UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

XMISSION, L.C., a Utah company,
 	
    Plaintiff,
 	
vs.
 	
LANCE TRIMBLE, an individual and
VANGUARD INTERACTIVE MEDIA, an
expired Utah limited liability company,
 	
    Defendants.
	REPORT & RECOMMENDATION
	
	  Case No.: 2:17-cv-00013
	
	District Court Judge Dee Benson
	
	Magistrate Judge Dustin Pead

INTRODUCTION

This matter is before the undersigned pursuant to a 28 U.S.C. §636(b)(1)(B) referral from District Court Judge Dee Benson.[1] On January 5, 2017, Plaintiff XMission L.C. (Plaintiff or XMission) filed a complaint against Defendants Lance Trimble (Trimble) and Vanguard Interactive Media, L.L.C (Vanguard) (collectively Defendants) alleging violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), 15 U.S.C. §§ 7701 et seq. and seeking statutory damages and a permanent injunction.[2]

Based on Defendants' failure to appear, obtain counsel or answer the complaint, even after receiving an extension of time within which to do so,[3] the clerk of court entered a default

---

[1] ECF No. 21.

[2] ECF No. 2.

[3] ECF No. 28.

certificate against Defendants on March 26, 2018.[4] Currently before the court is XMission's

motion for entry of judgment.[5] A telephonic hearing was held on May 15, 2018.[6] Attorney

Jordan K. Cameron appeared on behalf of XMission. Neither Defendant nor counsel appeared on

behalf of Defendants.[7]

On June 8, 2018, Trimble filed a letter responding to Plaintiff's motion.[8] XMission did

not object to the form or timing of Trimble's response, but filed its own reply memorandum.[9]

Although untimely, the Court considers the arguments raised in Trimble's response and now

rules as set forth herein.[10]

---

[4] ECF No. 34.

[5] ECF No. 35 (*redacted*); ECF No. 38 (*sealed*).

[6] ECF No. 42.

[7] ECF No. 43.

[8] ECF No. 45. As a pro se litigant, Trimble cannot legally represent a business entity and therefore his arguments are not raised on behalf of Vanguard. (ECF No. 22 at 4); *see Harrison v. Wahatoyas, LLC,* 253 F.3d 552, 556-67 (10th Cir. 2001) ("As a general matter, a corporation or other business entity can only appear in court through an attorney and not through a non-attorney corporate officer appearing pro se."); *see also* DUCivR 83-1.3.

[9] ECF No. 48.

[10] *See* DUCivR 7-1(a)(b)(3)(A).

SLC_3750677

BACKGROUND

The facts stated herein are as alleged in XMission's complaint and supporting declarations.[11] Defendant Trimble is an individual residing in Utah.[12] Defendant Vanguard is a Utah limited liability company which expired on the records of the state as of December 30, 2013.[13]

Plaintiff XMission was founded in 1993 and is a well-recognized Internet Service Provider (ISP) in Utah.[14] Over time, XMission has expanded its technical offerings to include cloud hosting, web hosting, email service and hosting, collaboration tools, business VoIP phone service and high speed internet connectivity solutions including optical Ethernet, copper and fiber.[15] XMission owns all the servers, routers, and switches on its network through which it hosts and provides Internet access services for its customers.[16]

On July 19, 2012, Trimble entered into an email Publisher Agreement (Agreement) with advertising network Adknowledge, identifying the publisher for purposes of Adknowledge's

---

[11] ECF No. 2; ECF No. 38-1; ECF No. 38-2.

[12] ECF No. 2, ¶2

[13] *Id*. at ¶3; ECF No. 38-4, Exhibit D.

[14] *Id.* at ¶ 9, *see also* ECF No. 38-1, ¶3, Exhibit A, *Declaration of Peter L. Ashdown*; ECF No. 38-1, Exhibit 1, *Articles of Organization of XMission, L.C.*; ECF No. 38-1 Exhibit 2, *Articles of Amendment to the Articles of Organization* and *Operating Agreement*.

[15] ECF No. 38-1, ¶¶4-6.

[16] *Id.* at ¶11.

records as Vanguard Interactive Media, LLC.[17] Trimble signed the Agreement personally.[18]

Between February and March 2015, XMission received at least 6,204 commercial emails sent

and/or initiated by or on behalf of the Defendants. The emails were sent from a series of domain

names registered by Defendants with false or inaccurate addresses.[19] The redirect information for

each email identified *adstation.subdomain.com*, which is owned and operated by

Adknowledge.[20] Adknowledge identified the sender domains used to send the emails in question

as belonging to the Defendants.

XMission asserts the 6,204 emails were sent from a series of domain names registered by

Defendants with false or inaccurate addresses in violation of various provisions of the

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), 15

U.S.C. §§ 7701-7713.[21] CAN-SPAM regulates the manner in which unsolicited commercial

emails are transmitted and makes certain conduct unlawful including the transmission of false or

misleading information.[22]

---

[17] ECF No. 38-1, ¶ 25, ECF No. 38-9, Exhibit I, *Adstation Integrated Agreement* (*sealed*).

[18] *Id.*

[19] ECF No. 38, ¶53; ECF No. 38-7, Exhibit G; ECF No. 38-3, Exhibit H, ECF No. 38-10, Exhibit J.

[20] ECF No. 38, ¶ 28; ECF No. 38-3, Exhibit C; ECF No. 38-10, Exhibit J; ECF No. 38-11,Exhibit K, email metadata (identifying each email routing).

[21] The court has subject matter jurisdiction pursuant to 28 U.S.C. §1331, for violations of the 15 U.S.C. §7701 et. seq., and pursuant to 15 U.S.C. §7706(g)(1) for case involving a civil action by an internet access service adversely affected by a violation of 15 U.S.C. §7704(a)(1), 15 U.S.C. §7704(b) or 15 U.S.C. §7704(d), or a pattern and practice that violates subparagraphs (2), (3), (4), and/or (5) of 15 U.S.C. §7704(a).

[22] *MySpace, Inc. v. The Globe.com, Inc.,* 2007 U.S. Dist. LEXIS 44143 at *3 (C. D. Cal. Feb.27, 2007); ECF No. 38-13, Exhibit M; 15 U.S.C. 7701 et seq.

ANALYSIS

I.   STANDING

A federal court lacks "subject matter jurisdiction to consider the merits of any claim unless the plaintiff has standing, irrespective of whether the issue is raised by the defendant."[23]

CAN-SPAM was passed into law in 2003 and regulates the manner in which unsolicited commercial emails are transmitted.[24] Under CAN–SPAM, an Internet access service provider "adversely affected" by a violation of 15 U.S.C. § 7704(a)(1), (b), or (d), or a pattern or practice that violates paragraph (2), (3), (4), or (5) of section 7704(a), may bring a civil action in any district court of the United States with jurisdiction over the defendant to enjoin further violation and recover damages.[25] Standing under CAN–SPAM involves two components: (1) a determination that plaintiff it is a bona fide Internet access service provider[26] and, (2) a finding that plaintiff was adversely affected by spam emails.[27] The issue of standing must be addressed before awarding damages under the statute.

---

[23] *Hoang v. Reunion.com, Inc.,* 2010 U.S. Dist. LEXIS 34466 * 7 (N. D. Cal. 2010) (*citing United States v. Hays,* 515 U.S. 737, 742, 115 S. Ct. 2431, 132 L. Ed. 2d 635) (1995).

[24] *See* 15 U.S.C. §§ 7701, *et. seq., see also United States v. Kilbride,* 584 F.3d 1240, 1256 (9ᵗʰ Cir. 2009) ("The CAN-SPAM Act was enacted to prevent senders of electronic mail from deceiving recipients 'as to the source or content of such mail' and to ensure the recipients 'have a right to decline to receive additional commercial electronic mail from the same source.") (*citing* 15 U.S.C. § 7701(b)(2)-(3).

[25] *See* 15 U.S.C. § 7706(g)(1) (authorizing a private right of action to a "provider of Internet access service.").

[26] *See Gordon v. Virtumundo,* 575 F.3d 1040, 1050 (9ᵗʰ Cir. 2009) (*citing*, 150 Cong. Rec. E72–02).

[27] *Id.* at 1049; *See also* 15 U.S.C. § 7706(g)(1).

a. XMission is a bona fide Internet access service.

CAN–SPAM defines Internet access service as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services."[28] Standing under CAN-SPAM is limited to "bona fide" Internet access services.[29] Courts have extended the definition of Internet access services to "include [ ] traditional [ISPs], any email provider, and even most website owners."[30]

In Utah, XMission is recognized as a well-known and legitimate ISP that offers various Internet access services, including email.[31] XMission owns, maintains and configures all the servers, routers, and switches on its network through which it hosts and provides internet access services to its customers.[32] Further, XMission maintains ownership, sole physical control and uninhibited access over its hardware.[33] As such, XMission operates as a bona fide Internet access

---

[28] 15 U.S.C. § 7702(11); *see also* 47 U.S.C. § 231(e)(4) (defining the term "Internet" as "the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information.").

[29] *See Gordon,* 575 F.3d at 1050 (*citing* 150 Cong. Rec. E72-02) ("[W]e intend that Internet access service providers provide actual Internet access service to customers.").

[30] *MySpace, Inc.* at *10; *see also Facebook, Inc. v. ConnectU LLC,* 489 F. Supp. 2d 1087, 1094 (N. D. Cal. 2007), ECF No. 38-14, Exhibit N.

[31] ECF No. 38-1, Exhibit A, ¶¶ 7-9.

[32] *Id.* at ¶11

[33] *Id.* at ¶14.

6

service and meets the first component of standing under CAN-SPAM.[34]

b. XMission is adversely affected by spam.

In order to establish standing under the "adversely affected" element of CAN–SPAM, the

harm "need not be significant in the sense that it is grave or serious, [but] the harm must be of

significance to *a bona fide* IAS [internet access service] provider—something beyond the mere

annoyance of spam . . . ."[35] Typically, "evidence of some combination of operational or technical

impairments and related financial costs attributable to unwanted commercial e-mail suffice."[36]

Impairments may "include network crashes, higher bandwidth utilization, and increased costs for

hardware and software upgrades, network expansion and additional personnel."[37] Moreover, it is

not necessary to prove that "the emails at issue adversely affect plaintiff, rather, that '[t]he e-

---

[34] Trimble argues that XMission is similarly situated to plaintiff in *Gordon v. Virtumundo, Inc.* and does not qualify as a bona fide ISP. 575 F.3d 1040 (9th Cir. 2009) (ECF No. 45.) XMission, however, is unlike the Plaintiff in *Gordon* who did not fit any reasonable definition of an Internet access service provider because he was:

> a registrant of a domain name, which he, through Omni, hosts on leased server space. He neither ha[d] physical control over nor access to the hardware, which GoDaddy own[ed], house[d], maintain[ed], and configure[d]. . . . Gordon's service appears to be limited to using his "Plesk" control panel, which he accesses via an ordinary Internet connection through an ISP, to set up execute other administrative tasks. Verizon enables his online access. GoDaddy provides the service that Enables ordinary consumers to create e-mail accounts, register domain names, and build personalized web pages. Gordon has simply utilized that service for himself and on behalf of others.

Gordon, 575 F.3d at 1052.

[35] *Id.* at 1053–54.

[36] *ZooBuh Inc. v. Better Broad., LLC,* 2013 U.S. Dist. LEXIS 77033 at *8 (D. Utah May 31, 2013) (*citing Gordon,* 575 F.3d at 1054); ECF No. 38-16, Exhibit P.

[37] *Gordon*, 575 F.3d at 1053.

7

mails at issue in a particular case . . . contribute to a larger, collective spam problem.'"[38]

To increase its capacity to deal with spam, XMission expends large sums of money in hardware acquisition, maintenance and other related expenses.[39] These expenses are necessary to address spam-related harm, spam filtering, employee time and other costs associated with problems caused by the receipt of spam.[40] During the time frame at issue in this case, XMission employed two (2) full-time workers to deal with spam related issues by adjusting filtering, responding to customer complaints, addressing blacklist issues, and acting as first responders to data security breaches and hardware issues caused by spam.[41] Additionally, XMission employed twelve (12) technicians and one supervisor, who dedicated part of their time, along with thirteen (13) servers to process and address spam related issues.[42] On average, approximately 40% and 85% of the email messages that XMission received on its system were spam emails of which the subject emails are a part.[43]

---

[38] *ZooBuh Inc.*, at *8 (*citing Gordon,* 575 F.3d at 1054).

[39] ECF No. 38-1, Exhibit A, ¶13; ECF No. 38-2, Exhibit B, ¶¶4-15, *Declaration of Mat White*.

[40] ECF No. 38-2, Exhibit B.

[41] ECF No. 38-1, ¶20; ECF No. 38-2, ¶5, Exhibit 1.

[42] *Id.* at ¶¶21-22; ECF No. 38-2.

[43] *Id.* at ¶¶27-31, Exhibit 14, Exhibit 15. XMission indicates that the number of spam received would be significantly higher if not for the precautions it has taken; including, subscribing to anti-spam services, including blacklists and creating customized and proprietary filtering rules and e-mail servicer configurations.

Trimble argues XMission must "prove unequivally [sic] that harm was caused to the plaintiff directly as the result of tortuous [sic] or inherently fraudulent activities."[44] This is incorrect. In order to establish adverse effect the harm "need not be significant in the sense that it is grave or serious, [but] the harm must be of significance to a bona fide IAS provider---something beyond the mere annoyance of spam . . . ."[45] Trimble also contends that XMission is simply a "litigation factory" who has previously sued and obtained monetary payments related to spam from other parties.[46] Any prior litigation, settlement or damage award, however, has no bearing on the unfavorable impact of spam and does not prohibit, or otherwise limit, XMission's ability to pursue statutory damages against Trimble for violations of CAN-SPAM.

As a bona fide Internet access server, it is undisputed that XMission experienced, and continues to experience, operational and technical impairments, with related financial costs, associated with its receipt of commercial email and spam.[47] During the time frame at issue XMission was adversely affected by spam and thereby satisfies the second component of standing. XMission is a bona fide ISP with standing to pursue its claims against Defendants under CAN-SPAM.

---

[44] ECF No. 45 at 1. Of note, Trimble pulls the words "tortuous" and "inherently fraudulent" from the courts' analysis of the preemptive effect of CAN-SPAM over state law. *See Silverstein v. Keynetics, Inc.,* 727 Fed. Appx. 244, 246 (9th Cir. 2018) (citation omitted). Those standards do not apply to the harm analysis required to show adverse effect for purposes of standing.

[45] *Gordon*, 575 F.3d at 1053-54.

[46] ECF No. 45. *See also Gordon*, 575 F.3d at 1067 (concurrence).

[47] ECF No. 38-1, ¶¶18-22; ECF No. 38-2, ¶¶4-15.

SLC_3750677

II.   DEFENDANTS' LIABILITY

CAN-SPAM assigns liability to two separate categories of actors: "senders" and "initiators".[48] An "initiator" is the party who "originate[d] or transmit[ed] such message" or who "procure[d] the origination or transmission of such message . . . ."[49] Importantly, CAN-SPAM recognizes that "more than one person may be considered to have initiated a message."[50]

Here, Trimble individually, and through his defunct entity Vanguard Media Interactive, acted as an email publisher through the Adstation marketing network offered by Adknowledge, Inc., pursuant to the Agreement dated July 19, 2012[51] Although Defendants contend they had no control over the emails' "from" names, subject headings, or other header information transmitted, Defendants are independently liable from any other party involved because Defendants "actually originated" the emails in question.[52] Therefore, Defendants are liable under the CAN-SPAM's definition of "initiate."

---

[48] *See* 15 U.S.C. § 7702(9), (16).

[49] 15 U.S.C. § 7702(9).

[50] *See id.*; *see also* 15 U.S.C. § 7704 (making it unlawful for any party, whether designated as a "sender" or "initiator" to "initiate the transmission" of an email that violates the Act); ECF No. 38-15, Exhibit O, 108 S. Rep. 102 at 14 ("more than one person may be considered to have initiated a message. Thus, if one company hires another to handle the tasks of composing, addressing, and coordinating the sending of a marketing appeal, both companies could be considered to have initiated the message–one for procuring the origination of the message; the other for actually originating it.); 15 U.S.C. § 7702(9), (16).

[51] *See* ECF No. 38-9, Exhibit I (*sealed*).

[52] *See* 15 U.S.C. § 7702(9).

SLC_3750677

III.   VIOLATIONS OF THE CAN-SPAM ACT

XMission alleges the 6,204 emails at issue are in violation of Sections 7704(a)(1),

7704(a)(1)(A), and 7704(a)(5)(A)(iii) of the CAN-SPAM Act. The court addresses each

provision herein.[53]

a.   15 U.S.C. § 7704(a)(1)—False Header Information

Header information includes a "from" line that identifies "or purport[s] to identify a

person initiating the message[.]"[54] The party responsible for the email determines what the

"from" line will be.

Pursuant to Section 7704(a)(1), CAN SPAM prohibits the transmission of a commercial

electronic mail message, or a transactional or relationship message, that contains, or is

accompanied by, header information that is materially false or materially misleading.[55] When

used with respect to false or misleading header information the term materially "includes the

alteration or concealment of header information in a manner that would impair the ability of an

Internet access service processing the message on behalf of a recipient . . . to identify, locate, or

respond to a person who initiated the electronic mail message or to investigate the alleged

violation."[56]

---

[53] XMission does not allege violations of 15 U.S.C. § 7704(a)(3) or § 7704(a)(4) and as a result
Trimble's arguments regarding the ability to unsubscribe to emails within ten days are inapplicable. (ECF
No. 45.)

[54] *See* 15 U.S.C. § 7704(a)(1)(B).

[55] *Id.*

[56] 15 U.S.C. § 7704(a)(6).

The 6, 204 emails in question contain "from" names that identify generic product categories, not any real person or business entity.[57] Specific examples of "from" lines used here include: 401K Plan, Here Airline Tickets, Brand Name Computers, Cable Internet, Dental Plans, Hotel, Jewelry Outlet, Lobster, Myrtle Beach, Online Coupons, Singles, Unsecured Loan and Window Coverings.[58] Because the emails use generic designations, XMission cannot rely on the "from" name to identify the source of the message.

Nonetheless, the use of a generic "from" name [59] alone is not necessarily a violation of CAN-SPAM because a party may rely on the accompanying WHOIS[60] information to identify the source of the message.[61] Each domain contains corresponding WHOIS information.[62] An

---

[57] ECF No. 38-3, Exhibit C; ECF No. 38-5, Exhibit E; ECF No. 38-11, Exhibit K; ECF No. 40.

[58] *Id.*

[59] A generic "from" name is distinguishable from a false or misleading "from" name that identifies a party not associated with or responsible for the email. A materially false or misleading "from" name violates CAN-SPAM's prohibition against the transmission of an email with "header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1) ("or is accompanied by").

[60] WHOIS information is header information that accompanies an email. "WHOIS is a publicly available online database through which users can access information regarding domains, including the registrant's name, address, phone number, and email address" *Gordon*, 575 F.3d at 1064, n. 22 (*citing Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act*, 70 Fed.Reg. 25,426, 25,446 n. 233) (proposed May 12, 2005) (to be codified at 16 C.F.R pt. 316). "WHOIS data is compiled by registrars from information submitted by registrants." *Id.; see also Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 395 (2d Cir. 2004) ("Applicants to register a domain name submit to the registrar contact information, including at a minimum, the applicant's name, postal address, telephone number, and electronic mail address. The ICANN Agreement, referring to this registrant contact information under the rubric 'WHOIS information' requires the registrar, under terms discussed in greater detail below, to preserve it, update it daily, and provide for free public access to it through the Internet as well as through an independent access port, called port 43."). Further, "free public access to WHOIS information . . . has two purposes. The primary purpose is to provide necessary information in the event of . . . disputes." *Register.com Inc.*, 356 F.3d at 418.

[61] *Gordon*, 575 F.3d at 1063–64 (finding, in the course of holding the claim was preempted, there was nothing "inherently deceptive" in the defendant's use of fanciful domain names based in part on the

12

email service provider should be able to rely on an email's accompanying WHOIS information to determine the actual source of the email. It is a violation of CAN-SPAM where the accompanying WHOIS information is false or misleading.[63]

Here, the WHOIS information accompanying each of the 6,204 emails contains a registrant address that is false and not associated with Defendants.[64] As a result, XMission is unable to rely on the intentionally generic "from" names or the accompanying inaccurate WHOIS registration information to identify the emails' source. This practice goes beyond the use of fanciful or creative "from" names and actually interferes with a recipient's ability to identify and contact the responsible party. The fundamental purpose of the "from" name is to "identify a person initiating the message."[65] The headers in the emails do not satisfy this purpose and, because the accompanying publicly available WHOIS information also contains false information, the emails violate § 7704(a)(1) of the CAN-SPAM Act.[66]

---

admitted fact that "a WHOIS search, or a similar reverse-look-up database, accurately identifies [the defendant] as the domain registrant and provides other identifying information"); *see also Balsam v. Trancos, Inc.,* 203 Cal. App 4th 1083, 1097 (Cal Ct. App. 2012).

[62] *Id.* at 1064 (*citing Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act*, 70 Fed. Reg. 25,426, 25,446 n. 233) (proposed May 12, 2005) (to be codified at 16 C.F.R pt. 316)).

[63] *See* 15 U.S.C. § 7704(a)(1) (it is "unlawful for any person to initiate the transmission of a commercial electronic mail message . . . that . . . is accompanied by, header information that is materially false or materially misleading.").

[64] ECF No. 38, ¶¶53-55; ECF No. 38-3, Exhibit C; ECF No. 38-11, Exhibit K.

[65] *See* 15 U.S.C. § 7704(a)(1)(B).

[66] 15 U.S.C. § 7704(a)(1)(A).

13

b. 15 U.S.C. § 7704(a)(1)(A)---False Domain

CAN-SPAM violations "are not limited to false or misleading header information alone."[67] Pursuant to 15 U.S.C. § 7704(a)(1)(A), "header information that is technically accurate but includes an originating . . . domain name . . . the access to which for purposes of initiating the message was obtained by means of false or fraudulent . . . representations shall be considered materially misleading . . . ."[68] Thus, even if an email contains accurate header information, if the domain name used to send the message was obtained by means of a false or fraudulent representation, any email sent from that domain is in violation of CAN-SPAM regardless of the accuracy of the header or other content.

The registration of a domain name by a domain registrant constitutes a representation.[69] Representations made by a domain registrant include "contact information, including at a minimum, the applicant's name, postal address, telephone number, and electronic mail address."[70] Where a domain registrant obtains a domain and provides a false address for inclusion in WHOIS, that domain is obtained with a false representation and therefore each email sent from the domain violates CAN-SPAM. Simply in registering a domain, the registrant makes a representation when it provides its address. If the address is false or inaccurate, this constitutes a false representation in violation of § 7704(a)(1)(A).

---

[67] *ZooBuh Inc.*, at *6; ECF No. 38-16, Exhibit P.

[68] 15 U.S.C. § 7704(a)(1)(A).

[69] *See ZooBuh Inc.*, *6–7.

[70] *Register.com Inc.*, 356 F.3d at 395.

14

Here, the 6,204 emails at issue were sent from domains which, at the time of the emails in question, had accompanying WHOIS information that included a non-existent and, therefore, false registration address.[71] Thus, the emails were sent from domains obtained through false representation (i.e., false address) in violation of 15 U.S.C. § 7704(a)(1)(A) of the CAN-SPAM Act.[72]

c.   15 U.S.C. § 7704(a)(5)(A)(iii)—Required Information

Section 7704(a)(5) of CAN-SPAM requires that every commercial email contain "a valid physical postal address of the sender."[73] In this case, the body of each email contained the address: 15890 El Camino Real, Carlsbad, CA 92009.[74] This address does not exist and has no connection with the "sender" of the emails.[75]

 None of the 6,204 commercial emails at issue in this case contain a valid physical address of the "sender" in the body of the email and are therefore in violation of 15 U.S.C. § 7704(a)(5)(A)(iii) of the CAN-SPAM Act.

---

[71] ECF No. 38, ¶¶53-55; ECF No. 38-3 Exhibit C; ECF No. 38-11, Exhibit K.

[72] Contrary to Trimble's argument, XMission did not easily ascertain that Defendant owned the sending domains. Because the sending domains were registered with false contact information, the only way XMission was able to determine that Defendant owned the domains was by processing metadata hidden in redirect information in the emails, connecting the data therein to the advertising network, Adknowledge, sending a subpoena to Adknowledge regarding the emails, and receiving from Adknowledge information that Defendant owned the domains. (ECF No. 48.)

[73] This section also requires that all commercial emails contain "clear and conspicuous identification that the message is an advertisement or solicitation" and "clear and conspicuous notice of the opportunity, . . . , to decline to receive further commercial electronic mail messages from the sender." 15 U.S.C. § 7704(a)(5)(A)(iii).

[74] *See* ECF No. 38-3, Exhibit C; ECF No. 38-11, Exhibit K.

[75] *Id.*

15

IV.   DAMAGES

A plaintiff may "elect to recover monetary damages in an amount equal to the greater of actual losses or statutory damages specified under the CAN-SPAM Act."[76] If statutory damages are elected, the court has wide discretion in determining the amount of statutory damages to be awarded, constrained only by the specified maxima and minima."[77] With respect to the calculation of statutory damages, each email may contain multiple violations and the amount is calculated by "multiplying the number of violations (with each separately addressed unlawful message that is transmitted or attempted to be transmitted over the facilities of the provider. . . treated as a separate violation) . . . ."[78] In this case, XMission elects to recover statutory damages pursuant to § 15 U.S.C. 7706(g)(3)(A) and seeks an award in the amount of $1,116, 720.

At issue are the 6,204 emails sent by Defendants in violation of 15 U.S.C. § 7704(a)(1) (carrying a penalty of up to $100 per violation), 15 U.S.C. § 7704(a)(1)(A) (carrying a penalty of up to $100 per violation), and 15 U.S.C. § 7705(a)(5)(A)(iii) (carrying a penalty of up to $25 per violation).[79] XMission does not seek the maximum statutory award per violation. Rather,

---

[76] *Tagged, Inc. v. Doe*, 2010 U.S. Dist. LEXIS 5428 *28 (N .D. Cal. Jan. 25, 2010) (*citing* 15 U.S.C. § 7706(g)(1)(B); ECF No. 38-18, Exhibit R.

[77] *Facebook Inc. v. Wallace*, 2009 U.S. Dist. LEXIS 107771 *2 (N.D. Cal. Oct. 29, 2009) (*citing, Columbia Pictures Television, Inc. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1194 (9th Cir. 2001)); ECF No. 38-17, Exhibit Q.

[78] 15 U.S.C. § 7706(g)(3)(A); *See ZooBuh Inc.,* at *10-11 (treating violations of 15 U.S.C. §§ 7704(a) and 7704(a)(1)(A) separately for purposes of analysis and the computation of damages); ECF No. 38-16, Exhibit P; *see also*, FTC's "*Compliance Guide for Business*" (stating, "[e]ach separate email in violation of the law is subject to penalties of up to $41,484 . . . .") *CAN-SPAM Act: A Compliance Guide for Business, Federal Trade Commission* (last accessed May 16, 2018), https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

[79] *See* 15 U.S.C. § 7706(g)(3). To seek damages for violations of §7704 (a)(2), (3), (4) or (5), requires evidence of a pattern or practice. *See* 15 U.S.C. §7706(g)(1). Here, XMission seeks damages for

16

XMission seeks $25.00 per violation of 15 U.S.C. § 7704(a)(1) (6,204 x25=$155,100), $25.00

per violation of 15 U.S.C. § 7704(a)(1)(A) (6,204 x 25=$155,100) and $10.00 per violation of §

7705(a)(5)(A)(iii) (6,204 x10=$62,040) amounting to a total base damage award of $372,240.00

(155,100 + 155,100 + 62,040=$372,240.00).[80] Exercising its broad discretion, the court

concludes that, in this case, the maximum amount allowed under CAN-SPAM is "unnecessary to

address the deterrent and punitive purposes of a statutory damages award."[81] As compared to the

the millions of emails at issue in other cases, Trimble sent 6,024 individual spam emails. [82] As a

result, the court adopts XMission's proposal and, as calculated above, concludes that a total base

damage award of $372,240.00 is appropriate.

Defendant's violations of §7704(a)(5) and has sued for every email in its possession that it was able to connect to Defendants. Because all of the 6,204 emails are in violation of §7704(a)(5) a pattern or practice is established.

[80] The amounts requested by XMission are similar to the awards in *Tagged, Inc. v. Does 1 through 10* and *Asis Internet Services v. Raush*, In *Tagged, Inc. v. Does 1 through 10*, the court awarded the plaintiff $151,975 for 6,079 emails sent by the defendant. 2010 U.S. Dist. LEXIS 5428 * 29-33. The court allowed "$25 per violation," instead of $50, based on the fact that defendant sent only 6,079 emails as compared to the millions of spam messages sent in other cases. Likewise, in *Asis Internet Services v. Rausch*, the Court awarded the plaintiff $865,340.00 for various violations of 15 U.S.C. 7704(a)(1) (which carries an up to $100 penalty) and 15 U.S.C. § 7704(a)(2) (which carries up to a $25 penalty). 2010 U.S. Dist. LEXIS 42952 (N. D. Cal. 2010). Specifically, the court only awarded $25 per violation of 15 U.S.C. § 7704(a)(1) noting, the case involved fewer emails and defendant "did not willfully violate an injunction." *Id.* at *23.

[81] *Yahoo! Inc. v. XYZ Companies,* 872 F. Supp. 2d 300, 308 (S. D. N. Y. 2011).

[82] *See Facebook v. Guerbuez*, 2008 U.S. Dist. LEXIS 108921 (N. D. Cal. Nov. 21, 2008) (awarding Facebook $873 million against Defendant who sent four million spam emails in violation of CAN-SPAM); *Myspace v. Wallace*, 2008 U.S. Dist. LEXIS 75752 (C. D. Cal. May 28, 2008) (awarding Myspace $233 million against defendant who sent 400,000 messages and posted 890,000 comments from 320,000 hijacked Myspace.com user accounts.).

SLC_3750677

Under CAN-SPAM 15 U.S.C. § 7706(g)(3)(C), a court may also award aggravated damages where a "defendant committed the violations willfully and knowingly. . . ."[83] Under such circumstances, "[t]he court may increase a damage award to an amount equal to not more than three times the amount otherwise available."[84] XMission seeks treble aggravated damages for a total award of $1,116,720 (372,240.00 x 3=$1,116,720), arguing Defendants willfully and knowingly transmitted emails with false addresses.

In *Zoobah*, Utah's District Court awarded aggravated damages based on "significant evidence" of the Defendants' use of an automated process to create sender email addresses.[85] Here, however, in light of the base award amount and the absence of direct evidence as to automation or willfulness[86] the court finds trebling unnecessary and declines XMission's invitation to award aggravated damages.[87]

Finally, pursuant to 15 U.S.C. § 7706(g)(1)(A), XMission seeks an injunction enjoining Defendants from further CAN-SPAM violations.[88] Upon review, XMission has substantially prevailed in this matter by demonstrating Defendants' violations of CAN-SPAM as to the 6,024

---

[83] 15 U.S.C. §7706(g)(3)(C).

[84] *Id*.

[85] *Zoobah* at *11.

[86] Trimble asserts the postal address errors were a "simple oversight" and "mistake" and there is no evidence of willfulness. (ECF No. 45.)

[87] *Facebook, Inc. v. Fisher et al.,* 2011 U.S. Dist. LEXIS 9668 *7 (N. D. Cal. Jan 26, 2011) (declining treble damages and awarding statutory damages of $50.00 per violation of CAN-SPAM); *Facebook, Inc. v. Wallace et al.,* 2009 U.S. Dist. LEXIS 107771 *8 (N.D. Cal. Oct. 29, 2009) (awarding statutory damages of $50.00 per violation and declining treble damages).

[88] 15 U.S.C. § 7706(g)(1)(A).

emails in question. Accordingly, an injunction should be entered prohibiting Defendants from sending, or causing to be sent, any email messages to XMission and its customers.

RECOMMENDATION

As set forth above, the court concludes: (i) XMission has standing as a bona fide Internet access service to pursue claims under the CAN-SPAM Act; (ii) Trimble is liable for the emails in question; (iii) 6,204 emails violate 15 U.S.C. §7704(a)(1) because they contained and were accompanied by generic "From" names and false or misleading WHOIS information; (iv) 6,204 emails violate 15 U.S.C. §7704(a)(1)(A) because they were sent from domains that were obtained with false or misleading registration information; and (v) 6,204 emails violate 15 U.S.C. §7704(a)(5)(A)(iii) because they include false addresses in the email bodies.

As a result, the court RECOMMENDS that XMission's Motion for default judgment be GRANTED (ECF No. 35) and that judgment is entered against Defendants and in favor of XMission in the amount of $372,240.00 in damages. The court further recommends an injunction is entered against Defendants in this case.

Copies of this Report and Recommendation are being sent to Defendants, who are hereby notified of their right to object.[89] Defendants must file any objection to this Report and Recommendation within fourteen (14) days after being served with a copy of it.[90] Failure to object may constitute waiver of objections upon subsequent review.

---

[89] *See* 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b).

[90] *Id.*

20

DATED this 24th day of August, 2018.

BY THE COURT:

_____

DUSTIN B. PEAD
United States Magistrate Judge

20