UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, CENTRAL DIVISION

ZOOBUH, INC., a Utah Corporation,
 	
     Plaintiff,
 	
 vs.
 	
 BETTER BROADCASTING, LLC., a Utah limited liability company; IONO INTERACTIVE, a company doing business in Utah; DOES 1-40,
 	
     Defendants.
	MEMORANDUM DECISION AND ORDER GRANTING DEFAULT JUDGMENT
	
	 Case No.: 2:11cv00516-DN
	
	 District Judge David Nuffer

Introduction

In this action involving unsolicited commercial email communications, commonly referred to as SPAM, plaintiff, ZooBuh, Inc. moved for default judgment, monetary damages, and a permanent injunction against defendants,[1] alleged spammers and alter egos, Better Broadcasting, LLC and IONO Interactive. ZooBuh was represented by Evan A. Schmutz, and Jordan K. Cameron of the law firm of Hill, Johnson & Schmutz, L.C. located in Provo, Utah.

Statement

The Controlling the Assault of Non-Solicited Pornography and Marketing Act located at 15 U.S.C. §§ 7701-7713 ("CAN-SPAM Act") was passed into law in 2003. Somewhat of a misnomer, the CAN-SPAM Act does not govern non-solicited and pornographic emails only, but rather, in relevant part, prohibits sending any commercial email with header information that is

---

[1] Motion and Memorandum for Entry of Default Judgement, docket no. 28, filed March 1, 2012; Motion to Enter an Order Re Standing and Damages, docket no. 40, filed June 1, 2012.

materially false or materially misleading, and requires the provision of certain content in the email bodies.

Plaintiff, ZooBuh, Inc. ("ZooBuh") was first formed in Utah in 2002 and incorporated in 2007.[2] ZooBuh is an Internet access service which provides email, chat, and blogging services to approximately 35,000 customers worldwide.[3] ZooBuh provides the service through its own equipment.[4]

Between February 18, 2011 and November 7, 2011, ZooBuh received at least 13,453 commercial emails sent and/or initiated by or on behalf of Better Broadcasting and/or Iono, its alter ego,[5] in violation of various sections of the CAN-SPAM Act.

On November 10, 2011, ZooBuh filed a First Amended Complaint[6] against the Defendants seeking statutory damages and a permanent injunction. The Defendants failed to appear and answer the Complaint. This Court entered a default certificate against the Defendants on March 7, 2012.[7] In support of ZooBuh's claims and request for damages, the Court requested that ZooBuh submit supplemental briefing and evidence on the issues of standing, violations of the CAN-SPAM Act, and damages.[8]

Based on the pleadings and evidence presented to it, the Court finds: 1) that ZooBuh is a bona fide Internet access service who was, and is continually, adversely affected by its receipt of SPAM emails, and therefore qualifies for standing as a private plaintiff under the CAN-SPAM

---

[2] Declaration of F. Alan Fullmer (Fullmer Declaration) ¶¶ 2,5, docket no. 43, filed June 1, 2012.
[3] Id. ¶¶ 4, 8.
[4] Id. ¶¶ 12-16.
[5] Id. ¶ 45.
[6] Docket no. 20, filed November 10, 2011.
[7] Entry of Default, docket no. 29, filed March 7, 2012.
[8] Motion to Enter an Order and Memorandum Re Standing and Damages, docket no. 40, filed June 1, 2012; Memorandum in Support of Motion to Enter Order and Memorandum Re Standing and Damages, docket no. 41, filed June 1, 2012.

Act; 2) that the emails in question contain violations of 15 U.S.C. § 7704(a)(1)(A), 15 U.S.C. § 7704(a)(1)(C), and 15 U.S.C. § 7704(a)(5); 3) that the Defendants engaged in practices in violation of § 7704(b)(2); 4) that ZooBuh is awarded damages in the amount of $1,608,360 and a permanent injunction.

<div align="center">**Analysis**</div>

I.   STANDING

It is well established that "the court *sua sponte,* can raise the issue of standing for the first time at any stage of the litigation." *New England Health Care Employees Pension Fund v. Woodruff*, 512 F.3d 1283, 1288 (10th Cir. 2008) (citing *Rector v. City and County of Denver,* 348 F.3d 935, 942 (10th Cir.2003)). The CAN-SPAM Act dictates that a provider of Internet access service "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 by the defendant, or to recover damages. 15 U.S.C. §7706(g)(1). A standing analysis under the CAN-SPAM Act consists of two parts: (1) whether the plaintiff is a *bona fide* Internet access service (*see Gordon v. Virtumundo*, 575 F.3d 1040, 1050 (9th Cir. 2009) (citing 150 Cong. Rec. E72-02)); and, (2) whether the plaintiff is adversely affected by SPAM emails (*see* 15 U.S.C. §7706(g)(1)). Whether a plaintiff has standing is a necessary question that the Court must answer prior to awarding any damages under the statute.

      a. Whether ZooBuh is a Bona Fide Internet Access Service

The CAN-SPAM Act 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."

15 U.S.C. § 7702(11); 47 U.S.C. § 231(e)(4). The Ninth Circuit suggested that standing be

limited to "bona fide" Internet access services, which is defined in the Congressional Record.

"[W]e intend that Internet access service providers provide actual Internet access service to

customers." *See Gordon*, 575 F.3d 1040, 1050 (9th Cir. 2009) (citing 150 Cong. Rec. E72-02).

The Ninth Circuit also suggested that there exists an ownership and control counterpart to being

a bona fide Internet access service. *See Gordon*, 575 F.3d at 1052. *Gordon* held that the plaintiff

did not qualify as an Internet access service despite providing email accounts because

> Gordon [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 e-mail accounts and log-in
> passwords and to 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. *Id.*

Courts have extended the definition of Internet Access Services to "include[ ] traditional [ISPs],

any email provider, and even most website owners." *MySpace, Inc. v. The Globe.com, Inc.,* No.

06-3391, 2007 WL 1686966, at *3 (C.D. Cal. Feb.27, 2007) *see also Facebook, Inc. v. ConnectU

LLC,* 489 F.Supp.2d 1087, 1094 (N.D. Cal.2007).

The Plaintiff, ZooBuh, offers email services, blog hosting, and chat services to its

customers.[9] ZooBuh has customers in all 50 states and in 27 different countries.[10] ZooBuh is

widely recognized as a legitimate email provider and has been featured in various publications.[11]

Unlike the Plaintiff in *Gordon*, ZooBuh owns, maintains and configures all the servers, routers,

and switches on its network through which it hosts and provides its internet access services to its

---

[9] Fullmer Declaration ¶ 4.
[10] *Id.* ¶ 7.
[11] *Id.* ¶ 6.

customers. Every ZooBuh email account is registered, hosted and serviced through ZooBuh's

own hardware. ZooBuh has sole ownership of all the hardware, complete and uninhibited access

to the hardware, and sole physical control over the hardware. ZooBuh also provides each of its

customers with their own web-based email portal (which ZooBuh designed, configured, and

maintains) through which the ZooBuh customers access their selected web-based services (i.e.,

email, blogs, chat.).[12] Accordingly, ZooBuh is a bona fide Internet access service and satisfies

the first part of the standing test under the CAN-SPAM Act.

b. Whether ZooBuh Is Adversely Affected by SPAM

The harm suffered by an Internet access service in order to establish standing under the

"adversely affected" part of the CAN-SPAM Act "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 . . . ." *Gordon*, 575 F.3d at

1053-54. In most cases, evidence of some combination of operational or technical impairments

and related financial costs attributable to unwanted commercial e-mail suffice. See *id*. at 1054.

Such impairments "include, but are not limited to, network crashes, higher bandwidth utilization,

and increased costs for hardware and software upgrades, network expansion and additional

personnel." *Id*. at 1053 (internal citations omitted). The CAN-SPAM Act does not require that a

plaintiff prove that the emails at issue adversely affect the plaintiff, rather, that "[t]he e-mails at

issue in a particular case . . . contribute to a larger, collective spam problem." *See Gordon*, 575

P.3d at 1054.

In *Facebook v. Power Ventures, Inc*., the Northern District of California provided a very

helpful analysis of the "adversely affected" requirement for standing. 844 F. Supp. 2d 1025

(N.D. Cal. 2012). There, the court determined that Facebook's receipt and analysis of

---

[12] *Id. ¶¶* 12-16.

approximately 60,000 messages constituted an adverse effect. *Id.* at 1032. At the time, Facebook's network consisted of 901 million users and Facebook had over 3,000 employees. *See* Facebook "Talking About It."[13] The harm suffered by Facebook with respect to the emails in question was attributable to Facebook's having to spend time and effort to determine the source of the emails, and taking steps to stop the emails. *Power Ventures* 844 F. Supp. 2d at 1031-32. In that case, the court held that Facebook did demonstrate an adverse effect, and that such was especially true because there were a documented 60,000 messages, and "the costs of responding to such a volume of spamming cannot be categorized as 'negligible.'" *Id*. at 1032.

In its ordinary course of business, ZooBuh utilizes SpamHaus, Razor, Pyzor and Spamassassin as a first line of defense for SPAM received on its system.[14] Despite its efforts to mitigate the harmful effects of SPAM, ZooBuh has experienced hardware crashes, server spikes, bandwidth spikes, kernel crashes, and customer complaints all as the result of a collective spam problem of which the emails in question were a part.[15] If not for its continuous receipt of SPAM email, ZooBuh could successfully service all of its approximately 35,000 customers through four servers.[16] Instead, ZooBuh has had to double its server capacity, at significant expense, in order to successfully service its customers. Even with eight servers, ZooBuh consistently deals with server spikes and crashes, and the servers are constantly pushed to capacity, which significantly decreases the life span of the servers and is expensive in power consumption.[17] Under these facts, ZooBuh satisfies the "adversely affected" requirement as stated by the *Gordon* court.

---

[13] https://www.facebook.com/pages/Talking-About-It/213156018796346?hc_location=timeline (last visited May 31, 2013).
[14] *Id. ¶* 17.
[15] *Id. ¶¶* 31-38.
[16] *Id. ¶* 25..
[17] *Id. ¶¶* 29-30.

ZooBuh's network consists of approximately 35,000 users,[18] ZooBuh has three employees,[19] and there are 13,453 emails at issue.[20]   Accordingly, the subject emails created a proportionately greater burden for ZooBuh than the 60,000 emails received by Facebook's 901 million users and over 3,000 employees. Similar to Facebook, for each email, ZooBuh had to expend man-hours and work to identify the source, examine the transmission information, examine and analyze the header information, take efforts to determine how and why the specific emails were able to circumvent and/or bypass preliminary filtering techniques, and to ultimately attempt to make the emails stop. ZooBuh efforts to deal with the spam cannot be categorized as negligible. *See Power Ventures*, 844 F. Supp. 2d at 1032. Under these facts, ZooBuh satisfies the "adversely affected" requirement as stated by the *Facebook* court.

In summary, the harm ZooBuh suffered, and continues to suffer, as the result of its collective SPAM problem is much more significant than the mere annoyance of having to deal with SPAM or the process of dealing with SPAM in the ordinary course of business (i.e., installing a spam filter to flag and discard spam). The harm ZooBuh suffered, and continues to suffer, is manifested in financial expense and burden; lost time; lost profitability; decreases in the life span of ZooBuh's hardware; server and bandwidth spikes; server crashes; and pre-mature hardware replacements. ZooBuh is adversely affected by a collective spam problem, which includes the emails in question, and that the second part of the standing test is satisfied. Therefore, ZooBuh has standing as defined by the CAN-SPAM Act to assert claims as a private party plaintiff.

---

[18] *Id. ¶* 8.
[19] *Id. ¶* 11.
[20] *Id. ¶* 45.

II.   ANTI-SPAM LAWS

Section 7704(a)(1) of the CAN-SPAM Act dictates that

It is unlawful for any person to initiate the transmission, to a protected computer, 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. . . [h]eader information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

15 U.S.C. §§ 7704(a)(1), 7704(a)(1)(C).

Section 7704(a)(1) further dictates that "header information that is technically accurate

but includes an originating electronic mail address, domain name, or Internet Protocol address

the access to which for purposes of initiating the message was obtained by means of false or

fraudulent pretenses or representations shall be considered materially misleading;" 15 U.S.C. §

7704(a)(1)(A). The conduct prohibited by section 7704(a)(1) is referred to in this order as

"Header Violations."

Section 7704(a)(5) of the CAN-SPAM Act dictates that

It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides--(i) clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender.

The conduct prohibited by section 7704(a)(5) is referred to in this order as "Content

Violations." The CAN-SPAM Act provides statutory damages against parties who engage in a

pattern or practice in violation of § 7704(a)(5). 15 U.S.C. § 7706(g)(1).

a.   Whether the Emails Contain Header Violations.

There are several decisions arising out of default judgment and summary judgment

proceedings wherein the courts awarded damages for Header Violations. In those cases, the

various courts determined that Header Violations existed where: the emails failed to identify that they came from the defendant, *see Tagged, Inc. v. Does 1 through 10*, No. C 09-01713 WHA, 2010 WL 370331 (N.D. Cal. Jan 25, 2010); the emails did not accurately identify any party, *see Facebook v. Wallace*, No. C 09-798 JF (RS), 2009 WL 3617789 (N.D. Cal. Oct. 29, 2009); and, the emails contained inaccurate sender names, *see Power Ventures,* 844 F. Supp. 2d at 1034-35. Though these decisions are helpful, they do not provide much analysis. Accordingly, it is helpful to look outside of CAN-SPAM decisions for direction on the interpretation of the statute.

California Business and Professions Code § 17529.5(a)(2) is substantially similar to § 7704(a)(1) of CAN-SPAM in that it prohibits commercial email which "contains or is accompanied by falsified, misrepresented, or forged header information." Cal. B&P Code § 17529.5(a)(2). Though the language is similar to the CAN-SPAM Act, the California code has been defined as prohibitive of "deceptive" header information only, thereby creating a more onerous burden on a plaintiff than the "materially misleading" standard of the CAN-SPAM Act and thereby avoiding pre-emption by the CAN-SPAM Act. *See Hypertouch v. Valueclick, Inc.*, 192 Cal. App. 4th 805, 825-830 (2011); *Asis Internet Services v. Subscriberbase Inc.*, No. 09-03503 SC, 2010 WL 1267763 (N.D. Cal. Apr. 1, 2010).

In consideration of the California Code's more onerous burden, the recent California appellate decision in *Balsam v. Trancos* is persuasive as to what constitutes a Header Violation under CAN-SPAM. 138 Cal. Rptr, 3d 108. (Cal. Ct. App. 2012). In *Trancos*, the plaintiff sued an email marketer, similar to Defendants in this case, for sending eight commercial email advertisements on behalf of companies that hired the defendant. *Id*. at 112. Before sending the emails, the email marketer privately registered the domains it used to send the emails with a proxy service. *Id*. at 112-13. The proxy service, in turn, displayed the proxy service's contact

information on the domain name registration records instead of the defendant's contact information. *Id.* . A recipient seeking to determine who sent the emails could not determine the sender because the domains were cloaked and a WHOIS look-up would reveal the proxy service's contact information and not that of the defendant. *Id.* at 118-23.

The appellate court applied CAN-SPAM's definition of header information and, noting CAN-SPAM's parallel provision to B&P Code § 17529.5(a)(2), the Court agreed that where the domain names in the emails did not represent a real company and could not be readily traced back to the sender, through available public databases such as WHOIS, such constituted falsification or misrepresentation for purposes of the statute. *Id.* at 122-23. As to privately registered domain names, the Court held "where, as in this case, the commercial e-mailer intentionally uses privately registered domain names in its headers that neither disclose the true sender's identity on their face nor permit the recipient to readily identify the sender . . . such header information *is* deceptive and *does* constitute a falsification or misrepresentation of the sender's identity," thereby meeting the more strict standard of the California Code. *Id.* at 118.

Because the California anti-spam statute has not been preempted, prohibits deception, and imposes a more onerous burden on a plaintiff than does the CAN-SPAM Act, the *Trancos* analysis reasonably extends to the CAN-SPAM Act. Accordingly, where an email contains a generic "from" name and is sent from a privacy-protected domain name, such that the recipient cannot identify the sender from the "from" name or the publicly available WHOIS information, such is "materially misleading" and is a violation of 15 U.S.C. § 7704(a)(1)(C).

In this case 13,333 of the emails contain a generic or nonsensical "from" line that does not identify any real business or individual. Examples of the "from" lines include: "Accounting Degree," "Add a Sunroom," "Adult Education," "Air Conditioner," "Airline Tickets," "Ink

Cartridges," and "Ultrasound Technician."[21]   Additionally, each of the 13,333 emails originated from a sender domain that was privacy-protected.[22]   Therefore, when a recipient of the email sought to identify the emailer through the publicly available WHOIS database, the WHOIS database record displayed the proxy service's contact information on the domain name registration records instead of the emailer's contact information, thereby preventing the recipient from identifying the emailer.[23]   Each of these 13,333 emails violates 15 U.S.C. § 7704(a)(1).

Header Violations under the CAN-SPAM Act are not limited to false or misleading header information. Under 15 U.S.C. § 7704(a)(1)(A), even header information that is technically accurate violates the CAN-SPAM Act when the email "includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations." 15 U.S.C. § 7704(a)(1)(A).

When a party registers a domain name with an ICANN compliant domain registrar, that registrant enters into a registration agreement with the domain registrar. In most, but not all cases, the domain registration agreement and the accompanying Terms and Conditions (collectively "Registration Documents") prohibit the use of the registered domain to send unsolicited commercial email or engage in other SPAM practices.[24]   Accordingly, in order to obtain the domains from the registrar, the registrant represents that it does not intend to use, and will not use, the domains for any purpose prohibited by the Registration Documents. If, as is the case here, the registrant does intend to use the domains for prohibited purposes, the registrant

---

[21] See list attached as Exhibit C to Fullmer Declaration.
[22] Declaration of Bryceson Ringwood (Ringwood Declaration) ¶ 9, docket no. 42, filed June 1, 2012.
[23] *See id.* ¶¶ 8-9.
[24] See eNom Registration Agreement and Abuse Policy, attached as Exhibit E. to Fullmer Declaration; Moniker Registration Agreement, attached as Exhibit F. to Fullmer Declaration.

obtained the domains under a false pretense, and the sending of any email in violation of the

Registration Documents violates 15 U.S.C. § 7704(a)(1)(A) on a per email basis.

In this case 13,452 of the emails originated from sender domain names registered with

eNom, Inc. and one email originated from a sender domain registered with Moniker Online

Services, LLC.[25]   Each of these registrars requires the party registering the domain to accept its

Registration Documents. The Registration Documents of each registrar contain a provision

whereby the registrant indicates that they will not use the domain name for purposes of sending

unlawful commercial email or SPAM. Accordingly, in order to obtain the domain names used to

send the emails in question, the Defendants represented to the domain registrars that the domain

names would not be used for SPAM purposes. However, the domain names were intended to be

used, and were used, for SPAM purposes. Consequently, the Defendants obtained the sender

domains, from which they sent 13,452 emails, under false and fraudulent pretenses in violation

of § 7704(a)(1)(A).

b. Whether the Emails Contain Content Violations.

The CAN-SPAM Act requires that any commercial electronic mail message provide (i)

clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear

and conspicuous notice of the opportunity to decline to receive further commercial electronic

mail messages from the sender; and (iii) a valid physical postal address of the sender. 15 U.S.C.

§ 7704(a)(5) (collectively "Required Content").

A determination of whether an email contains a Content Violation turns on the

interpretation of the term "clear and conspicuous." In a commercial communication through an

electronic medium "clear and conspicuous" is defined as follows: the "disclosure must be

unavoidable . . . [and] [a]ny visual message shall be of a size and shade, with a degree of contrast

---

[25] Ringwood Declaration ¶ 10.

to the background against which it appears, and shall appear on the screen for a duration and in a location sufficiently noticeable for an ordinary consumer to read and comprehend it." *F.T.C. v. Affiliate Strategies, Inc.*, No. 5:09-CV-04104-JAR-KGS, 2011 WL 3300097, *2 (D. Kan.Aug. 1, 2011).

The question presented to the Court in this case is whether Required Content provided in the emails through a remotely hosted image is clearly and conspicuously displayed. This Court determines that it is not.

The body of an email message can be drafted as text only, HTML, or both by using the MIME protocol.[26] Text emails are "plain text," which means there is no formatting, such as fonts, sizes, and colors. Every email client, even one with the most strict security settings, would likely be capable of reading text emails.[27] HTML allows a message to specify font families, sizes, colors, and to have italic, underline or bold letters. Email clients that are configured to read HTML will also read and display text, as HTML-capable email clients are capable of reading and displaying plain text. In contrast, email clients that are only capable of reading text, or email clients that are only configured to read text, will not read and display HTML.[28]

MIME is an Internet standard that extends the format of email to support message bodies with multiple parts. MIME is specified in six linked RFC memoranda: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049.2.[29] Because MIME extends the format of

---

[26] Letter of Opinion of F. Alan Fullmer (Fullmer Opinion) ¶ 22, docket no. 38, filed May 31, 2012. For an explanation of these terms, see Fullmer Opinion ¶¶ 1-5.

[27] *Id.* ¶¶ 23-24.

[28] *Id.* ¶¶ 26, 28-29.

[29] *Id.* ¶ 30. The RFC protocols together define email specifications for all Internet users. The Internet Engineering Task Force ("IETF") codifies standardizing decisions which are then published in Request for Comments ("RFC"). Many RFCs are the standards on which the Internet is formed. By way of example, the Internet Email RFC standards include: RFC 2049, which defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the MIME, redefines the format of messages to allow for: (1) textual message bodies in character sets other than US-ASCII; (2) an extensible set of different formats for non-textual message bodies; (3)

email to support message bodies with multiple parts, MIME allows email to be drafted in a

manner that the email can be read in more than one format. For example, using the MIME

protocol, an email can be drafted to have a text part, a HTML part, or both. MIME also allows

the emailer to include images as part of the message. There are three main types of images that

can be included within an email: "Attached," "Inline," and "Remote."[30] At issue in this case are

Remote images. Remote images are not part of the email body, but rather a link to a web server

that could be anywhere on the Internet and controlled by any unknown third party. [31]

The United States Department of Homeland Security through the United States Computer

Emergency Readiness Team ("US-CERT") is charged with providing response support and

defense against cyber-attacks for the Federal Civil Executive Branch and with information

sharing and collaboration with state and local government, industry and international partners.

US-CERT interacts with federal agencies, industry, the research community, state and local

governments, and others to disseminate reasoned and actionable cyber security information to

the public. US-CERT repeatedly warns against downloading remotely-hosted images in

email. [32] In the National Cyber Alert System, Cyber Security Tip ST04-007, US-CERT advised

as follows:

> Disable the automatic downloading of graphics in HTML mail – Many spammers send
> HTML mail with a linked graphic file that is then used to track who opens the mail
> message—when your mail client downloads the graphic from their web server, they
> know you've opened the message. Disabling HTML mail entirely and viewing messages
> in plaint text also prevents this problem.

National Cyber Alert System, Cyber Security Tip ST04-007, 2.[33]

---

multi-part message bodies, and (4) textual header information in character sets other than US-ASCII. (Fullmer
Opinion at 5, footnote 2.
[30] *Id.* ¶¶ 31-32.
[31] *Id.* ¶¶ 35.
[32] *Id.* ¶¶ 44-46.
[33] *Id.* ¶ 47. . This document is attached to the Fullmer Opinion as Exhibit C.

In the document entitled *Recognizing and Avoiding Email Scams*, US-Cert again warns "[t]here are a number of ways you can configure your email client to make you less susceptible to email scams. For instance, configuring your email program to view email as 'text only' will help protect you from scams that misuse HTML in email." *Recognizing and Avoiding Email Scams*, 8.[34]

Industry also warns of rendering HTML in email messages. In the document entitled *Technical and Policy Requirements for Sending Email to AOL*, AOL warns emailers that they will not support many of the features of HTML.[35] AOL also states that "[o]ne reason [the client does not support all features of HTML] is because of the security hazards involved with sending HTML e-mails. These e-mails can expose the unwary user to hostile viruses or other intrusive programs. . . . The common theme here is end-user security. Malicious e-mailers can bury a wide variety of harmful actions within the HTML e-mail, including programs that activate upon download." *Technical and Policy Requirements for Sending Email*, 2-3.[36]

In addition to the security threats inherent in remotely hosted images and the industry standards which typically prevent the display of remotely hosted images in email messages, remotely hosted images are not permanent. If the remotely hosted image no longer exists on the hosting server for any reason, then the image cannot be downloaded to the email client and can never be viewed by the recipient. Remotely hosted images typically do not have a very long shelf-life which means there is a small window of time where the image is viewable by the recipient. [37]

---

[34] Fullmer Opinion ¶ 49. This document is attached to the Fullmer Opinion as Exhibit D.
[35] Fullmer Opinion ¶ 50. This document is attached to the Fullmer Opinion as Exhibit E.
[36] Fullmer Opinion ¶ 51.
[37]*Id.* ¶¶ 36-37.

Given the strong concerns and recommendations against the downloading of remotely hosted images in emails, the industry standards that prevent the automatic download of Remote images in email, and the non-permanent nature of Remote images, the content of remotely hosted images in email communications is not unavoidable and is not likely to appear on the recipient's screen for a duration and in a location sufficiently noticeable for an ordinary consumer to read and comprehend it. *See F.T.C. v. Affiliate Strategies, Inc.*, 2011 WL 3300097, at*2. This opinion does not address what would constitute a "clear and conspicuous" provision of the Required Content, it merely addresses what is not. It is the opinion of the Court that there are many ways that an emailer could provide the Required Content in a "clear and conspicuous" fashion that would not include the use of Remote images.

In this case none of the Required Content appeared to be provided in the emails in any way. Nevertheless, if the Required Content was provided, it was through remotely hosted images, which images would be blocked by the majority, if not all, email clients, which images would only exist for a short time on a third party server, and which images would not likely be viewed by a recipient. In fact, at the time the emails were received and reviewed by the Plaintiff, none of the Remote images were viewable.[38] Accordingly, none of the emails in question provided clearly and conspicuously displayed Required Content and every email violates 15 U.S.C. § 7704(a)(5). Because all of the email in question violates 15 U.S.C. § 7704(a)(5), there is a pattern or practice by the Defendants of violating 15 U.S.C. § 7704(a)(5) and statutory damages are appropriate.

---

[38] [38]*Id.* ¶¶ 61-65, 67-70.

III.   DAMAGES

Under the CAN-SPAM Act, a plaintiff may elect to recover monetary damages in an

amount equal to the greater of actual losses or statutory damages. 15 U.S.C. § 7706(g)(1)(B). It

is well established that "[a] plaintiff may elect statutory damages regardless of the adequacy of

the evidence offered as to his actual damages and the amount of the defendant's profits . . . and 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."

Facebook. v. Wallace, 2009 WL 3617789 at *2 (citing *Columbia Pictures Television, Inc. v.*

Krypton Broad. of Birmingham, Inc., 259 F.3d 1186, 1194 (9th Cir. 2001)) (internal quotations

omitted).

In this case, ZooBuh elected to recover statutory damages pursuant to 15 U.S.C. §

7706(g)(3)(A) which are calculated by multiplying the number of violations by up to $100 in the

case of Header Violations and up to $25 in the case of Content Violations.

15 U.S.C. § 7706(g)(3)(A).

In *Wallace*, the court awarded the plaintiff $710,737,650 in damages. 2009 WL 3617789

at *2. The damage award was calculated by multiplying the number of emails by "$50.00 per

violation of the CAN-SPAM Act." *Id*. In determining to award $50.00 per violation, the court

looked at various factors. Specifically, the court stated that "[t]he record demonstrates that

Wallace willfully violated the statutes in question with blatant disregard for the rights of

Facebook and the thousands of Facebook users whose accounts were compromised by his

conduct." *Id*. Wallace's conduct included violating a temporary restraining order and

preliminary injunction. *Id*. Though the defendant's actions were severe, the court did not

believe that the actions merited an award in excess of seven billion dollars. *Id*. Accordingly,

instead of awarding the full $100 per violation and treble damages, the court scaled back its award to $50 per violation.

In *Tagged*, the court awarded the plaintiff $151,975 for 6,079 emails sent by the defendant.   2010 WL 370331, *12. There, the court awarded $25 per email because the defendant sent only 6,079 emails compared to the greater number of spam messages sent in other cases which had given larger damages awards. *See id*. at 11.

In *Asis Internet Services v. Rausch*, the Court awarded the plaintiff $865,340 for various violations of 15 U.S.C. § 7704(a)(1) (which carries up to a $100 penalty) and 15 U.S.C. § 7704(a)(2) (which carries up to a $25 penalty).   2010 WL 1838752, *7 (N.D. Cal. May 3, 2010). Specifically, the court awarded $25 per violation of 15 U.S.C. § 7704(a)(1) and $10 per violation of 15 U.S.C. § 7704 (a)(2). The court compared the case to *Wallace* and stated that "[t]his case involves far fewer emails than in [*Wallace*]." *Id* at *7. Further, the defendant "did not willfully violate an injunction" as was the case in *Wallace*. *Id*. After pronouncing the base award, the court considered the evidence that the defendant had also engaged in dictionary attacks and automated scripting in violation of 15 U.S.C. § 7704(b). *See id*. at *8-9. Based on that fact, the court awarded treble damages as allowed by the statute for a total damage award of $2,596,020. *Id*. at *9.

The instant case is most similar to *Asis*. Here, there are 13,453 commercial emails in question, each containing one or more violations of the CAN-SPAM Act. Specifically, there are 13,333 emails that violate 15 U.S.C. § 7704(a)(1)(C) (which carries an up to $100 penalty), 13,453 emails that violate 15 U.S.C. § 7704(a)(1)(A) (which carries an up to $100 penalty), and 13,453 emails that violate 15 U.S.C. § 7704(a)(5) (which carries up to a $25 penalty). The emails also contain significant evidence of other spamming practices, which illustrate the willful

nature of the violations. Such practices include, but are not limited to, the registration of many

.info domain names, image tracking, Bayes Poisoning, scripting, etc.[39] Accordingly, this Court

applies the *Asis* standard and awards $25 per violation of 15 U.S.C. § 7704(a)(1)(C) and §

7704(a)(1)(A), and $10 per violation of 15 U.S.C. § 7704(a)(5) for a total base damage award of

$804,180.

Under the CAN-SPAM Act, the Court can award aggravated damages where the

defendant "use[d] scripts or other automated means to register for multiple electronic mail

accounts or online user accounts from which to transmit to a protected computer, or enable

another person to transmit to a protected computer, a commercial electronic mail message."

15 U.S.C. § 7704(b)(2); 15 U.S.C. § 7706(g)(3)(C). Under these circumstances "[t]he court may

increase a damage award to an amount equal to not more than three times the amount otherwise

available." 15 U.S.C. § 7706(g)(3)(C).

In this case, there is significant evidence that the Defendants used an automated process

through which to create the sender email addresses from which to send the emails in question.

Specifically, the sender email addresses, when viewed alphabetically, demonstrate a pattern of

words selected in an ascending alphabetical order. Additionally, some of the words cross

domain names, indicating that the same script generated the domains by using a dictionary file.[40]

Such practices violate 15 U.S.C. § 7704(b) and entitle a plaintiff to treble damages. 15 U.S.C. §

7704(b)(2); 15 U.S.C. § 7706(g)(3)(C); *Asis*, 2010 WL 1838752 at *9. Accordingly, this Court

exercises its discretion to double the statutory damage award and applies the *Asis* standard for a

total damage amount of $1,608,360..

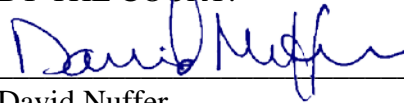---

[39]*Id.* ¶ 66.
[40] [40]*Id.* ¶ 66.

Under the CAN-SPAM Act, the Court can enter an injunction to enjoin further violations by the Defendants. *See* 15 U.S.C. § 7706(g)(1)(A). ZooBuh has substantially prevailed in this matter and has demonstrated the existence of violations of the CAN-SPAM Act in the emails in question. Accordingly, an injunction is entered against the Defendants in this case. The Defendants shall no longer send any commercial email to any ZooBuh customer.

ORDER

ZooBuh's motions for default judgment[41] and for an order regarding standing and damages[42] are GRANTED. Defendants are ordered to pay ZooBuh damages in the amount of $1,608,360. In addition, Defendants are enjoined from further violations of the CAN-SPAM Act.

Dated May 31, 2013.

BY THE COURT:

David Nuffer
United States District Judge

---

[41] Docket no. 28, filed March 1, 2012.
[42] Docket no. 40, filed June 1, 2012.