014). The functionality of the claim was to "secur[e] the data from unauthorized access." *Id.* at 390–92. The patent holder argued that separate algorithms were not required for the code limitations due to the *Katz* exception for

---

[26] Although the specification states that "storage unit 54 is used for *storing* the information . . . ." the parties stipulate that the functionality of Claim 82 is "*securing*" of information—not merely "storing."

"processing, receiving, and storing" data that general purpose computers could inherently perform. *Id.* at 391. The Federal Circuit rejected the patent holder's argument, explaining:

> The function of producing an access code by one chip and then the utilization of it by another chip to grant access to its stored data *goes beyond storing or retrieving data. It is the securing of data from unauthorized access that is claimed in this case.* The patentee clearly intends for the chips to be used in a *specific way for a special function*, unlike in *Katz.*
>
> Likewise, the production and use of a secret microcode *to limit access or for decryption goes beyond a general purpose function of a processor.* The use of the term "secret" is enough to distinguish from the generic use of a processor. The secret microcode limitation requires an algorithm for achieving that function. . . .

Id. at 392 (emphasis added).

In this case, the "securing" functionality of Claim 82 is nearly identical to the functionality of the disputed claim in *Spa Syspatronic*. Specifically, like in *Spa Syspatronic*, Claim 82 asserts a method of "securing" certain data from unauthorized access or tampering by interested parties. *See* '219 Patent col. 4 ll. 37–38 (amended version). For this reason, the Court finds that Claim 82's "securing" function cannot be implemented by a general purpose computer but instead must be implemented in a special purpose computer.

Because a special purpose computer is necessary to perform the functionality of Claim 82, *Aristocrat* applies and the Feldbau Patent must disclose an algorithm that performs the particular function of securing at least part of the authentication data against tampering by interested parties. *See Aristocrat*, 521 F.3d at 1333; *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1367 (Fed. Cir. 2008).

ii. Adequacy of Disclosed Algorithms

GoDaddy asserts that the specification discloses only one algorithm and endorses that algorithm as the corresponding structure. (Doc. 117 at 20–21). In its briefing, rather than discussing whether an algorithm is required, RPost merely advocates that the Court should adopt Judge Gilstrap's construction. *See* (Docs. 114 at 18–19; 119 at 18). During

1   the *Markman* Hearing, RPost stated that it offered GoDaddy's current proposal as an

2   alternative method before Judge Gilstrap, but did not in this case because Judge Gilstrap

3   rejected the method as too detailed. *See RMail*, 2013 WL 968246, at *31–35.

4   Initially, the Court finds that RPost's current proposal is flatly deficient. The

5   Federal Circuit has long held that "[s]imply disclosing a black box that performs the

6   recited function is not a sufficient explanation of the algorithm required to render the

7   [MPF] term definite." *Augme Techs., Inc. v. Yahoo! Inc.*, 755 F.3d 1326, 1337–38 (Fed.

8   Cir. 2014) (citing *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 518 (Fed. Cir.

9   2012)). Both "storage unit 54" and "storage device 106" are merely "black box" terms

10   found in Figures 2, 3, and 4 of the specification and do not provide an algorithm as

11   required by *Aristocrat*. Therefore, the Court rejects RPost's proposed construction.

12   Beyond "storage unit 54" and "storage device 106," the specification discloses

13   several methods of "securing" authentication-information. Namely, the specification

14   provides three separate and "relatively secure" methods of storing authentication-

15   information via storage unit 54 and a fourth "secure" method as an alternative. The

16   "relatively secure" methods disclose storage unit 54 as being (1) a "Write-Once-Read-

17   Many (WORM) device such as an optical disk or a Programmable Read-Only Memory

18   (PROM) device"; (2) "enclosed within a securable device"; or (3) "provided with read-

19   only access privilege." '219 Patent col. 7 ll. 46–51. The alternative "secure" method

20   requires "using a compression, private or public key encryption or scrambling technique,

21   a password, or a combination thereof such as those employed by the widely used RSA

22   encryption method, and by the PKZIP(tm) program from PKWARE Inc., Glendale Wis.,

23   U.S.A., and where the "securing" procedure, key or password are unknown to any

24   interested party." *Id.* col. 7 ll. 51–58. The question before the Court is which, if any, of

25   these methods set forth a sufficient algorithm that satisfies *Aristocrat*.

26   The first method discloses storage unit 54 as a "Write-Once-Read-Many (WORM)

27   device such as an optical disk or a Programmable Read-Only Memory (PROM) device."

28   *Id.* col. 7 ll. 46–48. As to the securing process, the specification explains that controller

- 133 -

1   56 "stores" and "retrieves" the information from storage unit 54, and "unsecures" the

2   information if it is "secured." *Id.* col. 7 ll. 59–col. 8 ll. 5. Under Federal Circuit law, "[i]t

3   is well settled that simply disclosing software . . . without providing some detail about the

4   means to accomplish the function, is not enough." *Function Media*, 708 F.3d at 1318

5   (citation and quotations omitted). This first method of "securing," however, does not

6   simply disclose the generic term "software," but provides particular types of software that

7   inherently assure that the data written on the device cannot be tampered with once it is

8   written on the device. *See Dictionary of Computer Science Engineering and Technology*

9   534 (Philip A. Laplante ed., 2000) (defining "write once read many" as "used to refer to

10   memory devices that allow data to be written once after device fabrication, and to be read

11   any number of times. A typical example is PROM."); *Dictionary of Information*

12   *Technology* 505 (Ramesh Bangia ed., 2d 2010) (defining WORM as "Storage device that

13   uses an optical medium that can be recorded only once. Updating requires destroying the

14   existing data . . . .").

15   The Court finds that the disclosed step of storing the authentication data on a

16   WORM device properly limits the scope of the "corresponding structure, material, or

17   acts" that perform the function of "securing," as required by § 112(6). Due to the innate

18   "secured" characteristic of a WORM device, the single step of storing the data on such a

19   device is all that is required to perform the claimed function of "securing at least part of

20   the authentication data against tampering by either the sender or the recipient." *See Noah*,

21   675 F.3d at 1313 (finding that a specification set forth a sufficient algorithm by

22   disclosing "that authorized agents are provided with passcodes and that agents cannot

23   enter, delete, review, adjust or process data inputs within the master ledger unless the

24   passcode is verified"). Consequently, the Court concludes that this method of "securing"

25   data from tampering by an interested party adequately sets forth an algorithm and

26   therefore constitutes corresponding structure. *See Ericsson*, 417 F.3d at 1249 (Fed Cir.

27

28

- 134 -

2005) ("[T]he corresponding structure for a § 112 ¶ 6 claim for a computer-implemented function is the algorithm disclosed in the specification.").[27]

As to the second method, the Federal Circuit holds that a purported algorithm cannot "merely provide[] functional language." *Ergo Licensing*, 673 F.3d at 1365. Moreover, simply reciting the claimed function in the specification, while including nothing about how the computer or processor ensures that those functions are performed, is not a sufficient disclosure for an algorithm. *See Blackboard, Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371, 1384 (Fed. Cir. 2009). Here, the specification simply discloses that storage device 54 is "enclosed within a securable device." '219 Patent col. Such nonce terminology merely discloses functional language without any form of structure. *See Williamson*, 792 F.3d at 1350 (citing *MIT*, 462 F.3d at 1354); *Robert Bosch, LLC v. Snap-On, Inc.*, 769 F.3d 1094 (Fed. Cir. 2014) (finding that the word "device" is generally a non-structural, nonce term (citing cases)). For this reason, the Court finds that a sufficient algorithm has not been disclosed for this method.

The third disclosed method to "secure" the authentication data via storage unit 54 is "it may be provided with read-only access privilege." '219 Patent col. 7 ll. 50–51. The specification devotes only one other sentence to this method: "[o]ne embodiment of secure storage is that which has read-only privileges." *Id.* col. 9 ll. 56–67. Unlike the first disclosed method of storing the data on a WORM or PROM device, the sole step of "[p]rovid[ing the data] with read-only privilege" does not set forth a step-by-step procedure for how the claim's function of "securing" is to be performed. *See Triton Tech of Texas, LLC v. Nintendo of Am., Inc.*, 753 F.3d 1375, 1378–79 (Fed. Cir. 2014) ("However, merely using the term 'numerical integration' does not disclose an

---

[27] The Court notes that storage device 106 also sets forth storing the data on "a WORM device, such as a PROM." '219 Patent col. 13 ll. 36–37. As the Court determined for storage unit 54, this sets forth sufficient structure. Further, because the algorithm is the corresponding structure, the WORM device is the structure, not simply storage device 106. *See Ericsson*, 417 F.3d at 1249.

1 algorithm—i.e., a step-by-step procedure—for performing the claimed function [of

2 integrator means]." (citing *Ergo Licensing*, 673 F.3d at 1365)). For example, the

3 specification does not explain how the data is "provided" with read-only access or who

4 has access to the data. For these reasons, the Court finds that this method fails to disclose

5 a sufficient algorithm.

6 The fourth method of "securing" authentication data is "using a compression,

7 private or public key encryption or scrambling technique, a password, or a combination

8 thereof, such as those employed by the widely used RSA encryption method, and by the

9 PKZIIP(tm) program from PKWARE Inc., Glendale, Wis., U.S.A., and where the

10 'securing' procedure, key or password are unknown to any interested party." The Court

11 finds that this method sufficiently describes an algorithm to accomplish the claimed

12 function of securing data against unauthorized access. *See Noah*, 675 F.3d at 1313.

13 Accordingly, the Court finds that the corresponding structure for "means for

14 securing at least part of the authentication data against tampering of the sender and the

15 recipient wherein the processor is combined with the means for securing" is "securing the

16 authentication data either (1) by storing the data on a write-once read-many ("WORM")

17 device such as an optical disk or a Programmable Read-Only Memory ("PROM") device;

18 or (2) by storing the data using a compression, private or public key encryption or

19 scrambling technique, a password, or a combination thereof, such as those employed by

20 the widely used RSA encryption method, and by the PKZIIP(tm) program from

21 PKWARE Inc., Glendale, Wis., U.S.A., and where the 'securing' procedure, key or

22 password are unknown to any interested party." *See Ericsson*, 417 F.3d at 1249.

23 **I.   "source transmitting system" (Term No. 10) / "destination
   receiving system" (Term No. 11)**

24

25 **1.   The Parties' Positions**

26 The primary difference between the parties' proposed constructions for these

27 disputed claim terms involves the word "system." RPost proposes that "source

28 transmitting system" be construed as "system for transmitting a dispatch for a sender"

1   and "destination receiving system" as "system for receiving a dispatch for a recipient."

2   (Doc. 114 at 19). RPost insists that its constructions are "consistent with the plain claim

3   language." (*Id.*)

4   Parroting its proposed constructions for "sender" (Term No. 5) and "recipient"

5   (Term No. 6), GoDaddy proposes that "source transmitting system" be construed as "the

6   computer that originates the dispatch" and that "destination receiving system" be defined

7   as "the computer that receives the dispatch at its intended destination." (Doc. 117 at 21).

8   GoDaddy explains that its proposed constructions are necessary to clarify that the two

9   systems are computer-based. (*Id.*) GoDaddy cautions that if the Court were to adopt

10   RPost's "ambiguous" constructions, the jury could misinterpret "system" to mean any

11   "system" regardless of whether it is computer-based. (*Id.*) Further, during the *Markman*

12   Hearing, GoDaddy argued that "system" is a nonce word that discloses no structure.

13   RPost replies that GoDaddy's ambiguity argument is "unfounded" because

14   GoDaddy stipulated to a construction of "sub-system" for another term. (Doc. 119 at 13);

15   *see infra* at 26. RPost also stresses that the "computer-based" limitation is already

16   disclosed in the claim, making a recitation of "computer" in either construction

17   unnecessary. (Doc. 119 at 13).

18   **2.   Analysis**

19   These two terms are disclosed in Claim 82 as follows:

20   **82**. An information dispatch system in an electronic communication
          network comprising;
21
          a *source transmitting system* coupled to the electronic
22   communicating network for sending a dispatch from a sender to a recipient;

23   a *destination receiving system* coupled to the electronic
     communication network for receiving the dispatch for the recipient
24
25   '219 Patent col. 4 ll. 4–9 (amended version) (emphasis added).

26   The Court finds little merit in GoDaddy's fear that the jury could misinterpret

27   "system" to be something other than a "computer-based" system. Claim 82's preamble

28   expressly states that both "source transmitting system" and "destination receiving

- 137 -

1   system" must be "*in* an electronic communication network." *Id.* col. 4 ll. 4–5 (emphasis

2   added). Moreover, Claim 82 requires that each "system" be "coupled to the electronic

3   communication network." *Id.* col. 4 ll. 6; *id.* col. 4 ll. 9. As a result, neither "system"

4   could be interpreted as anything other than a computer-based system. Moreover, while

5   the Court agreed with GoDaddy that the terms "recipient" and "sender" have "plain and

6   ordinary meanings" that include natural persons, the same does not hold true for "source

7   transmitting system" or "destination receiving system"—particularly when both systems

8   are "in an electronic communication network." The Court nevertheless concludes that the

9   jury would be aided by a construction that limits "system" as being "computerized."

10   Furthermore, the Court finds that limiting the term "system" to "computer" as

11   GoDaddy proposes would be improper. GoDaddy has not persuaded the Court that Claim

12   82 only embodies "computers" *per se*. While it is undisputed that each claimed "system"

13   must be "electronic" or "computerized," construing "system" simply as "computer" could

14   imply to the jury that the "transmitting" and "receiving" systems can only be

15   "computers" and not another type of computerized system.

16   Additionally, the Court is not convinced that GoDaddy's proposed language of

17   "originates" is accurate. Specifically, the claim does not disclose that the "source

18   transmitting system" originates the message. In fact, the parties stipulated that the

19   "*sender* originates" the entire content of the message. (Doc. 191-1 at 14) (emphasis

20   added). GoDaddy has not shown that "sender" and "source transmitting system" are

21   synonymous such that the doctrine of claim differentiation is overcome. *See Andersen*

22   *Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1369 (Fed. Cir. 2007) (explaining that

23   the doctrine of claim differentiation is based on "the common sense notion that different

24   words or phrases used in separate claims are presumed to indicate that the claims have

25   different meanings and scope." (quoting *Karlin Tech. Inc. v. Surgical Dynamics, Inc.*,

26   177 F.3d 968, 971–72 (Fed. Cir. 1999))).

27   GoDaddy's proposed construction for "destination receiving system" also includes

28   the limitation "at its intended destination." (Doc. 117 at 21). GoDaddy does not discuss

- 138 -

this proposed limitation in its briefing but explained at the *Markman* Hearing that "[t]he whole point of the invention is to confirm or verify that the message was delivered at its intended destination hence that aspect of GoDaddy's claim construction." As it found for Term No. 6, the Court concludes that including this limitation requires the jury to engage in unnecessary additional inquiry.

For these reasons, the Court construes "source transmitting system" as "computerized system for transmitting a dispatch for a sender" and "destination receiving system" as "computerized system for receiving a dispatch for a recipient."

VIII. Conclusion

For the foregoing reasons,

IT IS ORDERED that the Court adopts the constructions, pursuant to *Markman*, as set forth in this Order for the disputed terms of the Tomkow and Feldbau Patents.

IT IS FURTHER ORDERED that the parties may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this Order, other than the actual definitions adopted by the Court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the Court.

Dated this 19th day of January, 2016.