UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

BEYOND SYSTEMS, INC., Plaintiff, v. KRAFT FOODS, INC., *et al.*, Defendants.	)	Case No. 8:08-cv-00409 (PJM)(CBD)

PLAINTIFF'S OPPOSITION TO DEFENDANTS'
MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

Page

I. INTRODUCTION

Defendants Connexus Corp. ("Connexus") and Hydra LLC[1] ("Hydra") must show, to obtain summary judgment, that on the material facts that are not in dispute, Defendants deserve judgment as a matter of law. Defendants have failed to meet either their legal or factual burdens: (1) Defendants contend that BSI does not have statutory standing but concede that BSI provides services to its customers that meet the definition of an ISP under the statutes, and that it uses its own equipment to provide these services – the *sine qua non* of an ISP; (2) the Maryland and California anti-spam statutes are not preempted because CAN-SPAM expressly exempted state laws prohibiting falsity and deception in emails; (3) neither the Maryland nor the California statutes establish consent by the ISP as a defense, and no consent was given; (4) Defendants' theory that falsity and deception are actionable only if it affects a consumer's buying decision has no basis in law and ignores the purpose of the anti-spam statutes to discourage spam and to enable the targets of spam to protect themselves; therefore, falsity and deception that obscure the sender's identity, are designed to evade filters and/or dupe recipients into opening emails are material; and (5) Defendants contention that their emails do not violate the state statutes are insufficiently specific to serve as a basis for summary judgment.

II. FACTUAL BACKGROUND

Defendants are advertisers in and senders of commercial email. In addition to sending email themselves, Defendants also use "affiliates" to hit the "send key." Defendants contract with merchants who seek to attract potential customers to their websites.[2] Defendants receive

[1] Plaintiff herein submits this Opposition to Defendants' jointly-filed motion; however, because (1) Hydra's counsel has moved to withdraw, (2) Hydra has gone into receivership and transferred its assets to a successor company – Hydra Group LLC – with no notice to Plaintiff, and (3) because Hydra as a corporate defendant must be represented, it is Plaintiff's position that it should not be required to respond to Hydra's motion unless it retains new counsel.

[2] Ex. 1, Hydra's Resps. to Pl.'s First Set of Req. for Admission ("RFA") Nos. 3 & 4 (admitting Hydra's affiliates get paid for sending emails and Hydra contracts with advertisers in connection with commercial emails); Ex. 2,

payment from the advertiser when the customer takes the specified action on the merchant's website – be it a sale, providing a "lead," signing up for an offer, or something more. Defendants work with their clients to design the advertising in the emails, and then make the advertising available to their legion of "affiliates" through their password-protected websites.[3]

At this point, however, the similarity to the traditional advertising agency ends. Defendants contract with "spammers," whom they call affiliates, to send emails.[4] The affiliates go into Defendants' websites and receive the advertising content, instructions and payout information.[5] They also receive Subject lines and From lines for use in the ads – content alleged to be false and deceptive, as well as tracking/sales links, and opt-out links.[6] The affiliates then send the emails to lists of addresses generally several million names long.[7] Defendants typically host the images on their servers, meaning that when the email is received and opened, the image the recipient sees – *i.e.*, the pictures in the advertising in the email – are downloaded by the

---

Connexus' Resps. to Pl.'s First Set of Req. for Admission ("RFA") Nos. 3 & 4 (admitting Connexus' affiliates get paid for sending emails and Connexus contracts with advertisers in connection with commercial emails); Ex. 3, Hydra's Am. & Suppl. Resp. to Pl.'s First Set of Interrogs., Nos. 2 and 3 (identifying insertion orders as H00004593-4644); Ex. 4, Connexus' Am. & Suppl. Resp. to Pl.'s First Set of Interrogs., Nos. 2 & 3 (identifying insertion orders as C00000399-723, C00012274-12436, C00012836-12849, C00012852-12855, C00012863-12866).

[3] Ex. 5. Stafford Dep. at 53:17-54:1; Ex. 6, Steele Dep. at 24:24-25:11; Ex. 7, email from Hydra to affiliate Alchemy Digital Media (showing Hydra advertising the campaigns available on its site to its affiliates and pushing campaign recommendations).

[4] Ex. 1, Hydra's Resps. to RFA Nos. 1, 2, 25 (admitting Hydra and Hydra affiliates send commercial emails; "approved" Hydra "affiliates go into the Hydra Network and choose ad campaigns to send with regard to "campaigns approved for email distribution"); Ex. 2, Connexus' Resps. to RFA Nos. 2, 25 (admitting Connexus' affiliates send commercial emails; "approved" Connexus "affiliates go into the Connexus Network and choose ad campaigns to send with regard to "campaigns approved for email distribution") Ex. 5, Stafford Dep. at 53:9-54:1; Ex. 8, Gadde Dep. at 49:1-50:12.

[5] *Id.*; Ex. 9, Krelle Dep. at 32:19-36:22, 78:6-24; Ex. 10, Nugent Dep. at 43:13-45:4; Ex. 5, Stafford Dep. at 53:9-54:1; Ex. 8, Gadde Dep. at 49:1-50:12.

[6] Ex. 5, Stafford Dep. at 56:24-57:4; Ex. 11, sample Hydra campaign database page at H00004645-4647.

[7] For example, Connexus' affiliate MailCompanyX (against which this Court has entered a default in Case No. 09-00080 (PJM)) has over 300 *million* email addresses in its database. Shin Decl. ¶ 12; Ex. 2, Connexus' Resps. to Pl.'s First Req. for Admissions No. 72.

recipient's computer directly from the Defendants' servers.[8] The emails contain tracking/sales links, which, when you click on them, direct and re-direct you across the Internet, through a series of servers – from the spammer's, to Connexus' or Hydra's, and then to the advertiser's site. The path to the advertiser's site necessarily includes a stop through Defendants' servers so that they can record, using encoded information in the tracking/sales links, which affiliate sent that email, which campaign the email is a part of, and which advertiser sponsored that campaign.[9] From there, the recipient is directed to the advertiser's site. If he buys something or provides a lead or takes whatever action is required under the parties' contract, the advertiser's site fires a "pixel" – *i.e.*, sends a message back to Defendants telling them that the action was consummated, and noting the affiliate's ID and the campaign ID.[10] With this information, Defendants know how much they are owed from the advertiser for generating "x number" of leads at "$y" per lead, how much they in turn owe the affiliate – and what Defendants' cut is.[11]

Email advertising is virtually free to send, a fact that has led to abuses by spam purveyors who are indifferent to the complaints and costs spam generates because the abuses increase the number of mailboxes penetrated, and therefore profits. Case in point: BSI has received *over 20,000 emails from Hydra since the filing of this lawsuit*, and continues to receive spam from

[8] Ex. 9, Krelle Dep. at 32:15-36:22; Ex. 8, Gadde Dep. at 49:3-10; Ex. 12, PDF rendering of sample Hydra HTML creative from H10881 and associated source code (demonstrating Hydra's hosting of images).

[9] Ex. 1, Hydra's Resps. to RFA Nos. 147-153, 209.

[10] Ex. 1, Hydra's Resps. to RFA No. 13; Ex. 2, Connexus' Resps. to RFA No. 13.

[11] Ex.12, Hydra's Resps. to RFA Nos. 5 & 6 (admitting Hydra assigns an identification number to each affiliate and advertiser); Ex. 2, Connexus' Resps. to RFA Nos. 5 & 6 (admitting Connexus assigns an identification number to each affiliate and advertiser); Ex. 13, Whitridge Dep. at 35:17-36:8; Ex. 8, Gadde Dep. at 43:19-46:7.

Hydra as of this morning![12] If Hydra cared about compliance or this lawsuit, it would, as it easily could, instruct its affiliates to stop spamming BSI or terminate those affiliates.[13]

In an effort to curtail these abuses, state legislatures and then Congress prohibited some of the most widely-used practices designed to avoid filters and induce recipients into opening unwanted emails. Congress found that falsified headers "not only trick ISP's increasingly sophisticated filters," but "lure consumers into mistakenly opening messages from what appears to be people they know," and that senders use false or misleading Subject lines to "trick the recipient into thinking that the e-mail sender has a personal or business relationship with the recipient." S. Rep. No. 108-102, at 4, *reprinted in* 2003 U.S.C.C.A.N. at 2350.

This deceptiveness is directly related to spam's elusiveness. "The single greatest challenge for anti-spam law enforcement is to identify and locate the source of a particular spam campaign." *FTC Report: A CAN-SPAM Informant Reward System: A Report to Congress* at 10 (Sept. 2004) (hereinafter, "FTC Report"). The FTC reported to Congress that spammers are exceedingly difficult to identify because they obscure their identities: "Spammers routinely employ a variety of obfuscation techniques to conceal the source of their email." *Id*. at 10-11. The California legislature found that "[s]pam filters have not proven effective." because "[m]any spammers have become so adept at masking their tracks that they are rarely found, and are so technologically sophisticated that they can adjust their systems to counter special filters and other barriers against spam . . . ." Cal. Bus. & Prof. Code § 17529(f), (i). For these reasons, the anti-spam laws are most concerned with the sending of emails with falsity that obscures the

[12] Hydra spam from February 18, 2010 (Ex. 14).

[13] *See* Ex. 15, Dec. 7, 2009 Hrg. Tr. at 27-28 (inaccurately representing that Hydra has suppressed BSI's addresses). As this Court also knows, Hydra is trying to use a sham corporate change in identity to escape this litigation. *See* DE#s 280 & 287.

identity of the sender, falsity designed to evade filters, and falsity that is designed to cause recipients to open unwanted messages.

III. RESPONSE TO DEFENDANTS' STATEMENT OF UNDISPUTED FACTS

The allegations about BSI's "legitimacy" as an ISP are the focal point of Defendants' "undisputed facts." Because each material fact in support of those allegations is genuinely disputed, the fundamental requirement for granting a motion for summary judgment - that there is no genuine dispute of material fact – is absent here.

1. Defendants assert as an undisputed fact that "BSI is a lawsuit factory." Mot. at 3. To the extent that this is a factual assertion rather than aspersion, it is disputed.[14] P. Wagner Decl. ¶¶ 2-16.

2. Defendants assert as an undisputed fact that BSI is not a legitimate ISP. Mot. at 3-5. However, Defendants do not argue BSI does not provide services or have customers, therefore, the "legitimacy" of BSI, as a provider of services to customers, is not in issue. Nonetheless, BSI states that since its incorporation in 1996, it has engaged in the business of providing Internet-related services to the public. P. Wagner Decl. ¶¶ 2-16. Since 1996, BSI has provided multiple Internet-related services including, for example, email receipt, filtering and delivery. *Id*. ¶ 3. Currently, BSI receives approximately 1 million emails per day and delivers the legitimate emails to its customers. *Id*. ¶ 26. Besides email services, BSI also hosts web sites, DNS servers, streaming media services and e-commerce services, hosts the domains of its customers on its servers, and provides Internet-related technology consulting. *Id*. ¶¶ 6-9, 11-15, 22; Ex. 16, P. Wagner Dep. at 24:22-28:14.

[14] Plaintiff has inserted paragraph numbers to correlate with factual assertions for the convenience of the Court.

3. Since Defendants do not argue that BSI does not provide services or have customers, their "legitimacy" argument must be limited to asserting that BSI is not legitimate because it has an improper motive for bringing suit. This is not a factual premise, but merely Defendants' opinion. The factual predicate for BSI's lawsuit is clear: the spam emails Defendants sent and BSI received in the course of its ISP activities. The relevance of BSI's motivation to sue with regard to BSI's "legitimacy" is disputed, but is not a factual matter in any event. *See infra* section IV(A).

4. Defendants assert as an undisputed fact that BSI is not a legitimate ISP because Paul Wagner has dedicated significant time to this litigation. Mot. at 3. Plaintiff disputes Defendants' assertion generally, and in particular that it has bearing on BSI's ability to bring this suit. That the principal of a small business would be substantially occupied by contentious litigation that has involved intensive discovery and which is highly technical in nature is not surprising. Mr. Wagner, as an MIT graduate with a physics and mathematics background, has an in-depth understanding of email technology and has worked closely with the attorneys on these issues. Defendants misleadingly cite Mr. Wagner's testimony to suggest that the statement "all of BSI activity sort of relates to litigation" should be construed as an admission of "illegitimacy." Mot. at 3. However, as Mr. Wagner explains, "[s]ome weeks are extremely busy doing this kind of stuff and other weeks I'm doing consulting work or just trying to keep things operational, updating infrastructure…" Ex. 16, P. Wagner Dep. at 405:20-406:1. "There is a lot of time spent keeping servers running and restoring servers that have crashed. And yeah, so addressing problems as being apart from the lawsuits. So I don't know, but it varies week by week." *Id*. at 162:20-163:8. Most importantly, however, Mr. Wagner has had to spend a very substantial

amount of time uncovering and analyzing Defendants' connection to 74,000 deceptive emails. P. Wagner Decl. ¶ 17.

5. Defendants assert as an undisputed fact that BSI is not a legitimate ISP because "BSI's only profit center since 2001 is litigation proceeds." Mot. at 3. First, it is unclear what a "profit center" refers to, but regardless, this bald assertion of fact is disputed. Defendants blatantly misrepresent Plaintiff's interrogatory response which plainly show that for 2000-2008, BSI generated [redacted] in gross revenue – not including any litigation proceeds – and has expended [redacted] in Internet business related costs. BSI's expenditures graphically evidence its investment in running its business. Ex. 17.

6. Defendants attempt to argue that BSI is not a legitimate ISP by impugning Hypertouch. Mot. at 4. Defendants raise no actual facts about Hypertouch as an ISP, but speculate over motives for suing spammers. To the extent that Defendants' red herring needs further explanation, much of what Hypertouch has received in settlements he has given to charity. J. Wagner Decl. ¶ 13. Hypertouch is an ISP providing Internet services to its customers and receives a large amount of spam as a result. *Id.* ¶ 1; *see Hypertouch, Inc. v. Kennedy-Western Univ.*, No. C04-05203 SI, 2006 WL 648688, at *4 (N.D. Cal. Mar. 8, 2006). Ironically, Defendants raise the issue of motives while they have themselves sued Hypertouch in a third-party action alleging that it shares some portion of *Defendants' own liability* for having sent the emails at issue to BSI.

7. Defendants allege that BSI and Hypertouch have "sued over identical emails." Mot. at 4. Defendants do not identify any such emails. Their tactic seems to be to suggest these emails relate to them, but, even if the statement were true, none of those emails relate to Defendants or their liability – that "issue" relates to the Kraft Defendants and the terms of a

settlement agreement with Hypertouch only, and is a disputed fact in any event. Therefore, it is not a fact that has bearing on this motion. Further, each ISP that handles the spam emails has a separate right of action.

8. Defendants assert as an undisputed fact that BSI "intentionally captured" and "archived" the spam. Mot. at 5. By "captured" what Defendants misleadingly mean is that the emails Defendants addressed and sent to BSI's domains were routed to BSI as they should have been and were received, filtered, processed and stored. These functions are normal and proper. *See infra* section IV(A); Levine Decl. ¶¶ 10-15; Klensin Decl. ¶¶ 46-48. BSI disputes that there is anything improper about this, assuming that is Defendants' insinuation in this "undisputed fact." Further, Defendants do not assert that BSI took any direct or express actions to sign up to receive spam. In fact, all of the emails at issue in this case are unsolicited – BSI never opted in or signed up for a single one. P. Wagner Decl. ¶¶ 44-45.

9. Defendants assert as an undisputed fact that Joe Wagner set up addresses and submitted *opt-outs* "knowing that 'alleged' spam would be sent to such addresses." Mot. at 5. First, Joe Wagner knew no such thing, and Defendants' citations provide no support for their statement. Even if the Court were to accept the remarkable argument that taking actions to *avoid* receiving spam is equivalent to *consenting* to spam, first, Defendants fail to allege what opt-outs were used or what emails at issue relate to any such opt-outs, and therefore Defendants assert no basis of summary judgment on any emails. Second, Defendants argument necessarily admits that the opted-out addresses were illegally used by their own affiliates as spam addresses. Third, Hypertouch never opted-in or signed up for a single email. J. Wagner Decl. ¶¶ 8-9. In 2005, Joe Wagner created unique email addresses to use in opt-out requests in order to monitor whether his opt-out requests were honored. Ex. 18, J. Wagner Dep. at 154:4-20. What in fact happened was

that the spammers involved – Kraft – released the address used only for the purpose of the opt-out to spammers, and Wagner began to receive spam at that specific address. J. Wagner Decl. ¶ 11. Defendants further allege that Hypertouch submitted nonsensical addresses to websites. Mot. at 5. Defendants do not identify any such address. In 2005, Joe Wagner filled in some webpages on Connexus' eMarketPanel site to investigate an "incentive offer" (*i.e.*, get a "free" product for signing up) in order to see if the offer could be fulfilled, or whether it was false as suspected. He did not fish for spam: Wagner was gathering information concerning Connexus' practices in support of his allegations of spamming against Connexus and he used "nonsense@example.com" to *prevent* spam at his business addresses. Ex. 18 at 461:6-462:14. Some research is necessary to cut through the multi-layered duplicity of spam. Defendants further allege that the "gotcha@hypertouch.com" address was "created for / on behalf of BSI" to trap spam. Mot. at 5-6. That address was used by Joe Wagner to attempt to opt-out of receiving emails, not to "catch" spam. Ex. 16, P. Wagner Dep. at 350:12-16; 353:7-8 ("So opt out I guess would take – I take to mean to indicate an intention not to receive e-mail at a certain e-mail address."). Opting-out from receiving spam, including to see whether that request will be honored, cannot be construed as seeking spam, and does not provide Defendants a basis for summary judgment on any issue. Defendants' assertion amounts to a damnation of their own practices – that opting-out is such a farce that it is a calculated means to attract more spam.

10. Defendants assert as an undisputed fact that BSI and Hypertouch published addresses. As a factual matter, BSI never published any addresses for the sole purpose of receiving spam. P. Wagner Decl. ¶ 44. Defendants allege that Joe Wagner published addresses on his webpage for "the 'sole' purpose of receiving alleged 'spam' and filing lawsuits." Mot. at 6. Defendants cite nothing to support this statement. In 1999, Hypertouch posted email

addresses on its website *that it specifically wanted no spam sent to*. This was done to comply with then-California law, § 17538.45, which required actual notice to spammers to be legally protected from spam. In essence, Defendants' argument is that the existence of technology such as web crawlers, which bad actors might use for illicit purposes such as illegal address harvesting – a practice explicitly outlawed by Cal. Bus. & Prof. Code § 17529.4 – should have caused Hypertouch to refrain from complying with the law because spammers were likely to steal the addresses, as was done. J. Wagner Decl. ¶¶ 6-7. This argument is meritless and Defendants here neither assert nor support any facts, let alone facts relevant to BSI's legitimacy as an ISP.

11. Defendants assert as an undisputed fact that wildcard addresses are spam traps. Mot. at 6. Again, this is argument, not a fact, let alone an undisputed one. To begin with, Defendants twist what BSI's experts have said. For example, Dr. John Klensin stated: "It's a common practice among many ISPs who create mailboxes whose purpose it is to identify incoming messages as spam in order to detect – well, in order to detect incoming messages as spam." Ex. 19, Klensin Dep. at 190:23-191:17. Dr. Klensin noted that "Microsoft, for example, is rumored to use those very heavily in their filtering systems because if they see particular kinds of message patterns or message sender patterns, show up in those spam trap messages, that information gets introduced into their filtering models." *Id.; see also* Klensin Decl. ¶ 50; Levine Decl. ¶¶ 10, 12. Moreover, BSI did not set up any accounts for the purpose of receiving spam. P. Wagner Decl. ¶ 44; Ex. 20, Resnick Dep. at 145:8-10 ("Q Have you ever seen any evidence that BSI is using a spam trap in this case? A No, I don't believe so."). Resnick Decl. ¶¶ 48-50. Wildcard means that a system can receive any combination of characters left of the "@[domain]." Wildcards have multiple uses unrelated to spam, including creating business-relationship-specific email addresses, such as "rick-applestore@hypertouch.com," delivering

emails to addressees even if the address is in error, or accepting email addresses that might match a particular entity's account or in a particular entity's mailbox, but has no particular relation, among other reasons.[15] Ex. 20, Resnick Dep. at 98:14-99:5; Resnick Decl. ¶¶ 30-31. Such a system is common to many mail providers such as Yahoo, Google and Microsoft.[16] Ex. 22, Levine Dep. at 218:17-219: 10 (testifying he offers wildcard as an option and most businesses take that option). For instance, Yahoo offers small business email accounts featuring "catch-all" email addresses to help their businesses.[17] Wildcards are perfectly legitimate tools. Ex. 22, Levine Dep. at 218:17-219:10; Levine Decl. ¶¶ 13-14; Resnick Decl. ¶¶ 30-31. If there is a factual dispute over whether BSI's use of wildcard email addresses was consent to receive spam, and there should not be, then there exists no basis for summary judgment on this point.

12. Defendants assert as an undisputed fact that BSI "redirected emails intended for others to [itself] knowing they would be 'spam'." Mot. at 6. Again, Defendants misrepresent the issue. BSI reclaimed some accounts that were abandoned because of spam. P. Wagner Decl. ¶ 48. BSI reclaims the accounts so that if legitimate mail comes in it can be forwarded to the former user. *Id.*

13. Defendants assert as an undisputed fact that BSI "facilitated the receipt of emails by 'white listing' addresses" "instead of blocking spam." Mot. at 7. The first part of this statement is an alleged fact, the second an argument (that BSI *should* have to block spam). Defendants do not identify any email that was white listed. *Six emails out of 74,000* contain the header "x-wlist-pattern" indicating automatic white listing by BSI's commercially-purchased

[15] Ex. 21, J. Wagner Deposition in Hypertouch v. Valueclick, et al., at 154:7-155:16.

[16] *See* <http://www.google.com/support/a/bin/answer.py?hl=en&answer=33962> (Gmail offers "catch all" feature for emails), and <http://www.google.com/support/appsecurity/bin/answer.py?hl=en&answer=138313 http://support.microsoft.com/kb/324021> (Microsoft describes how to activate "catch-all" accounts).

[17] *See* <http://help.yahoo.com/l/us/yahoo/smallbusiness/domains/domainfeatures/email/email-03.html> (Yahoo offers "catch-all" feature for small business email).

spam filter – SpamPal, which replaced SpamAssasin as BSI's filter software. SpamPal is factory pre-set to white list domains from which no spam comes for a seven-day period – *i.e.*, trusted sites. Because the spam sent by Defendants and their affiliates is designed to trick filters into thinking it is *not* spam, the filter mistakenly whitelisted these emails without any intervention from Mr. Wagner. Therefore this disputed fact fails to help Defendants in any event. As for whether BSI should be blocking, there is no such requirement and blocking is generally regarded as a bad idea for security reasons.[18] Resnick Decl. ¶¶ 32, 42; Klensin Decl. ¶¶ 45-48; Levine Decl. ¶ 11. Whether an ISP delivers spam to subscribers or sends the message back to its sender, the ISP faces essentially the same burden – it must determine what the message is and where it should be sent. Resnick Decl. ¶ 33; Klensin Decl. ¶¶ 45, 51. In short, it is entirely appropriate, if not preferable, for an ISP to accept all email and not reject suspected spam in order not to lose legitimate email, bounce spam to other innocent parties, or provide spammers information as to what addresses are valid or invalid. Klensin Decl. ¶¶ 48, 51-52; Levine Decl. ¶¶ 11-13; Resnick Decl. ¶¶ 32, 42.

14. Defendants assert as an undisputed fact that BSI agreed to receive and store all alleged spam that Hypertouch sent to BSI. Mot. at 7. BSI owns the hypertouch.com domain. Just as emails to any legitimate citizen might be sent from Google and over Comcast before delivery to that person, when Defendants' affiliates address an email to "[address]@hypertouch.com," in order for that email to arrive at BSI the header routing information in the email directs it to the "flags" raised on the Internet which indicate to a piece of mail what route to follow to get to its destination. In the case of the hypertouch.com domain, that route is first to Hypertouch, Inc. because is the contract receipt point for BSI's

[18] The Maryland statute expressly provides that an ISP "may block" and not be held liable for doing so, obviously meaning that an ISP may choose not to block. Md. Comm. Code § 14-3002(d).

hypertouch.com email. Incoming mail to those addresses is filtered and delivered by Hypertouch to its users, and the rest of the mail is then relayed to BSI for filtering and delivery. For other BSI-owned domains, such as castalia.net, those emails travel over ISPs other than Hypertouch for delivery to BSI, or might go directly to BSI. P. Wagner Decl. ¶¶ 19-21. Hypertouch and BSI have multiple independent reasons for routing the email from its designated receipt point at Hypertouch, Inc. to BSI, only one of which is to archive, including but not limited to: (1) BSI has infrastructure (software and hardware) better able to process and store 1 million emails per day (600,000 daily from Hypertouch); (2) to avoid losing emails when and if there may be errors in the routing tables; and (3) Hypertouch's users sometimes abandon addresses that get swamped by spam, but later learn that a legitimate email was sent to the abandoned address (Hypertouch then asks BSI to search for and retrieve such "false positives" and produces them to grateful clients); (4) BSI has always elected to configure its systems to receive all emails to the domains at which it receives any email as a matter of policy (to be able to create email addresses on the fly to give to vendors and others, to receive misaddressed but legitimate emails, etc.). P. Wagner Decl. ¶¶ 27-28; J. Wagner Decl. ¶ 3. In short, Defendants complain that BSI agreed with Hypertouch to have *its own mail* routed to it, and complain that BSI stored the evidence of Defendants' illegal spamming. On one hand, Defendants criticize BSI for archiving emails because they claim it shows that BSI is a lawsuit factory, but on the other hand criticize BSI for not taking steps to "preserve evidence" in a way that agrees with Defendants' television-inspired "forensic" requirements. Neither position has any merit.

15. Defendants assert as an undisputed fact that all 74,000 emails are invalid, based on four conclusory, inaccurate and misleading bullet points. Mot. at 8. As an initial matter, *this is not a fact in dispute because Defendants concede "that the emails reflect events that BSI*

claims they reflect." Mot. at 9. Thus, at least for the purposes of this motion, the parties concede that the emails are accurate and not "altered," "spoliated," etc. In the event Defendant changes its mind on its concession, Plaintiff continues to assert this fact as true. First, Defendants argue that BSI "knowingly destroyed original emails." Mot. at 8. What Defendants seem to mean is that routing emails from a server and releasing that space from the server to allow normal mail receipt to continue constitutes destruction of emails. This argument has no basis. Klensin Decl. ¶¶ 60-64; Levine Decl. ¶ 19; Resnick Decl. ¶¶ 44-45. Further, Defendants' pseudo-science notion of supposed "original emails," Mot. at 8, is inaccurate and irrelevant – the original emails are those sent by Defendants' spammers. Plaintiff has matched the creatives that Defendants have produced to the emails at issue, conclusively demonstrating that the emails that were received are the emails that were sent.[19] Second, by "altered," they seem to assert that "Received headers" were added to the emails, just as every server is programmed to do. Defendants' negative insinuation has no basis. Klensin Decl. ¶¶ 64; Levine Decl. ¶ 19; Resnick Decl. ¶¶ 18, 20, 43, 45. Third, by "spoliated" they seem to mean that "From separators" were inserted by the email client (in most cases, the Eudora email program) just as every email client does in one form or another. Again, this argument is pseudo-science and is contravened by those qualified to have an opinion. Klensin Decl. ¶ 65; Resnick Decl. ¶¶ 43-45. Fourth, when Defendants refer to "duplicates" they do not account for multiple downloads caused by spam-induced crashes of BSI's servers. Levine Decl. ¶ 21. As for the glitchy emails, as with all computer scripts, BSI's extraction scripts resulted in errors. These errors were isolated and generally limited to two types – misparsed "From separators" caused by text in the emails, and *7 emails out of 74,000* that lacked headers because they were misparsed as a result of a hashbuster greater than 1,000 lines

[19] *E.g.*, Ex. 23, extracted entry from Connexus campaign spreadsheet at C12881.xls; Resnick Decl. ¶ 71 (matching 24,304); Shin Decl. ¶ 29 (matching 20,917 e-mails).

in length inserted by the spammer. Klensin Decl. ¶ 65; Ex. 24, Cohen Dep. at 1154:12-1155:19 ("fabrication error" refers to 7 emails). These few errors do not call into question the validity of 74,000 emails. Levine Decl. ¶¶ 16-20; Levine Dep. at 399:9-400:7 ("vast majority of technical errors are characteristic of spam, not of forged evidence."); Ex. 22, Levine Dep. at 397:4-398:8 ("a handful of the messages" might be duplicates); Ex. 19, Klensin Dep. at 160:4-8. Dr. Klensin's reference to "fatally damaged" emails referred to three emails. Klensin Decl. ¶ 65. Further, what Defendants do not say is that their exhibit print outs of the emails were altered by their own doing – removing lines from the emails – *i.e.*, changing the emails from how they were produced when shown to Plaintiff's experts. Klensin Decl. ¶ 65; Levine Decl. ¶ 17; Resnick Decl. ¶ 43. Finally, Defendants assert that Mr. Resnick stated they were "not stored as email messages." Mot. at 9. Once again, Defendants miscite the transcript. Resnick Decl. ¶¶ 43-45.

16. Defendants assert as an undisputed fact that Paul Wagner was not deceived into buying any goods. Mot. at 9. Wagner was not, but his company's computer systems were deceived into receiving the false emails Defendants sent. Defendants do not address this fact. The fact that ISPs *qua* ISPs do not need to react or respond when establishing a violation of law will be addressed in depth below. *See infra* section IV(C)(3).

17. Defendants assert as an undisputed fact that BSI "manufactured" the claims by searching for emails attributable to Defendants and which contain falsity. Mot. at 9.[20] What Defendants appear to be saying is that once Paul Wagner determined that some particular facet of the emails, such as a domain name, was attributable to them, he searched the emails for that facet. If the asserted fact is an accusation that BSI only encountered the emails at issue when BSI searched for them, that is incorrect. The searches were on emails that had already been

[20] Defendants attempt to make use of a privileged document at 7-8 which Plaintiff requested back once it became aware via this motion that it had been inadvertently produced. It should not be considered as it is the subject of Plaintiff's motion for its return. DE #290. Plaintiff contests the relevance of this non-factual argument anyway.

received. P. Wagner Decl. ¶ 26. Other than complaining that they were caught, it is not clear what Defendants seek to prove with this assertion

18. Defendant asserts additional facts at 13-16. These "facts" are not presented by Defendants as undisputed as they must be on summary judgment, and therefore those facts should be presumed to be disputed, although they are addressed *infra* section IV(A) in any case.

IV. ARGUMENT

A. BSI Has Standing To Sue Under Maryland And California Law.

Although Defendants implicitly concede BSI is an ISP, they assert that Plaintiff lacks statutory standing because, as their argument goes, it is "a lawsuit factory and not legitimate ISP." Mot. at 10. A federal court sitting in diversity and applying state law must decide standing based on what rights state law affords. *Gen. Tech. Applications, Inc. v. Exro Ltd.*, 388 F.3d 114, 118 (4th Cir. 2004). Where standing is raised in the context of summary judgment, the traditional summary judgment analysis is applied and the evidence must be considered in the light most favorable to plaintiff. *Maryland Highways Contractors Ass'n v. Maryland*, Case No. R-89-2410, 1990 U.S. Dist. LEXIS 19238 (D. Md. June 19, 1990) (attached hereto as Ex. 25).

The Maryland and California statutes expressly grant a private right of action to "interactive computer service providers" and "electronic mail service providers," respectively. Md. Comm. Code § 14-3003(3); Cal. Bus. & Prof. Code § 17529.5(b)(1)(A)(ii). BSI is both. Under MCEMA, an "'Interactive computer service provider' means an information service, system, or access software provider that provides or enables computer access by multiple users to a computer service." Md. Comm. Code § 14-3001(c)(1). Under Maryland law, an ICSP is broadly defined, using the same definition as in the Communications Decency Act. *See* 47 U.S.C. § 230(f)(2). Under the CDA, "interactive computer service" has been very broadly construed to include ISPs, as well as a range of other Internet services, such as on-line

newsletters, websites and hosts of websites.[21] *See Batzel v. Smith*, 333 F.3d 1018, 1030 n.15 (9th Cir. 2003) ("a wide range of cyberspace services, not only internet service providers" are "interactive computer services"). Likewise, California broadly defines what constitutes an "electronic mail service provider." An "'Electronic mail service provider' means any person, including an Internet service provider, that is an intermediary in sending or receiving electronic mail or that provides to end users of the electronic mail service the ability to send or receive electronic mail." Cal. Bus. & Prof. Code § 17529.1(h). Services provided to customers define the test and BSI meets all elements. Defendants do not dispute that BSI "provides or enables computer access by multiple users to a computer service" "is an intermediary in sending or receiving electronic mail" and "provides to end users of the electronic mail service the ability to send or receive electronic mail."

Defendants rely on *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040 (9th Cir. 2009) as the basis for their argument Plaintiff lacks standing. In *Gordon*, the court determined plaintiff lacked standing because he was not "adversely affected" as required under CAN-SPAM.[22] 575 F.3d at 1057. The court also found that the plaintiff was not an "Internet access service." *Id*. at 1052. The court gave a narrowing construction to the definition of "Internet access service" based on its reading of CAN-SPAM's legislative history, the fact that CAN-SPAM does not allow individual recipients of emails to sue. *Id*. at 1050. The court's analysis was "heavily

[21] *See, e.g., Universal Commc'n Sys., Inc. v. Lycos, Inc*., 478 F.3d 413, 419 (1st Cir. 2007) (Internet message board website "enable[d] computer access by multiple users to a computer server," namely, the server that hosted the web site, therefore, Lycos, the website operator, was provider of interactive computer service); *Carafano v. Metrosplash.com, Inc*., 339 F.3d 1119, 1123-24 (9th Cir. 2003); *Zeran v. America Online, Inc.*, 129 F.3d 327, 328 (4th Cir. 1997).

[22] Implicit in the 9th Circuit's decision is the finding that plaintiff had constitutional standing, otherwise the court could not have proceeded to consider the merits of the dispute. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 96-97, 97 n.2 (1998) (because constitutional standing is necessary to the court's jurisdiction, as a general rule it must be addressed before proceeding to the merits.).

influence[d]" by the statements of two members of Congress who indicated that only "bona fide" Internet access services should be permitted to sue under CAN-SPAM.[23] *Id*. at 1049-50.

Gordon is inapposite. First, *Gordon* plainly did not hold that plaintiffs have no standing under state law. In fact, *Gordon* acknowledged that the Washington State statute at issue in that case provided a broader statutory standing basis than CAN-SPAM. *Id.* at 1058 (finding "[i]n contrast to the more restrictive standing requirement of the CAN-SPAM Act, the [Washington State statute] authorizes an individual recipient of a commercial e-mail message or an "interactive computer service" to bring a private action."). Maryland and Washington use the same definition of "Interactive computer service [provider]," which the court acknowledged provides a broader basis for standing.[24] *See id.* California also uses an expansive definition, requiring only the provision of email sending or delivery services. Cal. Bus. & Prof. Code § 17529.1(h). In addition, *Gordon* held that CAN-SPAM imposes an "adverse effect" and a "bona fide" requirement. These additional requirements are not found in the Maryland and California statutes. Maryland and California "plainly omitted" an "adverse affect" or "bona fide" requirement.[25] *See id*. at 1069. In any event, BSI is legitimate and harmed as explained herein.[26]

[23] The court did not define what, for purposes of CAN-SPAM, constitutes a "bona fide" Internet access service, but did find that Gordon and his "gordonworks.com" domain did not meet the standard. *See generally id.* at 1051-52.

[24] *Compare* Wash. Rev. Code § 19.190.010(8) *with* Md. Comm. Code § 14-3001(c)(1).

[25] Both states use "bona fide" in other contexts in their commercial codes. Judge Gould recognized in his concurring opinion in *Gordon* this is substantive difference with regard to statutory interpretation. 575 F.3d at 1069. Compare, for example, Md. Comm. Law § 11-204 ("bona fide employees") and Cal. Bus. & Prof. Code § 17701 ("bona fide organization").

[26] Even if an "adverse effect" were required, the Ninth Circuit stated: "It is notable that Congress conferred standing only on adversely affected IAS providers, but not adversely affected consumers. Logically, the harms redressable under the CAN-SPAM Act must parallel the limited private right of action and therefore should reflect those types of harms uniquely encountered by IAS providers." *Gordon*, 575 F.3d at 1053. Logically, therefore, since the Maryland and California legislatures *did not* restrict standing to "adversely affected IAS providers," and included "consumers," the harms redressable under the state statutes are *not* limited to solely "those types of harms uniquely encountered by IAS providers," but also include the ordinary harms affecting consumers.

The legislative histories of the Maryland and California statutes do not provide any basis to narrow standing. The original version of House Bill 915 (which later became MCEMA) did not address ISPs bringing suit. Ex. 26. The Attorney General's Office testified that the bill without standing for ISP's "would have little impact in preventing deceptive spam."[27]; *see also infra* section II(C)(2). The Attorney General's Office urged that the committee amend the bill to take the Washington state approach "which gives consumers and Internet service providers the right to bring an action against the sender of the deceptive e-mail and collect statutory damages." *Id*. California also expanded its then-current law to specifically include recipients and ISPs.

Finally, the facts that animated the Gordon court decision on standing under CAN-SPAM are readily distinguishable from those presented by BSI. Gordon did not own his own computer equipment. *Gordon*, 575 F.3d at 1045. By contrast, BSI has been in business since 1996, prior to the enactment of either the Maryland or California anti-spam statutes, and has purchased its own equipment, buys its own upgraded hardware and software, and provides its services through that equipment from its facilities in Silver Spring, Rockville and Washington, DC. P. Wagner Decl. ¶ 4. Through its equipment BSI provides Internet access (*i.e*., connectivity) services for customers via BSI's dedicated high-speed lines. *Id*. ¶ 11. BSI provides wired and wireless connectivity for residents living near BSI's three Points of Presence. *Id*. ¶¶ 6-7. Unlike Gordon, BSI does not access its services and the Internet "via an ordinary Internet connection," but rather has equipment on site, plus pays hundreds of dollars to three separate upstream providers for "business-" or "ISP"-level connections to its three Points Of Presence in Silver Spring, Rockville and Washington. *Id*. ¶ 4. BSI was founded before there were spam laws, and the majority of its users have been with BSI since before 2004. *Id*. ¶ 2; *see also Gordon*, 575 F.3d at 1056 (citing

[27] Ex. 27, Attorney General's Office letter; the State of Maryland Consumer Protection Division and the Maryland Department of State Police also supported the Maryland bill that became MCEMA. *See* Ex. 28.

Hypertouch, 2006 WL 648688, at *4 n.2 (rejecting argument that Hypertouch was "professional plaintiff" that entered the ISP business for the sole purpose of bringing anti-spam lawsuits)).

"Gordon hosted a domain ("gordonworks.com") on server space he leased from GoDaddy, a domain registrar and web hosting company that also sells e-business related software and services." 575 F.3d at 1045. By contrast, BSI has "physical control over [and] access to the hardware, which [BSI, not GoDaddy] owns, houses, maintains, and configures." P. Wagner Decl. ¶ 4.; *id*. at 1052. "The GoDaddy service allowed Gordon to virtually access the server to manage his domain." *Id*. at 1045. By contrast, BSI owns multiple domains (such as hypertouch.com or castalia.net) which it hosts on its own servers. *Id*. ¶ 7, 10. Besides various email services, BSI also hosts web sites, DNS servers, streaming media services and an e-commerce service (*i.e*., BSI pays $71.95/month to processor Card Services International for its Merchant Account). *Id*. ¶ 7. BSI also hosts the domains of its customers on its servers. *Id*. ¶ 8. BSI hosts 111 domains and websites. *Id*.. For example, it currently hosts websites for Pronto Labels (at http://www.prontolabels.com) and Prince I and Prince II Hotels in Vietnam (at http://www.princehotelhanoi.com). *Id*. ¶ 13. For these customers, this is their business' interface to the Internet and a source of sales and advertising. Moreover, BSI does not rely on a service such as GoDaddy that enables consumers to create e-mail accounts, etc., but rather provides its own similar services. *Id*. ¶ 4.

Gordon was "never compensated for any of his purported Internet services, and his only income source has come from monetary settlements from his anti-spam litigation campaign." 575 F.3d at 1056. By contrast, as BSI's interrogatory responses show, since 2000 it generated over [redacted] in ISP-related gross revenue and expended over [redacted] in ISP-related costs. *See supra* section III(¶ 5). That in and of itself should end the Gordon comparison. While

BSI – like so many companies in the Internet space – might not be profitable, its expenditures graphically evidence its investment in infrastructure to run its business. Further, BSI, like Yahoo and Google, provides free email services for some clients. Provision of free services certainly does not change the fact that big ISPs are "email service providers." *See* 575 F.3d at 1050 n.9.[28]

Unlike Gordon, BSI never "configured the e-mail server to provide an automated response to all commercial e-mail sent to [its] accounts." *Id*. at 1046. P. Wagner Decl. ¶ 46. Also, Gordon "created additional e-mail accounts through the gordonworks.com domain for his "clients" – about six friends and family members." *Id*. at 1045-46. By contrast, BSI has approximately 326 customers and has had upward of 475. *Id*. ¶ 9. Some are family members, some are friends, and others clients. *Id*. ¶ 19. BSI provides email accounts through its hypertouch.com, beyondsystems.net, castalia.net, safemailbox.com, and safemailbox.net domains. *Id*. ¶ 10. BSI handles approximately one million emails per day. *Id*. ¶ 26. In addition, unlike Gordon, BSI provides multiple other services which delineate its identity as an active ISP, such as website hosting, domain hosting, DNS, and secondary services, including back up services supporting the connectivity of the 200-plus users at St. Luke's House. *Id*. ¶ 15.

Gordon "used the accounts he created to monitor for 'data collection' and 'research purposes.'" 575 F.3d at 1046. By contrast, BSI has not set up email accounts purposefully designed as spam traps or repositories. P. Wagner Decl. ¶ 44, although this a common and acceptable industry practice used by, for example, Microsoft. No one would contend that Microsoft's status as an "email service provider" is negated because it uses spam traps – 130,000 of them in fact.[29] The FTC relies upon Microsoft's spam traps in its prosecution of spammers.[30]

[28] (holding district court correctly rejected that providers of free services did not qualify as IAS providers citing Congress' mention of Microsoft's free e-mail service when discussing effects of the increasing volume of spam).

[29] "Microsoft maintains more than 130,000 MSN Hotmail 'trap' accounts to investigate patterns within spam." http://www.microsoft.com/presspass/features/2005/oct05/10-27Zombie.mspx (Ex. 29). As of Nov. 2008, Microsoft

Gordon "registered jim@gordonworks.com and the gordonworks.com e-mail addresses of his "clients" in response to various online promotions and for numerous prize giveaways. Gordon estimates that, in doing so, he subscribed, or 'opted in,' to e-mail mailing lists somewhere between 100 and 150 times." 575 F.3d at 1046. By contrast, BSI has never opted-in to any advertising mailing list. P. Wagner Decl. ¶ 44. All the emails at issue – 74,000 – are unsolicited. *Id*. Defendants try to claim that BSI signed up for spam, without ever giving specifics. Mot. at 5. BSI has attempted to *opt-out* using safemailbox.net. *See supra* section III(¶ 9). Gordon admitted "setting up domains as 'spam traps' [gordonworks.com] with the sole purpose of receiving as many e-mail marketing messages as possible." 575 F.3d at 1056. None of BSI's domains are "spam traps." P. Wagner Decl. ¶ 44; Resnick Decl. ¶¶ 46-50.

"At his instruction, Gordon's 'clients' relinquished control of their e-mail accounts." 575 F.3d at 1046. By contrast, BSI has never instructed anyone to relinquish control of an email account. P. Wagner Decl. ¶ 48. *BSI never provided the vast majority of email addresses receiving spam to anyone — that is obvious, because the addresses are false, i.e., made up*. *Id*. A few customers such as Wagner's brother, Dr. Peter Wagner, have abandoned accounts because of spam, and the account has reverted back to BSI which has kept the account active in the event that legitimate mail gets directed to that account, *id*., but that is a far cry from Gordon.

Gordon's harms, according to the court, were self-imposed. 575 F.3d at 1057. Defendants make this argument. Mot. at 17. The 9th Circuit, in the second of its three cites to

---

has filed 92 spam lawsuits and "over 200 legal actions" against spammers. *See* http://download.microsoft.com/download/2/2/D/22DFC1E7-0260-4AF7-8B81-D3D17ADA5A05/TwC_Elites_Support_for_CAN_SPAM_Nov08.docx

[30] *See, e.g., FTC v. Kinion*, Case No. 05C 6737, n.6 (N.D. Ill.) (brief attached as Ex. 30).

Hypertouch,[31] found Hypertouch's harms to be adequate for standing. *Id*. at 1054 (citing *Hypertouch*, 2006 WL 648688, at *4 (finding evidence of "decreased server response and crashes," "higher bandwidth utilization," and "expensive hardware and software upgrades" sufficient harm for statutory standing)). J. Wagner Decl. ¶¶ 1, 3. BSI has suffered the same harms found adequate in *Hypertouch* for standing under CAN-SPAM, as well as harms recognized by Congress: "the cost of 'investing in new equipment to increase capacity. . . [and] maintaining e-mail filtering systems and other anti-spam technology on their networks to reduce the deluge of spam' as undesirable consequences facing the typical ISP. S. Rep. No. 108-102, at 6." P. Wagner Decl. ¶ 50. Spam has caused BSI's servers to crash; slowed server response; increased costs for network expansion; higher bandwidth utilization; and forced upgrades of costly hardware and software.[32] *Id*. ¶ 50. In addition, based on the number of gigabytes of the spam sent to BSI, and the number of spam, per day (or per minute), spam's bandwidth utilization can be readily determined as reflected in the emails themselves, logs and other associated records reflecting this actual harm that BSI. Ex. 16, P. Wagner Dep. at 1039:12-1041:18.

Defendants make various other inaccurate and irrelevant catch-all factual assertions beginning at 13. With regard to: Paul Wagner spending substantial time on this litigation, this is addressed at section III(¶ 4); BSI being litigious, *see supra* section II (Hydra emails keep coming) and *section* III(¶¶ 1, 5); *Gordon*, 575 F.3d at 1057 (acknowledging "harmful effects

[31] *Gordon*, 575 F.3d at 1056, 1051, 1054 (citing *Hypertouch*, 2006 WL 648688 with approval for rejection of argument that Hypertouch was a "professional plaintiff" that entered the ISP business for the sole purpose of bringing anti-spam lawsuits; noting holding "a provider of e-mail service alone [like Hypertouch], without any other services, qualifies" under CAN-SPAM; and stating Hypertouch has a sufficient "combination of operational or technical impairments" to constitute material harm and have standing).

[32] *Gordon* reads CAN-SPAM to require more injury to the ISP than the costs associated with carrying spam, likely requiring "physical harm" to ISPs. However, this perversely punishes ISPs that invest in infrastructure. Carried to its conclusion, as an ISP invests more in expensive, upgraded technology, its systems become less likely to crash – even though the spam load has increased from about 40% of all email in 2004 to 90-95% now – and as a result, the ISP becomes less likely to be adversely affected, despite the increased amount of spam it receives.

spam and spamming practices, both lawful and unlawful, have upon businesses and consumers" and "need of [ISPs], both small and large, for a legal remedy against law-breaking spammers"); and BSI's marketing, many small businesses advertise through word of mouth and through the Internet, as does BSI, and as do Defendants. At 14, Defendants contend BSI is not a "robust ISP." Dr. Klensin has made clear that even though BSI is not a large-scale, international ISP, it is still an ISP. Klensin Decl. ¶ 66; Ex. 19, Klensin Dep. at 61:7-11. Further, Plaintiff's experts have made clear, there is nothing wrong or inadequate with how it is operating; how the emails were received, saved, processed or stored; or BSI having saved the emails in archives. Klensin Decl. ¶¶ 60-66; Levine Decl. ¶¶ 22-23, 15-16; Resnick Decl. ¶ 29, 43-45.

Defendants also purposefully conflate spam filtering with blocking of emails. Mot. at 14. This is examined at section III(¶ 13). Spam filtering means detecting and flagging probable spam and then handling it differentially. Resnick Decl. ¶¶ 34, 42; Klensin Decl. ¶¶ 45, 57; P. Wagner Decl. ¶ 29. What matters is that BSI, contrary to Defendants' blatantly and demonstrably false assertion, Mot. at 14, does take precautions by filtering. BSI filters using commercial filtering software – SpamAssasin and SpamPal. P. Wagner Decl. ¶ 26. BSI also relies in part on its upstream providers to assist in filtering spam, viruses and other threats. *Id.* ¶¶ 25-26. So, to the extent that Defendants are arguing that BSI does not filter, or is not avoiding spam by filtering (as Gordon apparently was not), that assertion is false and disputed. In addition, Defendants unbelievably cite Joe Wagner as "confirming" that "BSI . . . is not doing any filtering". Mot. at 15. Defendants' penchant for misrepresenting the record knows no bounds. Mr. Wagner was stating simply that there is no selectivity to the emails going to BSI – *i.e.*, BSI is not receiving and archiving only spam messages, but all messages. P. Wagner Decl. ¶¶ 26-28.

As for blocking, even if BSI used filters to block spam *it would not stop the influx given that spammers use numerous tactics to evade spam filters*. Klensin Decl. ¶ 48; Resnick Decl. ¶¶ 34-42. Indeed, the inability of filters to block spam provided part of the impetus for the enactment of anti-spam statutes. *See infra* section IV(C)(2). The law does not require ISPs to embark on such windmill tilting.

Defendants also misleadingly argue that BSI "intentionally facilitated reception" of the emails. Mot. at 14-15. This is demonstrated to be an issue of disputed fact at section III(¶13). Defendants also argue that BSI was not damaged like a traditional ISP. Mot. at 15. This has already been addressed, *supra* pg. 23, but suffice to say the loss of customers is not the only possible harm, and here is not relevant because BSI's customers' emails are not at issue, only those it received as an ISP. As for their apportionment point, Mot. at 15-16, Plaintiff need not apportion damages for each of Defendants' tens of thousands of emails, and that is not a summary judgment theory in any event. *See Asis Internet Servs. v. Active Response Group*, No. C07 6211 THE, 2008 WL 2952809, at *5 (N.D. Cal. July 30, 2008) (holding that plaintiff need not show that a particular email caused particular adverse effect). Finally, Defendants resort to an appeal to the Court to give them the benefit of public policy. Mot. at 16. Public policy favors the victims of Defendants' countless unsolicited, deceptive emails.

A. BSI Did Not Consent To Receive Defendants' Emails

Defendants argue that the routine receipt, filtering and delivery of mail constitute implicit consent to receive their spam. Mot. at 17-19. Conversely, Defendants also contend that BSI's failure to block their spam constitutes implicit consent to receive their spam. Defendants cite to a general California statute, Cal. Civ. Code. § 3515, and Maryland case law, but the application of these principles to this case is ludicrous. A man does not consent to having a rock thrown through his window because he does not erect and close shutters. These arguments fail legally,

are factually unsupported by their citations to the record and are controverted by Plaintiff's declarations, and would not be dispositive in any event.

Consent to the receipt of email advertisements is specifically defined in the California statute under which BSI is suing. The statute states:

> "Direct Consent" means that the recipient has expressly consented to receive e-mail advertisements from the advertiser, either in response to a clear and conspicuous request for the consent or at the recipient's own initiative.

Cal. Bus. & Prof. Code § 17529.1(d) (emphasis in original). Code § 17529.5(b)(1)(A)(iii) provides actual damages for a "recipient," as opposed to an ISP or the Attorney General, of any illegal commercial email plus statutory damages for illegal "unsolicited commercial e-mail." § 17529.5(b)(1)(A). "Unsolicited commercial e-mail" in turn, is defined, in part, as email which lacks "direct consent." *Id*. § 17529.1(o)(1). This has two implications. First, because the "unsolicited commercial e-mail" element only applies to individual recipients, and not ISPs or the AG, it is clear that consent is not a requirement of the California statute for ISPs. This makes sense – ISPs *qua* ISPs do not have consensual or "preexisting customer relationships" with merchants – they are the mailmen who deliver mail to the people who have those relationships. Therefore, consent is not an element of the statute, and like Maryland, it is the sending of false mail, whether solicited or not, to an ISP, that is illegal. Second, because § 17529 explicitly defines the required consent, the more general provisions of § 3515 are not applicable. *People v. Benhoor*, 99 Cal. Rptr. 3d 827, 837-38 (Cal. Ct. App. 2009) ("It is a settled rule of statutory construction that a special statute dealing expressly with a particular subject controls and takes priority over a general statute."); *see also Lake v. Reed*, 940 P.2d 311, 321 (Cal. 1997) ("[A] more specific statute controls over a more general one").

Defendants mischaracterize the testimony of Plaintiff's experts. As described above, *supra* section III(¶ 11), Plaintiff did not employ spam traps. Furthermore, as also explained above, *supra* section III(¶¶ 11, 13), the policy not to reject emails and to use wildcards have valid business purposes and therefore Plaintiff has every right to use them. *See Ford v. Gouin*, 834 P.2d 724, 735 (Cal. 1992) (acceptance of risk is not voluntary when exercising a right or privilege that the defendant has no right to deprive plaintiff of exercising) (citing Restatement (Second) Torts, § 496E, subd. (2)). As also discussed, *supra* section III(¶ 10), the email addresses that Plaintiff published were done so to fulfill a statutory notice requirement. Furthermore, the publication explicitly stated "THE SENDING OF UNSOLICTED EMAIL ADVERTISING … TO ANY OF THE EMAIL ADDRESSES… SHOWN ON THIS PAGE IS EXPRESSLY AND EXPLICILITY PROHIBITED." Ex. 31, Resnick Dep. Exhibit 258. The fact that Defendants and their affiliates "harvested" those address and sent them spam is a further violation of the California statute. Cal. Bus. & Prof. Code § 17529.4.

Defendants also attempt to twist an inapplicable assumption of the risk principal – failure to take preventive measures – into a form of consent. Mot. at 19. Even if the preventive measures standard were generally applicable, the measures suggested by Defendants have been taken or they would interfere with BSI's business operations and thus deprive Plaintiff of its right to operate its business. *See Ford*, 834 P.2d at 735. Defendants simply reiterate the same discredited points: with regard to BSI's use of spam filters, *supra* section III(¶ 11); wildcards, *see id.*, its routing of emails, *see id.* (¶ 14); BSI not soliciting spam, *see id.* (¶ 8). Furthermore, as approximately 95% of all email is spam, accordingly, barring ISPs from transmitting email to each other in order to avoid consenting to receive spam would mean no ISP could transmit email.

Regarding Maryland law, the Maryland cases that Defendants cite are not even about consent, they are assumption of the risk cases. Notably, assumption of the risk is not an applicable defense to intentional acts, such as sending emails. *See infra* section IV(C)(2); *Janelsins v. Button*, 102 Md. App. 30, 42 (1994) ("Historically, the doctrine of assumption of the risk has provided a defense only to actions for negligence. It has little or no application in the case of intentional or reckless conduct.") (citing *Ordway v. Superior Court*, 243 Cal. Rptr. 536, 542 (Cal. Ct. App. 1988)). Consent is only a defense when it negates an element of an intentional wrong. *E.g*., *Katsenelenbogen v. Katsenelenbogen*, 368 Md. 122, 131 n.1 (2001) (battery occurs when "one intends a harmful or offensive contact with another without that person's consent"). However, the Maryland statute does not include a consent element that can be negated. The Maryland statute makes it unlawful for a person to send false or misleading electronic email. Md. Comm. Code § 14-3002(b). Consent is not an issue in the Maryland statute. The same is true in California. Further, it is illogical to argue that one could consent to something that is false, misleading or deceptive, and in any event, Plaintiff never granted such consent. *See supra* section III(¶¶ 8-14).

Finally, the *Gordon* holding, cited by Defendants provides no support for consent as a defense. Mot. at 17-18. Defendants' cite to the concurrence which reasons that statutory remedies are available to plaintiffs similar to Gordon (those who "gratuitously created circumstances that would support a legal claim") under statutes such as housing "testers." *Gordon*, 575 F.3d at 1067-69. The reasoning of the *Gordon* concurrence indicates Gordon would have standing under the Maryland and California statutes, *infra* section IV(A), but that is neither here nor there because the reasoning is based on the specific statutory definition in CAN-SPAM's standing provision and must be viewed in that context, and because BSI is bona fide.

B. BSI's Claims Under Maryland And California Law Are Not Preempted

BSI's claims are not pre-empted by CAN-SPAM. Defendants misrepresent the holdings of *Mummagraphics* and *Gordon*. Those opinions do not find – or even imply – that CAN-SPAM preempts all state law claims that do not prove the elements of common law fraud. Rather, those courts held only that state law claims based on mere "immaterial errors" in commercial email are preempted. *See Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348, 353 (4th Cir. 2006); *Gordon*, 575 F.3d at 1061-62.[33] These holdings are consistent with the language of the CAN-SPAM savings clause, which protects from preemption those state statutes that prohibit falsity or deception in commercial email. Tellingly, Defendants seek summary judgment on preemption and yet do not even discuss the text of the preemption savings clause.

1. State law claims grounded in falsity or deception are not preempted.

Congress in the CAN-SPAM Act "allows states to prohibit 'falsity or deception' in commercial email messages." *Mummagraphics*, 469 F.3d at 354; *accord Gordon*, 575 F.3d at 1061. The plain language of CAN-SPAM, its structure, and its legislative history make clear that CAN-SPAM does not preempt state laws directed to false and deceptive content in email transmissions, such as California and Maryland's anti-spam statutes. The 4th Circuit's interpretation of CAN-SPAM's preemption clause is consistent with this reading because the *Mummagraphics* court simply found that the terms "falsity" and "deception" in the context of CAN-SPAM refer to "torts involving misrepresentations," not mere "bare error." *Mummagraphics*, 469 F.3d at 354; *see also Gordon*, 575 F.3d at 1061. The 4th Circuit never suggested – let alone held – that a claim based on state law must prove the required elements of common law fraud in order to survive preemption.

[33] Defendants briefly discuss the California Superior Court decision in *Hypertouch v. Valueclick*, however that decision is presently on appeal, and would have little persuasive authority in any event because as an unpublished Superior Court opinion not even California state courts permit citation to it. California Rules of Court Rule 8.1115.

When addressing questions of express preemption, the Court begins its analysis "'with the assumption that the historic police powers of the States [are] not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.'" *Altria Gp., Inc. v. Good*, 129 S. Ct. 538, 543 (2008) (citation omitted) (alteration in original). "That assumption applies with particular force when Congress has legislated in a field traditionally occupied by the States. . . . Thus, when the text of a preemption clause is susceptible of more than one plausible reading, courts ordinarily 'accept the reading that disfavors preemption.'" *Id*. (quoting *Bates v. Dow Agrosciences LLC*, 544 U.S. 431, 449 (2005)). Regulating deceptive conduct and false advertising implicates consumer protection, an area long regulated by the States. *See Am. Consumer Public Ass'n, Inc. v. Margosian*, 349 F.3d 1122, 1131 n.12 (9th Cir. 2003) ("Consumer protection is a 'matter firmly committed to the states' under their police powers.") (citation omitted). Moreover, "any understanding of the scope of a preemption statute must rest primarily on 'a fair understanding of *congressional purpose*'," as well as the 'statutory framework', and the 'structure and purpose of the statute as a whole'." *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485-86 (1996) (citation omitted). The statutory framework, structure, and purpose of CAN-SPAM make clear that it "saves" more than common law tort claims from preemption.

The CAN-SPAM preemption provision states:

> This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, ***except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto*.**

15 U.S.C. § 7707(b)(1) (emphasis added). This clause has two parts. The portion up to "except" defines the outer boundary of preempted state laws. The latter portion of the provision – the savings clause – carves out a subset of state laws that are exempt from preemption.

Significantly, Congress did not use the word "fraud" to describe these saved claims, but rather used a phrase with a known meaning in the federal canon. The savings clause refers to "falsity or deception," which terms are necessarily broader than fraud. *Compare United States v. Ninety-Five Barrels*, 265 U.S. 438, 443 (1924) (in construing the word "deceive" in the Food and Drug Act, the Court observed that "[d]eception may result from the use of statements not technically false or which may be literally true") *with* Restatement (Second) of Torts § 527(a) (1977) (where maker of representation knows it is capable of both true and false interpretations, and makes it "with the intention that it be understood in the sense in which it is false," it is fraudulent). The savings clause's plain language is determinative. *See Cipollone v. Liggett Group Inc*., 505 U.S. 504, 521-22 (1992); *see also Asis Internet Servs. v. Subscriberbase Inc.*, No. 09-3503 SC, 2009 WL 4723338, at *3, 8-9 (N.D. Cal. Dec. 4, 2009) (finding terms "falsity or deception" should be read broadly "saving more than just common law fraud claims and narrowing the pre-emptive effects of" CAN-SPAM).

Further, a narrow reading of the CAN-SPAM savings clause like that advanced by Defendants would render the entire savings clause meaningless. The preemption clause at issue does not encompass common law tort claims. It preempts state positive laws only – "statute, regulation or rule" – and then saves a subcategory of those laws. *See Sprietsma v. Mercury Marine*, 537 U.S. 51, 63 (2002); *Cipollone*, 505 U.S. at 519. Thus, there was no need for Congress to "save" common law fraud claims because they are not preempted in the first place.[34] To give the savings clause meaning, it should be interpreted to "save" state legislative

[34] Congress refers to "common law" when it intends to include it within the scope of a preemption clause. *E.g.*, Copyright Act of 1976, 17 U.S.C. § 301(a) (preempting rights "under the common law"). Indeed, as discussed above, the references to "tort law" and "acts of fraud" in the subsection that follows the general preemption clause shows that Congress was cognizant of common law fraud actions and did not intend to preempt them. *See* 15 U.S.C. § 7707(b)(2)(A), (B) (expressly stating that state laws relating to tort or acts of fraud actions are not preempted).

enactments and executive pronouncements that prohibit falsity or deception in emails, as distinct from common law claims.

Simply put, CAN-SPAM does not equate "falsity or deception" with fraud. Indeed, the savings clause requires the opposite conclusion – *i.e.*, that falsity and deception are independent concepts from fraud – by also saving "other" state laws that "relate to acts of fraud":

> (2) State law not specific to electronic mail
>
> This chapter shall not be construed to preempt the applicability of–
>
> (A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or
>
> (B) ***other State laws to the extent that those laws relate to acts of fraud*** or computer crime.

15 U.S.C. § 7707(b)(2). If Congress had intended its savings clause in § 7707(b)(1) to only "save" state laws that prohibit common law fraud in the context of email transmission, then it need not have separately addressed state laws that prohibit "fraud" in § 7707(b)(2). *See TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) ("It is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.'"). The bifurcated structure of § 7707(b) can only be read to mean that Congress intended to exempt both state laws that address false and deceptive content in e-mails such as California and Maryland's anti-spam statutes, *as well as* common law fraud claims under state law.

The structure of CAN-SPAM also demonstrates that the terms "falsity or deception" do not refer only to common law fraud. CAN-SPAM also refers to falsity and deception in its substantive provisions governing commercial email and requires that those terms be consistent with the definition of the same terms in the FTC Act. *See* 15 U.S.C. § 7704(a)(2). Under the FTC Act, in turn, "an act or practice is deceptive if first, there is a representation, omission, or

practice that, second, is likely to mislead consumers acting reasonably under the circumstances, and third, the representation, omission, or practice is material" *FTC v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009) (internal quotation and citations omitted) (emphasis added). "Deceptive" as applied to the FTC Act, then, does not require actual reliance and injury, and, accordingly, does not mean fraud.

Thus, "[t]he CAN-SPAM Act's repeated references to the FTC Act definition of 'deceptive' practices strongly suggest that Congress intended the phrase 'falsity or deception' in Section 7707(b)(1) to encompass more than refer to, or at least encompass, that definition, not just state tort law." *Asis Internet Servs. v. Consumerbargaingiveaways*, 622 F. Supp. 2d 935, 942 (N.D. Cal. 2009). In short, nowhere in the statute did Congress equate the terms "falsity" or "deception" with common law fraud, and there is no reason to define deception differently from how it is used in other subsections of CAN-SPAM, such as §§ 7704(a)(2) and 7707(a)(2). *See Asis Internet Servs.*, 2009 U.S. Dist. LEXIS 112852, at *3 (finding use of word "fraud" elsewhere in CAN-SPAM and statute's references to "deception" as used in FTC Act invite clearly suggest more that common law fraud claims saved).

At the time Congress passed CAN-SPAM, 37 states already had in place statutes regulating unlawful commercial e-mail. Congress could have preempted completely state law, but by carving out a "savings" clause that exempts from preemption those statutes, regulations and rules that "prohibit falsity or deception" in commercial email, Congress created a dual regime of state and federal regulation. *See, e.g., Wright v. Gen. Mills, Inc.*, No. 08cv1532 L(NLS), 2009 WL 3247148, at *2 (S.D. Cal. Sept. 30, 2009) ("[T]he inclusion of an express preemption provision that permits state regulations that are identical to federal law demonstrates that state regulation and enforcement can exist along with federal regulation.") (citing

Freightliner Corp. v. Myrick, 514 U.S. 280, 288 (1995)). This balance struck by Congress is completely consistent with the historical, complementary relationship between the federal and state governments in the area of regulating deceptive consumer practices. *See, e.g.*, 16 C.F.R. § 0.17 (2009) (FTC's mission includes "to assist and cooperate with … state … agencies in consumer protection enforcement and regulatory matters."). Furthermore, because CAN-SPAM and the state anti-spam statutes have a "common purpose" in preventing false and deceptive practices, the presumption against preemption has "special force" here. *Pharm. Research & Mfrs. of Am. v. Walsh*, 538 U.S. 644, 666 (2003) (quotations and citation omitted); *see also In re Farm Raised Salmon Cases*, 175 P.3d 1170, 1176 (Cal. 2008) ("[c]onsumer protection laws such as the [UCL], false advertising law, and CLRA, are within the states' historic police powers and therefore are subject to the presumption against preemption.") (quotations and citation omitted) (alteration in original), *cert. denied*, 129 S.Ct. 896 (2009); *accord Pinney v. Nokia, Inc.*, 402 F.3d 430, 454 (4th Cir. 2005).[35]

In enacting CAN-SPAM, Congress intended to protect commercial email generated by law-abiding businesses engaged in legitimate practices from a tangle of differing state standards technical requirements. But Congress made clear that state statutes prohibiting falsity and deception remained in place "because they target behavior that a legitimate business trying to comply with relevant laws would not be engaging in anyway." S. Rep. No. 108-102 at 22, *reprinted in* U.S.C.C.A.N. at 2365; *see also Gordon*, 575 F.3d at 1045. Thus, Congress explicitly left room for the States to exercise their police powers and regulate deceptive conduct

[35] Shortly after CAN-SPAM's enactment, the California Legislature revisited § 17529.5 to make clear that the state prohibitions against false and deceptive spam are *not* preempted. *See* S.B. 1457, Assembly Committee Analysis, 2003-2004 Sess., at 4 (Cal. June 15, 2004) (CAN-SPAM "did not preempt the private right of action consumers and ISPs have against those who send spam with misleading or falsified headers and information, as well as the advertisers of those products."), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1451-1500/sb_1457_cfa_20040613_185546_asm_comm.html.

in e-mails. *See Beyond Systems, Inc. v. Keynetics, Inc*., 422 F. Supp. 2d 523, 537-38 (D. Md. 2006) (holding MCEMA not preempted).

Because "falsity" and "deception" are not synonymous with fraud, *Mummagraphics* and *Gordon* cannot be read to establish that BSI must prove the required elements of common law fraud for its claims to survive preemption. Rather, their interpretation of the CAN-SPAM preemption clause is consistent with the analysis above – finding that state-law claims based on falsity or deception in commercial e-mails survive preemption.

2. Falsity and deception in spam are inherently material.

Defendants' syllogistic theory that only material falsity is illegal, and only falsity on which consumers rely in a buying decision is material, must be rejected. The falsity targeted by the state statutes is, in general, falsity that impairs or obscures the identification of the sender, which is designed to evade filters and/or which misleads about the nature of the email. Such falsity is "material" in itself because it direct relates to the harm caused by spam – the fact of having to receive the email in the first place, the inability to contact the sender and the deception about the content. Moreover falsity of this sort – the kind prohibited by the state statutes – is purposeful and has no legitimate purpose – whether technical or business.

"*Spamming is intentional conduct* essentially directed at, among others, servers and their owners." *Aitken v. Commc'ns. Workers of Am*., 496 F. Supp. 2d 653, 660 (E.D. Va. 2007) (emphasis added). And the principle harm in spam is receiving the emails in the first place. In *MaryCLE* and the three cases it relied upon, the defendants had sent unsolicited marketing emails. "[I]n each of those cases, the plaintiffs were the recipients of the unwanted emails *and the receipt of the emails was the injury*.... In fact, in *MaryCLE*, as well as the three cases relied upon therein, the *cause of action was based on a statute that prohibited sending the emails that were the subject of the suits*." *Strudwick v. Whitney*, No. 24-C-08-000767, slip op. at 25 (Md.

Cir. Ct. Aug. 28, 2009) *available at* 2009 WL 3197887 (citing *MaryCLE, LLC v. First Choice Internet, Inc*., 166 Md. App. 481, 504 (2006)) (emphasis added). Additionally, when the Assistant Attorney General of Maryland wrote to the House Committee regarding HB 915, he pointedly identified the harm addressed by the bill:

> House Bill 915 would address e-mail messages that make the sifting process more difficult by misrepresenting either the sender or the subject matter of the e-mail message. In addition to lost productivity, deceptive spammers often disguise pornographic e-mail by misrepresenting the subject matter, which may then be opened by unsuspecting consumers or their children.

Ex. 27. Thus the harm targeted by MCEMA was the receipt of spam which makes it harder to find important messages, identify the sender, and identify the nature of the email. In other words, spammers' attempts to evade filters are illegal not because they mislead spam filters – *they are illegal because they are misleading, as evidenced by their successful evasion of spam filters*.[36] The Maryland Economic Matters Committee floor report on HB 915 identified that under then-current law, "[a] practice that is prohibited by the Maryland Consumer Protection Act violates the Act, regardless of whether a consumer in fact has been misled, deceived, or damaged as a result of the practice." Ex. 33. Thus, it is well established in Maryland law that the State in the consumer protection area has outright prohibited acts such as the sending of unsolicited commercial email, and prohibited deceptive trade practices without requiring reliance because deceptive practices are in themselves harmful, material and intentional.

Similarly, California SB 186 was "intended to address a problem well known to all e-mail users, *the proliferation of unsolicited e-mail ads, or spam*."[37] Ex. 34 (emphasis added).

---

[36] Evidence of the deceptive nature of the spam can be seen, for example, in SPAM-H000208, where a fraudulent domain registration and false HELO resulted in the successful deception of BSI's SpamPal filter (*i.e.* "X-SpamPal: PASS"). Ex. 32. *See also* section III(¶ 13).

[37] info.sen.ca.gov/.../sb_186_cfa_20030904_114452_asm_floor.html.

The bill "[c]ontains legislative intent language delineating the adverse consequences of e-mail spam," *id*., which clearly identifies the targeted harm as the falsity in the email itself –

> Many spammers have become so...technologically sophisticated that they can adjust their systems to counter special filters and other barriers against spam.... There is a need to regulate the advertisers who use spam, as well as the actual spammers, because the actual spammers can be difficult to track down due to some return addresses that show up on the display as "unknown" and many others being obvious fakes and they are often located offshore.

Cal. Bus. & Prof. Code § 17529. *See also* S. Rep. No. 108-102, at 2, *reprinted in* 2003 U.S.C.C.A.N. at 2349 (noting prevalence of falsity related to sender or nature of email: "66 percent of all spam contains some kind of *false, fraudulent, or misleading information*, either *in the e-mail's routing information, its subject line, or the body of its message*.") (emphasis added). The harm of spam is in the receipt of the deceptive advertising. Being duped into buying something is an exacerbation of the harm. The issue is not what constitutes material falsity because the statutes already provide for what is "material."

3. Fraud reliance as the standard for falsity for an ISP is unsupported in law and reason.

Defendants argue that since BSI cannot show any material falsity, it cannot show misrepresentation as a matter of law and its claims are preempted. Mot. at 26. This is another way of saying that BSI cannot show reliance on falsity that rises to the level of fraud in order to escape preemption. Defendants' argument that BSI's allegations of falsity involve mere immaterial errors depends on this Court agreeing that BSI must show that the falsity affected a consumer's buying decision. Mot. at 27-29.[38]

[38] *See* Mot. at 27-29 ("BSI's allegations of falsity have nothing to do with a consumer's decision to purchase anything"; "To" fields … have nothing to do with material terms a consumer might consider when deciding to purchase goods or services"; "consumers do not use domain name registrations to decide whether or not to purchase goods advertised in emails"; "statements in emails falsely imply[ing] a relationship with the sender …do not relate

Defendants' argument is defective because they mistakenly conduct their analysis of the facts and law through the prism of a consumer rather than an ISP. For an ISP, falsity rooted in reliance makes no sense. This critical misstep undermines their fraud and falsity analysis.

Underscoring that common law fraud cannot be all that remains to the states after CAN-SPAM is the fact that making an ISP (or the Attorney General, for that matter) prove fraud is nonsensical. First, ISPs are companies that act as the mailmen of the Internet. *ISPs do not "read" the mail; ISPs qua ISPs do not make purchases, and therefore do not rely on the content of advertising to make buying decisions.* ISPs act through their computer systems to filter and flag the email based on the filter's analysis of the content of the header and body. Klensin Decl. ¶ 45-50; Resnick Decl. ¶¶ 27, 34-37. ISPs are deceived by falsity designed to impede or evade their filters. A fraud standard simply makes no sense when applied to an ISP because an ISP does not "rely" on the emails in the sense of a buying calculation, but instead relies on representations made about, *inter alia*, the source of the message and identity of the sender (*e.g.*, Received header, domain and IP address, Froms).

Second, reliance in connection with falsity in a header – for example, false information about the transmission path – makes little sense in the context of individuals being affected in their buying decisions. An email misrepresenting such a fact is deceiving as to the sender not because it affects a buying decision, but because of the facial misrepresentation and because it impairs the ability to determine who sent it. Falsity in the header designed to impair that ability and consequently which also impairs filters is material – *so much so that the 9th Circuit just sent people to jail for it. See United States v. Kilbride*, 584 F.3d 1240, 1257 (9th Cir. 2009) (affirming convictions in case where "[i]n the headers of their bulk emails, Defendants

---

to a consumer's decision to purchase goods or services"; "HELO/EHLO fields … are never seen by ordinary consumers and therefore are immaterial to a consumer's decision to purchase goods or services").

intentionally replaced the email addresses from which the emails were sent with fictitious addresses. It is quite obvious that this diminish[ed] the ability of recipients to identify, locate, or respond to Defendants or their agents….”). Because falsity affecting a buying decision is not required, this Court must reject each of Defendants’ arguments at 24-30.

4. Defendants’ argument that Plaintiff’s claims are preempted because Plaintiff was capable of attributing the emails to them is unsupported in law and reason.

Defendants argue that Plaintiff’s claims are preempted if the identity of the advertiser is apparent from the emails. Mot. at 30-31. Defendants carefully – but quite noticeably – omit reference to their role in the transaction, and contend that if the *advertiser’s* identity is transparent, then the emails cannot be deceptive. Emails can be false or deceptive in numerous other ways, however, including in obscuring the identity of *Defendants* and the statutes create liability for the parties that encouraged or assisted in the sending of spam.

Omega does not support Defendants’ preemption argument. In *Omega*, the parties responsible for sending the email were accurately identified, and no other falsity present in the spam, here we are discussing the import of senders who do not identify themselves and the fact of emails replete with falsity. In addition, the purported advertiser is often just a façade – a d/b/a – shielded from identification by false and/or anonymous domain registrations, such that the mere fact that an advertiser’s name is visible, can be meaningless to identifying who the actual parties are behind the email. For example, Connexus owns “millions literally” of domains. Ex. 35, Son Dep. at 159:12-15.

Defendants secondly argue that since the emails ultimately were attributed to them then the “the alleged inaccuracies in the headers could not have impaired the efforts of any recipient.” Mot. at 31. Defendants cite no law in support of their position, however, “impair” does not mean

prevent, but to make more difficult. *Kilbride*, 584 F.3d at 1258.[39] Here, the emails are replete with falsity that impairs the ability to identify Defendants, and therefore, the falsity is not preempted even under Defendants' own argument. Moreover, Defendants and their affiliates employ various tactics to purposefully obscure their identity, such as anonymous / proxy registrations. *See id.* at 1259 ("private registration for the purpose of concealing the actual registrant's identity would constitute 'material falsification.'"). Therefore, because Plaintiff was able to identify Defendants' complicity in the spam – despite their best efforts to impair that ability – cannot mean its claims are preempted.

C. Defendants' Emails Are Replete With Falsity and Deception Which Defendants Cannot Show Is, As A Matter Of Law, Not Illegal

In order for the Court to grant summary judgment on falsity, as a matter of law, Mot. at 26-30, it must find that Defendants have indisputably made a showing that Plaintiff cannot prove that *any element* of the 74,000 emails is false – not a single From:, To:, Subject, HELO, registration, opt-in statement, etc.[40] Defendants have made no effort to do so.[41] Moreover, Defendants' argument hinges on whether the falsity in an email affects a consumer's decision to purchase. *See supra* note 39. If this Court rejects that approach, either because fraud is not

[39] ("'[I]mpair' clearly is not synonymous with 'completely obstruct.' To impair, according to its plain meaning, merely means to decrease."; falsifying the contact information in a domain registration "intentionally decreas[es] the ability of a recipient to locate and contact the actual registrant, regardless of whether a recipient may still be left some avenue to do so.").

[40] Defendants do not address other types of falsity the emails such as false Dates and false use of famous corporate names not associated with the offer (such as Louis Vuitton, Vespa and Apple).

[41] Notably, Connexus and Hydra do not actually assert that their misrepresentations regarding Free or other falsity types such as false Froms, HELOs, Tos, were, in fact, immaterial, *but rather that they cannot be material*. Mot. at 26. Accordingly, the court, even if it were to apply the FTC standard, would not need to decide whether a representation must be "'likely to affect [consumers'] choice of, or conduct regarding, a product'." *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1096 (9th Cir. 1994) (citations omitted) (alteration in original). That said, the FTC's material falsity standard is off point for the same reasons as stated in section IV(C)(3). The FTC standard was not developed in the spam context and is not meant to be applied here because the purpose of the anti-spam statutes is first and foremost to prevent against having to receive unwanted emails. However, if the court determined that "deceptive" as defined by the FTC, which is a "material misrepresentation" by definition, is the standard for "deceptive" in the state statutes, then the types of deception referred to in the statutes must be presumed to be material since they are defined as such, and cannot therefore be simple or bare error, or for that matter, preempted, as a matter law.

required, makes no sense with regard to an ISP, or any other reason, *supra* sections IV(C)(1-4), then it must reject all of Defendants' section B(iii).

First, Defendants argue that "To" fields cannot be false as a matter of law. Mot. at 27. Falsity in headers is proscribed by California. § 17529.5(a)(2). "To" fields contain information about a recipient of an email. A common spammer trick is to use a false information in the "To" field to induce a recipient to open the email. Resnick Decl. ¶¶ 17, 63; Klensin Decl. ¶¶ 31, 42. For example, Sebastian Barale in his emails sent on behalf of Connexus used a rotating array of false "To" names. The only reason to do this is to cause the recipient to want to open the email to assess its contents and why it was sent to his address with a name other than his own. *Id.*

Second, Defendants argue that Subject lines cannot be false as a matter of law. Defendants point to three Subject lines that they disagree are false, or in other words, cannot be likely to deceive or have the capacity, tendency, or effect of deceiving the recipient. Mot. at 27; *see* Md. Comm. Code § 14-3002(b)(2)(iii); Cal. Bus. & Prof. Code § 17529.5(a)(3). On the basis of that "analysis" they attempt to cast out all Subject lines, but they cannot. Defendants provide Subject lines to their affiliates. *Supra* section II & note 6. Many of those Subject lines contain offers of "free," "complimentary" or "no charge" goods and services where the goods or services are not "free," but require a purchase or commitment. This is classic false advertising.[42] Levine Decl. ¶¶ 25, 32. Furthermore, the likelihood that Subject lines will be misconstrued – such as for a "free" offer – and that Defendants know this, and that it is *purposeful*, is readily apparent from Defendants' own documents, testimony and practices. Ex. 36, H0010506-10521; Ex. 35, Son Dep. at 133:2-134:14 ("common knowledge within the industry" "there were certain words that you weren't to use" because filters would pick them up). Resnick Decl. ¶ 35. Hydra and

[42] *See also* 16 CFR 251.1 (2009) ("FTC Guide Concerning The Use of the Word 'Free' And Similar Representations").

Connexus' monitoring service, Lashback, also reports "false subject lines" to them – making it readily apparent that Defendants are well aware of what constitutes a false Subject line. Defendants argue in a footnote that Plaintiff cannot prove the Subject lines were false in the case where it did not produce the images that must be separately downloaded with the email. Mot. at 28 n. 5. First, the images are not needed to show falsity. Levine Decl. ¶¶ 42, 45. Second, Defendants have produced many of these images in discovery that have been matched to the emails not only proving the emails are theirs but also undercutting their argument about proving falsity. *See supra* section II note 18 & ¶ 15.

Third, they argue that if the body of the email clarifies the "headline" (which they equate to the Subject line), then it cannot be false. Mot. at 27. However, Subject line falsity, per the statute, is adjudged by whether the Subject line itself could deceive – no provision is made for clarification that forces people to open the emails and root around through whatever disclaimers might (but probably are not) present. *See infra* section IV(C)(2); *FTC Report*, at 4; *see also FTC: Big Print. Little Print. What's the Deal?* ("Consumers should not have to wander through an electronic maze to discover important conditions or limitations of an offer.").[43] In any event, such as inquiry as to whether the image clarified the Subject line is an issue of fact.

Third, Defendants argue that false registration of the domains cannot be false as a matter of law since "consumers do not use domain name registrations to decide whether or not to purchase." Mot. at 28. This badly misses the mark. First, an email appearing to come from a reputable domain name may well influence a consumer. For example, an email purporting to come from "Applestore.com" may well lead a person to believe that Apple is the advertiser or a sponsor of the advertising. Second, at the most basic level, falsely registering a domain name is

[43] http://www.ftc.gov/bcp/edu/pubs/business/adv/bus44.shtm.

only done for one reason – to impair people from identifying the person or entity behind – the origin – of that domain/email. *See* Md. Comm. Code § 14-3002(b)(2)(ii). In *Kilbride*, the 9th Circuit held that obscuring the identity of the sender through false or anonymous domain registrations constituted falsity. *See Kilbride*, 584 F.3d at 1258, 1259.[44] As the FTC reported to Congress, perhaps the most difficult problem associated with spam is its untraceability. *FTC Report*, at 10 ("The single greatest challenge for anti-spam law enforcement is to identify and locate the source of a particular spam campaign."). This untraceability "makes it possible, indeed cost efficient, for spammers to send email messages to millions of email accounts worldwide, while allowing them to hide their identities and the origins of their email messages." *Id*. For these reasons, Connexus, Hydra and their spammers use thousands of "throw away," private, and falsely registered domains to hide their relationship with the emails. Hydra even privately registered its domains hydramedia.com, lynxtrack.com, imglt.com and ltpic.com, which are found in the emails. Moreover, the use of false registrations violates ICANN-accredited domain registrar policies, and the use of anonymous registrations in connection with sending spam does as well.[45] Klensin Decl. ¶¶ 24, 25, 35-37.

Fourth, Defendants argue that falsely stating or implying that the email was solicited cannot be false as a matter of law. Mot. at 28. Their argument, incredibly, seems to be that it is acceptable to lie. At bottom, these false statements deceptively mischaracterize a relationship between the sender and recipient, and thus relate, *inter alia*, to the "origin or the transmission

[44] ("It should have been clear to Defendants that intentionally falsifying the identity of the contact person and phone number for the actual registrant constitutes intentionally decreasing the ability of a recipient to locate and contact the actual registrant, regardless of whether a recipient may still be left some avenue to do so." "private registration is a service that allows registration of a domain name in a manner that conceals the actual registrant's identity from the public absent a subpoena.").

[45] *See* ICANN's Generic Names Supporting Organization's Whois report at http://gnso.icann.org/issues/whois/. See also Section 3.3 and 3.7.7 of ICANN's standard Registrar accreditation agreement at http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm

path of the commercial electronic mail." Md. Comm. Code § 14-3002(b)(2)(ii). Statements implying or expressly stating that the recipient received the email because of its relationship with the sender, where no relationship exists, is quintessential falsity in the area of advertising. Spammers commonly attempt to induce the reader to open an email or transact business by making the reader believe he might have signed up to receive the advertising. This sort of trickery is a spin on that sort frequently seen, for example, in Subject Lines that use the convention of "Re:" or "Fw:" to suggest that the email is a reply to your email or sent by someone you know. Resnick Decl. ¶ 37. When false, the statement that the person signed up for the email is fundamentally material because in addition to being purposeful (here it is because all of the emails were unsolicited), it is an untruth about directly consenting to receive the email. *See supra* section IV(B).

Fifth, Defendants argue that false Froms cannot be false as a matter of law. Defendants seek summary judgment on tens of thousands of emails based on a single, *one-sentence* assertion that "claims involving "From" fields "simply alleging that the headers contained 'incomplete' information" "are preempted." Mot. at 28-29. Defendants provide no examples of what they are referring to and no analysis whatsoever. It is untenable to argue that false Froms – *i.e.*, misrepresentation about the sender's identity, is not material or illegal. Md. Comm. Code § 14-3002(b)(2)(ii); Cal. Bus. & Prof. Code § 17529.5(a)(2); *see Kilbride*, 584 F.3d at 1257. Resnick Decl. ¶¶ 15, 52, 61, 64-65, 67; Klensin Decl. ¶¶ 27-30; Levine Decl. ¶¶ 22, 23, 29. This is archetypical spammer falsity perpetrated for only one reason: to obscure the identity of the sender from angry recipients.

Sixth, Defendants argue that false HELOs cannot be false as a matter of law. Mot. at 29. Many emails at issue contain false information in the HELO field in the header. When the

computer sending an email connects with the computer receiving an email, such as BSI's servers, it identifies itself with an IP address or a domain name. That is, the sending machine says to the receiving machine, "Hello. I am [apple.com][38.112.47.17] and I would like to send you mail." Most receiving systems, like BSI's, then perform an automated look up of the domain or IP to determine whether the IP address and domain match. ISPs do this because legitimate commercial emailers do not rotate their IP addresses or their domains, thus a failure to match the two is indicative of unwanted mail. Klensin Decl. ¶53. In addition, ISPs use this information to determine whether the mail should be filtered based on the sender's IP address or domain, *i.e.*, whether it has been *previously identified* as a sender of spam. That a consumer might not see the HELO exchange is entirely irrelevant to the fact that ISPs rely on the validity of the HELO in making critical determinations about filtering. False HELOs, therefore, impair the ISPs' ability to identify the sender, and to filter unwanted mail. This is exactly the type of falsity targeted by the statutes. What is at issue here is patterns of false mismatching HELOs and HELOS that cannot legitimately exist under the accepted conventions for top-level domain names, such as entirely numeric domains. Resnick Decl. ¶ 62. This is quintessentially "misleading information about the origin or the transmission path," in violation of § 14-3002(2)(ii), and "falsified, misrepresented, or forged header information," in violation of § 17529.5(a)(2). While mismatching HELOs do occur for valid reasons as Dr. Klensin noted, that is not what is at issue here. Resnick Decl. ¶ 22; Klensin Decl.¶ 22. Legitimate email marketers do not change around their IP addresses, rotate their domains, or send bulk email from a coffee shop or library.

D. Identification Of Falsity In No Way Equates To A "Labeling Requirement"

Defendants contend that BSI seeks to impose "labeling requirements." Mot. at 31-32. CAN-SPAM preempted laws 20 states' laws that had required a label, such as Cal. Bus. & Prof. Code § 17538.4, which required "ADV:ADLT:" for material only viewable by those over 18

years old.[46] Nothing remotely similar is at issue here. Defendants argument confuses the statutory requirement that *content not be false* with a demand for "specific types of labels." BSI has never claimed that "the emails must identify the sender in the "From" fields or that emails must not identify the subject matter of the email in the "From" field." Mot. at 32. BSI has claimed an email From field is illegal where it (1) falsely, deceptively or misleadingly identifies the sender; (2) where the description of the sender is false, e.g., it purports to come from Apple Store but does not; and (3) where the description bears no relationship with the content of the email and is therefore misleading about the subject matter as well as not accurately identifying the sender. Defendants cite to their Exhibit 26 (Legend for Master Spreadsheet) to support its contention. The relevant portion reads: "**Violation Codes** … VIO-FRN False, misleading, falsified, misrepresented, and/or forged information about origin or transmission path in From: name (aka "From: display name" or "quoted name.")." Ex. 26 to Mot. at 1. Review of that exhibit indicates that the document is BSI's spreadsheet of codes given to Defendants to show them what is false about each email and is not a labeling demand. BSI's claims are in accordance with this legislative intent. *E.g.*, Exs. 27, 33, 34.

Defendants also mention "To" fields, citing "Book Lover" as an example, but do not identify that any such email is at issue, therefore it is a hypothetical argument. Paul Wagner testified that the "quoted name should contain the identity of the person associated with the mailbox… *or else it should not have a quoted name*." Ex. 16, P. Wagner at 440:5. Notably, Defendant does not mention Mr. Wagner's qualifying statement in its motion. Common sense and the RFCs support this position that the recipient should be identified in the To field. Klensin Decl. ¶ 31; Resnick Decl. ¶¶ 17, 53, 63. This is not a "specific labeling" requirement, but merely

[46] *Subject Line Labeling As a Weapon Against Spam: A CAN-SPAM Act Report to Congress* at 3 (June 2005) *at* www.ftc.gov/reports/canspam05/050616canspamrpt.pdf.

a prohibition against falsity designed to circumvent filters. For instance sending an email to "Mark" <jim@hypertouch.com> is an example of falsity. Klensin Decl. ¶¶ 31, 42-43. Sending the same email content to jim@hypertouch.com with hundreds of different names in the familiar To field (Mark, Marissa, Mack, Macenzie …) is deliberately false. Resnick Decl. ¶ 63; Klensin Decl. ¶ 42. Defendant's argument that BSI's is seeking to impose a labeling requirement is unsupported and untrue, and therefore should be denied.

E. Knowledge Or Intent Are Not Elements Of The Statutes, But Defendants Have Both General And Specific Knowledge of Falsity In Any Event

Again, Defendants try to import requirements that do not exist in the subject statutes. Mot. at 32-33. Knowledge or intent are not elements of the Maryland and California statutes. *See* Md. Comm. Law § 14-3002; Cal. Bus. & Prof. Code 17529.5. As previously stated, once it is determined that fraud is not required, then this argument fails. *Supra* section IV(D).

Defendants, like Captain Renault in Casablanca, are *shocked*, *shocked* to find that *spamming* is going on in here! But their feigned surprise is just that. Defendants regularly receive reports from their third-party monitors LashBack and UnSubCentral (not including what they receive in complaints from individuals, ISPs and their advertisers) of thousands of violations of law.[47] Connexus, for example, received for the period of March 31, 2008, through September 16, 2008, *a total of 3,250 reported possible violations of federal law*, including: 1,699 reports of "Suppression List Abuse," 1,081 reports of "Failure to Unsubscribe," 140 reports of "No Postal Address," 59 reports of "Bad Unsubscribe," 24 reports of "Deceptive

[47] Ex. 1, Hydra's Resps. to Pl.'s RFA Nos. 58, 156, 190; (admitting "Hydra receives reports from third party vendors notifying it of potential violations of CAN-SPAM by its affiliates" and Hydra "ha[s] been warned by advertisers because of complaints regarding emails [its] affiliate sent"); Ex. 2, Connexus' Resp. to Pl.'s RFA Nos. 58, 156 (admitting "Connexus receives reports from third party vendors notifying it of potential violations of CAN-SPAM by its affiliates"); Ex. 5, Stafford Dep. at 43:1-46:22; Ex. 10, Nugent Dep. at 26:2-27:14.

Subject Lines," and 247 reports of "Deceptive From Lines."[48] Likewise, Hydra's compliance manager John Stafford wrote in May 2008:

> In the past 90 days, Hydra has recorded 6,319 Failure to Honor Unsubscribe violations. Deduct 944 for a faulty suppression list for campaign 6495 and allow an overly-generous 30% deduction for errors, and the final count comes to 3,763, or 42 violations per day. Next are the counts for Suppression List Abuse, the most serious of violations; Missing or malfunctioning Unsubscribe Options; Deceptive Subject Lines; and Deceptive From Lines. During the same 90-day period, Hydra was held accountable for 244 Suppression List Abuse Violations; 1,054 Missing or malfunctioning Unsubscribe Mechanisms; 374 Deceptive Subject Lines and 280 Deceptive From Lines.[49]

That's at least 3,763 reported possible violations of federal law over just a 90-day period, some 42 per day. This indicates that Defendants had knowledge if that is relevant.

In addition, Defendants know they are spamming BSI. First, Hydra has known since February 2008, when this suit was filed, that it is spamming BSI, and yet it has sent over 20,000 emails to BSI since then. Further, Defendants "investigated" the addresses they have been spamming, requesting their affiliates provide verification information to show that the addresses opted in. For example, Connexus requested opt-in information from their affiliates for the hypertouch.com addresses in the emails at issue to which it sent spam, all of which were false.[50] Connexus also had fake opt-in information for Joe Wagner's "fg@hasit.com" address, under the name "Russell Fincher," but when the Compliance Manager was told it was false of this, she shrugged it off saying, "I don't know. We take what [the affiliates] give us."[51]

F. Both The Maryland And California Statute Provide A Remedy To Plaintiff

[48] Ex. 37, C00002815-C0002882.

[49] Ex. 38, H00001696-H0001701.

[50] Ex. 39, C00012856-C00012860, attachments at C00012861-C00012862.

[51] Ex. 40, Stevenson Dep. 68:4-69:3.

The only way in which to accomplish the objectives of both Maryland and California in protecting each of their respective citizenries is to enforce both states' laws. Otherwise, this Court must discriminate against one legislature and not enforce its law.

Defendants are wrong that their violation of the anti-spam statute of one state insulates them from liability for violation of the statute of another state. The California and Maryland statutes proscribe different acts. Defendants have violated the California statute by *sending* unsolicited bulk e-mail *from* California. Cal. Bus. & Prof. Code § 17529.5(a) and the Maryland statute by causing illegal emails to be "sent to an electronic mail address that the sender knows or should have known is held by a resident of the State [of Maryland]." Md. Comm. Law § 14-3002(b). When the elements of one cause of action do not duplicate the elements of another, one single act of a defendant can result in multiple causes of action. *See Globe Am. Cas. Co. v. Chung*, 76 Md. App. 524, 539 (1988), *vacated*, 322 Md. 713 (1991); *Microsoft Corp. v. Evans*, Civ. No. 1745, 2007 U.S. Dist LEXIS 77088, at *26–27 (E.D. Cal. Oct. 17, 2007) (holding statutory damages available under both Copyright Act and Lanham Act).

A single wrong can be legally actionable in several – or in fact all – states. Forty states sued tobacco companies to recover damages arising from the identical conduct of tobacco companies. *See, e.g.*, *In re Corr-Williams Tobacco Co.*, 691 So. 2d 424 (Miss. 1997). Each state's citizenry has a separate remedy for the same conduct.[52] Here, Defendants' conduct triggers and violates two separate statutes of two different states. *Gordon*, 575 F.3d at 1063 ("a single e-mail could instantaneously implicate the laws of multiple jurisdictions as it journeys through cyberspace, traveling over various facilities before reaching its intended recipient . . . .").

[52] *See Beyond Systems, Inc. v. Keynetics, Inc*., 422 F. Supp. 2d 523, 535 (D. Md. 2006) ("MCEMA was passed largely because the financial and social burden of UCE on Maryland consumers is great. Maryland certainly has an interest in protecting its consumers, not only from the costs associated with UCE proliferation, but also from becoming the victims of fraud and schemes initiated by false and misleading e-mail. . . .") (quoting *MaryCLE*, 166 Md. App. at 591); Cal. Bus. & Prof. Code. §§ 17529(d).

Defendants completed violating California law when they sent spam from California, § 17529.5(a), and then began violating Maryland law by sending the spam into Maryland to an address presumed to belong to a resident, Md. Comm. Code § 14-3002(c). "One begins where the other ends. . . ." *Globe*, 547 A.2d at 661 (*quoting St. Louis, I.M. &S.R. Co. v. Craft*, 237 U.S. 648, 658 (1915)).

Defendants rely on a single, truncated quotation from *Montgomery Ward & Co. v. Cliser* for the proposition that "'the law does not permit double satisfaction for a single injury,'" Mot. at 35, but ignore the remainder of the quotation that limits its applicability to situations where there is "'recover[y] twice for the same elements of damage growing out of the same occurrence or event'." *Montgomery Ward & Co.*, 298 A.2d 16, 27 (Md. 1972) (quoting 25 C.J.S. *Damages* § 3)). Defendants rely (Mot. at 35) on a single quote from *United States v. Rachel*, but ignore the *Rachel* court's reliance on *Kramer v. Emche*, the most significant and relevant case on this issue. Mot. at 35. *Kramer* instructs courts to permit multiple causes of action "where the injuries sustained are 'related' rather than the 'same.'" 64 Md. App. 27, 39 (1988) (quoting *Huff v. Harbaugh*, 49 Md. App. 661 (1981)). Defendants' act of sending spam from California and to Maryland are related, but not the same. *Kramer* also states that determining whether injuries are "related" or "same," is "a question of fact." *Id.* This alone is sufficient to deny Defendants' motion on this point.

CONCLUSION

Plaintiff respectfully submits that Defendants' motion must be denied.

Respectfully Submitted,

/s/

Thomas M. Barba (US DC-MD Bar No. 28487)
John J. Duffy (US DC-MD Bar No. 28613)
Jennie L. Kneedler (US DC-MD Bar No. 28617)
STEPTOE & JOHNSON LLP
1330 Connecticut Ave NW
Washington, DC 20036
T: 202-429-3000
F: 202-429-3902
tbarba@steptoe.com
jduffy@steptoe.com
jkneedler@steptoe.com

Anthony A. Onorato (US DC-MD Bar No. 28622)
STEPTOE & JOHNSON LLP
750 Seventh Ave., Ste. 1800
New York, NY 10019
T: 212-506-3900
F: 212-506-3950
tonorato@steptoe.com

Of Counsel:

Stephen H. Ring (USDC-MD Bar No. 00405)
Law Offices of Stephen H. Ring, P. C.
20300 Seneca Meadows Parkway, Suite 200
Germantown, MD 20876
T: 301-540-8180
F: 301-540-8195
shr@ringlaw.us

Mike Rothman (USDC-MD Bar No. 14568)
Law Office of Michael S. Rothman
401 E. Jefferson Street, Suite 201
Rockville, MD 20850
T: 301-251-9660
F: 301-251-9610
mike@mikerothman.com

Counsel for Plaintiff Beyond Systems, Inc.

Date: February 18, 2010