

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND

---

BEYOND SYSTEMS, INC.	:	
	:	
	:	
Plaintiff,	:	Case No. 8:08-CV-00409-PJM
	:	
v.	:	The Honorable Peter J. Messitte
	:	
KRAFT FOODS, INC., et al.,	:	Magistrate Judge Charles B. Day
	:	
Defendants.	:	
	:	
	:	

---

**KRAFT’S POST-TRIAL BRIEF AND  
MEMORANDUM IN SUPPORT OF ITS MOTION  
FOR SUMMARY JUDGMENT**

**TABLE OF CONTENTS**

	<b>PAGE</b>
INTRODUCTION .....	1
STATEMENT OF UNDISPUTED FACTS .....	4
I. BSI’S LITIGATION MILL. ....	4
A. Overview.....	4
B. The Origins Of BSI’s Litigation Factory.....	5
C. BSI and Hypertouch Leverage Their Relationship To Multiply Claims. ....	6
D. BSI’s Method For Attracting Spam And Multiplying Claims.....	7
1. BSI’s Use Of Spam Traps To Attract Unsolicited Email. ....	7
2. BSI Knowingly And Intentionally Accepts Spam From Hypertouch.....	9
3. The Wagners’ Contemporaneous Correspondence Further Reflects BSI’s Scheme To Attract And Collect Spam.....	11
E. Band Of Brothers: BSI’s And Hypertouch Coordinate Their Efforts To Sue The Same Defendants On The Same Emails.....	12
1. Kennedy-Western University.....	14
2. World Avenue.....	15
3. Connexus.....	15
4. Kraft .....	16
II. BSI’S ALLEGED BUSINESS OPERATIONS.....	17
A. BSI Makes No Attempt To Block Its Receipt Of Spam. ....	18
B. BSI’s Routing Relationship With Hypertouch. ....	18
C. BSI’s Email Services. ....	19
D. BSI’s Infrastructure.....	19
E. BSI’s Business Operations Generally.....	22

- ARGUMENT ..... 23
- I. PROPERLY CONSTRUED, THE MARYLAND AND CALIFORNIA STATUTES REQUIRE THAT TO HAVE STANDING A PLAINTIFF MUST BE A *BONA FIDE* ICSP OR EMSP ADVERSELY AFFECTED. .... 23
  - A. General State And Federal Standing Requirements..... 23
  - B. Applicable Rules Of Statutory Construction. .... 24
  - C. BSI’s Expansive Definition of ICSP And EMSP Is Unreasonable And Should Be Rejected In Favor Of A *Bona Fide* Requirement..... 25
    - 1. The Statutes’ Definitions of ICSP and EMSP Are Ambiguous..... 25
  - D. The Court Should Construe The California & Maryland Statutes Consistent With The Parallel Provisions Of CAN-SPAM. .... 30
    - 1. The Compelling Rationale For Adopting A *Bona Fide* Requirement Under The State Statutes. .... 31
    - 2. BSI Cannot Establish On The Undisputed Record That It Was “Adversely Affected.” ..... 35
  - E. BSI’s Interpretation Of The State Statutes Raises Issues Of Preemption. .... 38
- II. DEFENDANTS ARE ENTITLED TO SUMMARY JUDGMENT ON THE UNDISPUTED RECORD THAT BSI CONSENTED TO RECEIVE THE EMAILS AT ISSUE. .... 41
- CONCLUSION..... 43

Pursuant to the Court's August 24, 2012 Order, Defendants Kraft Foods, Inc., Kraft Foods Global Inc., and Vict. Th. Engwall & Co, Inc. (collectively, "Kraft") submit the following Post-Trial Brief and Memorandum in Support of their Motion For Summary Judgment.

### **INTRODUCTION**

The Court should enter judgment in Defendants' favor and dismiss Plaintiff Beyond Systems Inc.'s ("BSI") complaint for two independent, yet interrelated reasons. (1) BSI lacks standing to bring its claims in accordance with the jury's Phase II verdict that it is not a *bona fide* Interactive Computer Service Provider ("ICSP") or *bona fide* Electronic Mail Service Provider ("EMSP") under Maryland or California law, respectively. (2) BSI's claims fail as a matter of law given the undisputed evidence that it intentionally invited and consented to the harm it alleges for purposes of manufacturing this lawsuit.

The facts material to this preliminary phase of the case are straightforward and undisputed. By all accounts, BSI is a litigation factory. It is in the business of collecting spam and suing anyone it deems to be a "spammer." All of BSI's activities relate to litigation, to which its owner Paul Wagner devotes forty or more hours a week. BSI has filed over two-dozen spam related lawsuits, seeking millions of dollars in statutory damages for emails it made no attempt to avoid and, in fact, went to considerable lengths to attract. All told, BSI has collected over \$1 million from its litigation venture since 2005, more than three times the revenue from its alleged business operations.

The basic strategy behind BSI's litigation scheme is simple: Place email servers in two states – Maryland and California – with hefty statutory penalties for unsolicited email. Use those servers to seek out and collect as much spam as possible. Route the spam through a server in California first, which then automatically forwards it to a server in Maryland. Archive the emails indefinitely. Mine them for deep-pocket defendants to sue, sometimes years after the

emails were received. Market a prospectus of potential cases to law firms that will take the cases for a contingency fee. Bring separate lawsuits – one in California, one in Maryland – asserting multiple claims on the same emails. Attempt to leverage the sheer volume of emails collected, regardless of whether they are unlawful or not, to coerce large settlements. Rinse and repeat.

This case, and the emails and claims on which it is based, is the direct product of BSI's scheme.

At issue following the Mini-Trial is whether the Court should adopt the jury's Phase II verdict and enter judgment in Defendants' favor on the ground that the Maryland and California definitions of ICSP and EMSP include a *bona fide* requirement similar to CAN-SPAM's analogous definition of "Internet Access Service" ("IAS") provider. As we discuss below, the Maryland and California statutes should be construed to incorporate a *bona fide* requirement to avoid the absurd implications that would otherwise result. While BSI argues that the statutes should be literally construed, that argument, as BSI and its expert Peter Resnick conceded, leads to the illogical and plainly untenable result that anyone who provides a connection to the internet or acts as an "intermediary in sending email – whether it be through a laptop, home Wi-Fi network, or even a cell phone – is an ICSP or EMSP with a right to sue. Clearly that was not the intention of the State Legislatures here. To the contrary, statutory interpretations such as BSI's that lead to "absurdity" or "mischief" are to be avoided. Under well-established rules of statutory construction, courts are to promote substance over form, and give statutes a reasonable and common sense construction consistent with the structure and purpose of the statute as a whole.

Here, reason and common sense dictate the exact opposite of what BSI advocates. Instead, the structure, legislative history, and underlying public policy of the State statutes reflect

that the definitions of ICSP and EMSP should be interpreted to require a *bona fide* requirement similar to the Ninth Circuit's construction of CAN-SPAM in *Gordon v. Virtumundo*, 575 F.3d 1040 (9th Cir. 2009). Faced there with a statutory definition equally ambiguous as those at issue here, *Gordon* sought to construe CAN-SPAM's standing requirements in a way that gave effect to legislative purpose and intent, while striking an appropriate balance between all competing concerns. In doing so, the court concluded that to have any meaningful application at all, standing as a service provider must be limited to *bona fide* service providers genuinely harmed by statutory violations. Not parties who, although possessing the minimal indicia of an email or internet provider, are answering the "siren song" of statutory damages based on claims artificially manufactured through self-inflicted and otherwise avoidable harm.

This same fundamental point – that a plaintiff must have been genuinely harmed before allowed to seek redress – resonates throughout our jurisprudence. Interpreting the Maryland and California statutes to incorporate this basic principle, by requiring not only that they be *bona fide* but also genuinely affected by the statutory violations alleged, avoids the unreasonable and undesired results of BSI's proposed interpretation, while at the same time protects the right of legitimate service providers to seek redress for genuine harms. Just as importantly, it ensures continuity between State and Federal law, consistent with express Congressional intent and the preemption provisions of CAN-SPAM. Accordingly, for the reasons discussed below in Arg. § I., the Court should construe the Maryland and California statutes to require a *bona fide* requirement, adopt the jury's Phase II verdict, and enter judgment in Defendants' favor.

As set forth in more detail in Connexus' Motion and supporting Memorandum, there is an additional ground for dismissing BSI's complaint on the undisputed record. The undisputed evidence establishes beyond doubt that BSI invited, openly welcomed, and thus ultimately

consented to any harm it claims to have suffered. It is fundamental principle of American jurisprudence that a party cannot cry foul over alleged wrongdoing to which it knowingly and intentionally agreed. For this additional reason, BSI's complaint should be dismissed.

**STATEMENT OF UNDISPUTED FACTS<sup>1</sup>**

BSI consists of two separate but related operations. One is the litigation mill through which BSI generated the claims at issue in this case. The other is BSI's provision of limited internet and email services to a handful of "customers" (comprised mainly of family members and friends), which it uses to facilitate and support its litigation efforts.

**I. BSI'S LITIGATION MILL.**

**A. Overview.**

As Wagner admitted at trial, "all of BSI's activity sort of relates to litigation." (6/27, P. Wagner at 107.) To that end, Wagner spends "a good 40 hours a week at least" working on litigation and in some weeks "well over 40." (Ex.1, P. Wagner Dynamic Dep. at 71-72.) In this case alone, Wagner attended up to at least three dozen depositions. (*Id.* at 123.)

Wagner has filed on BSI's behalf more than two-dozen spam-related lawsuits. (6/27, P. Wagner at 112.) Since 2005, BSI has earned over \$1 million from litigation activities. (6/27, P. Wagner at 125; DX 385.A.) Its revenue from business operations is only a third of that, or just north of \$300,000. (*Id.*)

---

<sup>1</sup> Citations to the record are as follows: Exhibits introduced into evidence at trial are denoted as "PX" or "DX." Citations to the trial transcript are referenced by the date of the testimony, the name of the witness, and the transcript page number (*i.e.*, 6/27, P. Wagner at \_\_\_\_.) The transcripts for June 19-21 are divided between morning and afternoon sessions. For these days, we cite to the morning transcript as, *i.e.*, "6/20M" and the afternoon as "6/20A."

**B. The Origins Of BSI's Litigation Factory.**

By any measure, Paul and Joe Wagner are serial litigants. Combined, the brothers have filed close to 70 lawsuits over a five year period, a remarkable number by any stretch. (DX 4; 6/27, P. Wagner at 112; 6/26, J. Wagner at 180.) Paul Wagner began his career in litigation by first going after “junk fax” marketers in the early 2000s. (DX 434; 6/27, P. Wagner at 88-94.) In each of the junk fax cases he filed, Wagner identified BSI's principal place of business as his Washington, D.C. residence. (*Id.*) None of the cases were filed in Maryland. (*Id.*)

That all changed once Maryland enacted the Commercial Electronic Mail Act (“Maryland Act” or “CEMA”) in May 2002, at which point Wagner abandoned his pursuit of junk fax marketers and switched his focus to spam litigation. (DX 39; 6/27, P. Wagner at 98-49.) Wagner's reason for doing so was simple: As he explained to his brother Joe at the time, junk fax lawsuits were “truly small potatoes compared to the spam cases that BSI now has on hand.” (DX 64.) In other words, there was a lot more money to be had in spam litigation. (6/27, P. Wagner at 26-27.)

Wagner knew as early as August 2002 that CEMA had been enacted and was to become effective October 1, 2002. (DX 36; 6/26, J. Wagner at 156-57.) In September, he purchased from Joe for \$1 a “little MacIntosh email server” (*i.e.*, “mini-Mac”) that Joe had left at their parents' Maryland home. (DX 39; 6/26, J. Wagner at 152-58.) Wagner designated the server as BSI's “mail gateway” (DX 70.1) and, despite the fact he lived in D.C., left it in Maryland in order to avoid any argument that mail sent to the server was not covered by the Maryland Act. (DX 103; DX 108.)

**C. BSI and Hypertouch Leverage Their Relationship To Multiply Claims.**

The Wagner brothers began marketing potential spam cases to prospective law firms towards the end of 2002. (DX 55; DX 57; DX 64.) In December 2002, Paul and Joe drafted a “report on illegal spam received by Beyond Systems of Maryland” to send to law firms “to try to get them to see if they were interested in helping [BSI] sue.” (6/26, J. Wagner at 94-97, 98-99.) Among other things, the “pitch piece” emphasized that BSI’s “email counts” and “corresponding damages” were “increas[ing] daily,” and that they expected to obtain more spam from marketers who had “only discovered BSI as a target.” The email stated:

It is important to keep in mind that BSI observes an INCREASING volume of spam directed to its servers. Moreover, we continue to encounter NEW SOURCES of spam, such as domain names associated with BSI that already receive streams of UCE’s but are being discarded. As a result, the email counts (and corresponding damages) increase daily. Many of the spammers with lower counts only recently discovered BSI as a target . . . we have only been collecting data for 2+ months. It is also well known that spammers often sell and trade their email address lists.”

(DX 55.2 (caps in original).)

In subsequent correspondence, Paul suggested they revise the report to emphasize the number of potential defendants BSI had already identified “who are bound to hold significant insurance and/or assets.” (DX 57.1.) Joe responded that they should include in the “report” a statement to the effect that: “[w]hile none of the current round of defendants are well know[n] businesses, the size and diversity of businesses will grow[] as the spammer’s lists propagate and merge with other lists.” (*Id.*; 6/26, J. Wagner at 98-99.)

Paul was even more explicit about BSI’s intent to “trap spam” in a later email:

The spammers are often small operations, but the clients tend to be larger and more established. According to the Maryland statute, either conspirator is on the hook . . . California law has a different form of anti-spam law *with incentives for ISP’s to trap spam.*

(DX 64.1 (emphasis added); 6/26, J. Wagner at 100 (Q: “You and your brother were telling the prospective lawyer that you’re sending this to . . . that this could be a good investment because the anti-spam laws have incentives for ISP’s to trap spam; correct? A: Yes.”)

“Trap spam” is exactly what BSI did.

**D. BSI’s Method For Attracting Spam And Multiplying Claims.**

**1. BSI’s Use Of Spam Traps To Attract Unsolicited Email.**

Both Wagners admitted that 99% of all emails BSI receives are spam. (6/26, J. Wagner at 159, 160-61; 6/20A, P. Wagner at 54.) Knowing this, BSI takes no action to filter incoming emails, or to block or reject the delivery spam. (6/22, Marti at 66; 6/21A, Resnick at 54; 6/26, J. Wagner at 163-64, 169; 6/20M, P. Wagner at 43-47.) Instead, it is BSI’s “policy” to accept and archive indefinitely *all* incoming email, including emails addressed to non-existent users or accounts. (*Id.*)

To increase its flow of incoming spam, BSI also intentionally set “spam traps” designed to attract spam to fictitious and otherwise unused email accounts created solely for the purpose of collecting such emails. BSI’s expert witness, Dr. Peter Resnick, described a spam trap as an email address or account “whose sole purpose is to cause spammers to send spam to it.” (6/27, Resnick at 159.) As he explained:

One of the ways that a spam trap might happen is if there’s an email address that appears on a website, maybe hidden, you know, behind a picture or something. It’s just a web page, but they know they’ve never given that out to anybody as an e-mail address. It’s hiding in the hidden text. Many folks who send out unsolicited commercial e-mail or any kind of spam, for that matter will do searches on web pages looking for things that look like email addresses. Well, if one of them comes across this web page and finds something that looks like an e-mail address, they try and send it a piece of spam.

(6/21A, Resnick at 56-57; 6/27, P. Wagner at 111.) Another BSI expert, Dr. Richard Levine, explained in his deposition that “the more you publish an e-mail address, the more likely it is that

that address will get spam. And if the address happens to be handled as a spam trap, as a catchall, then the catchall will get a lot of spam. It can be used as a spam trap.” (Ex. 2, Levine Dep. at 631-32.)

A “catchall,” or “wildcard,” is an account that accepts all email sent to a certain domain name, even if the email was not addressed to a real user or address. (6/27, P. Wagner at 108-09; 6/26, J. Wagner at 61-63.) Email sent to a domain but not addressed to an existing account is likely to be spam. (6/26, J. Wagner at 76.) The Wagners admitted that BSI uses wildcards, two of which they identified as \*@hypertouch.com and \*@safemailbox.com. (6/26, J. Wagner at 82; 6/27, P. Wagner at 109.)

Consistent with Resnick and Levine’s description of a spam trap, Defendants’ Exhibits 360 and 361 are screen shots of a website Hypertouch posted that published thousands of randomly generated, fictitious names and email addresses to BSI’s hypertouch.net and safemailbox.net wildcard accounts. (DX 360, 361; 6/26, J. Wagner at 82, 83, 109-113.) The actual email addresses were hidden behind the website text where, as Resnick explained, they would be picked up by mechanical “spam crawlers” looking for addresses to which to send spam. (6/26, J. Wagner at 111.)<sup>2</sup> Emails sent to the fictitious addresses were delivered to BSI, some directly, others indirectly through Hypertouch’s servers. (*Id.* at 112-13.)<sup>3</sup>

---

<sup>2</sup> That BSI used wildcards for the purpose of collecting spam is also reflected, *inter alia*, by a November 26, 2002 email exchange in which Joe wondered if the reason BSI had not yet received certain spam emails to its safemailbox.net address was that it had been “flagged as a trap address.” (DX 50.1) Paul responded: “Are there Web sites that assist spammers by listing trap addresses? Or is that info only shared by small teams of spammers privately? (I can’t believe that the diverse set of spammers I communicated with all would fear the safemailbox.net domain; perhaps it takes a few days . . . .)” (*Id.*)

<sup>3</sup> Another way the Wagners attracted spam was through “opt-out” links. (6/26, J. Wagner at 108; 6/27, P. Wagner at 110-11); DX 50.1, 11/25/02 email from Joe to Paul: “Now I can say with first hand knowledge that removes just get one’s address signed up for more spam.” Paul

**2. BSI Knowingly And Intentionally Accepts Spam From Hypertouch.**

The email server responsible for accepting delivery of an email sent to a particular domain name is determined first by the mail exchanger record, or “MX record,” created for that domain. (6/21M, Resnick at 88-89; 6/26, J. Wagner at 64-66). Once at the designated server, the mail is then routed to its addressed recipient by that server’s “routing tables” or “routing rules.” (6/26, J. Wagner at 66; 6/27, Resnick at 153, 155; 6/27, J. Wagner 82-85.)

Here, the Wagners configured their MX records to deliver emails sent to their domains to Hypertouch’s servers in California. (6/26, J. Wagner at 66, 70, 159; 6/21A, Resnick Dep. at 77-78.)<sup>4</sup> Upon its arrival, mail would be automatically routed to its addressed account or inbox by the “routing tables” Joe created. (6/26, J. Wagner at 61-62, 66.) If an email did not “match” the servers’ routing rules – *i.e.*, it was not addressed to a real user or account and, therefore, likely spam – Hypertouch’s servers automatically forwarded the email BSI. (*Id.* at 61-62.) As Joe explained: “when spam comes in, there is a routing table that routes email to various accounts. And if it does not match any of the routing rules for all the other accounts . . . it is routed to BSI.” (*Id.* at 61.)

In short, the Wagners set up Hypertouch’s routing tables to intentionally route spam to BSI. As Joe testified:

---

responds: “if you want to add to my list of removal sites, I’ll submit opt-out requests to them as well.”)

<sup>4</sup> Joe Wagner claimed that he asked Paul in 2002 or 2003 if he could route spam to BSI’s servers because he was running out of server capacity to handle them all. (6/26, J. Wagner at 158-59.) But as Resnick testified, Wagner could have as easily routed the emails to another Hypertouch server, as opposed to sending them to BSI. (6/27, Resnick at 154-55: “Q: Joe Wagner could have another server set up so that whatever email was or is being routed to Paul Wagner in Maryland is routed to another server within his garage, correct? A: Sure, lots of companies do that sort of thing, exactly that.”)

Q: And you knew at that time that the emails, the Hypertouch.com emails that you would be routing [to BSI] contained spam; is that right?

A: Absolutely.

Q: And you asked Beyond Systems to receive those emails, right?

A: Yes.

Q: And Beyond Systems said yes, correct?

A: Yes.

(6/26, J. Wagner at 170.)

Both Wagners admitted that Hypertouch or BSI could have “bounced” or rejected the incoming spam instead of accepting delivery. (6/26, J. Wagner at 162-63; 6/20M, P. Wagner at 42-48; 6/22, Marti at 66-67.) The mail delivery software they used, for example, allowed them to reject delivery of “fraudulent” emails sent to their domains that did not match their servers’ routing tables.<sup>5</sup> (*Id.* at 163-64; DX 135.) The Wagners turned this setting off on both their email servers:

Q: So there was a setting in CG Pro that allowed you to bounce a fair bit of e-mail and specifically the fraudulent ones, correct?

A: That would include fraudulent ones, yes.

Q: And that setting was turned off?

A: Correct.

Q: By Beyond Systems?

A: Yes, it was turned off in both of our systems.

(6/26, J. Wagner at 164-65.)

---

<sup>5</sup> For example, if an email were addressed to xyz@hypertouch.com and there was not a corresponding mailbox for this address, the email would normally be rejected. The Wagners, however, disabled this feature so that they would capture the erroneously addressed email message.

According to Joe, that was “the whole point” of setting up the routing tables the way they did. BSI “want[ed] to collect spam.” (6/26, J. Wagner at 80-81, 170.)

**3. The Wagners’ Contemporaneous Correspondence Further Reflects BSI’s Scheme To Attract And Collect Spam.**

While this testimony leaves no room for doubt, the Wagners’ contemporaneous email correspondence – produced after four years of litigation only weeks before the Mini-Trial – provides an equally compelling window into BSI’s actions. The evidence includes:

- DX 135: Email from Joe to Paul: “Looks like you’ve turned on return-path verification . . . Unfortunately in CGPro that means if it doesn’t verify, you don’t accept the email. So . . . you are bouncing a fair bit of email and specifically the fraudulent ones . . .” Paul responds: “Thanks! Glad you’ve been through all of this already.” Joe testified that he was “worried,” because CGPro “wasn’t set correctly,” that BSI’s email server “was not going to accept spam.” (6/26, J. Wagner at 77.)
- DX 132: Email “Re: spam should be flowing again.” Paul to Joe: “No emails have arrived yet – but perhaps it takes a moment . . . It’s a floodin’ all right! Txs.” Joe responds: “Cool.”
- DX 159: Email from Paul to Joe: “One thing – I am once again not receiving Hypertouch spam to support@beyonddsystems.net (since 9/1/2004). Can you check whether you are forwarding me such emails, please. . .?” (6/26, J. Wagner at 78-79.)
- DX 173: Email “Re: Ema no longer receiving hypertouch.com spams.” Paul to Joe: “ema.beyonddsystems.net went down for 14 hours, until 90 minutes ago (when mom rebooted it). Can you please resume the flow of emails to it?” Joe responds: “The smtp hold is released, 61000 messages are on their way.”

- DX 185: Email from Joe to Paul: “spam should be flowing now.” As Joe explained at trial, the mailbox referred to in the email’s re line, safemailbox@linkcenter.net, was hosted by one of BSI’s email servers, Linkcenter. (6/26, J. Wagner at 81-82.)
- DX 108: Email from Paul to Joe: “Joe, am now receiving Hypertouch spam again (to beyondsystems.net), as usual. Everything normal. Thanks.” (6/26, J. Wagner at 64.) Paul goes on to ask: “This evening I will bring [a server] up to the parents’ house. Do you want to point Hypertouch’s spam to it as the first recipient . . . It can forward copies to our California and DC servers. Motivation: Protection of Maryland anti-spam law.” (*Id.* at 65-66.)
- DX 155: Email “Re: spam stoppage.” Joe to Paul: “It looks like I haven’t received any Hypertouch spam (which you normally forward to support@beyondsystems.net, I think) since August 22, 2004. Do you mind checking that, please?”
- DX 152: Email “Re: spam to hypertouch.com.” Paul to Joe: I don’t seem to be getting much Hypertouch spam, if any, lately. Do you mind checking that?”
- DX 112: Email “Re mail is back to forwarding.” Joe to Paul: “When I checked at 10pm, PST, the queue was empty so I restarted the forwarding.” Paul responds: “Thanks. Now that I think about it, the number of spams to support@beyondsystems.net did slow to a virtual standstill for a few hours.” (6/26, J. Wagner at 73.)

**E. Band Of Brothers: BSI’s And Hypertouch Coordinate Their Efforts To Sue The Same Defendants On The Same Emails.**

BSI filed the first of its two dozen spam-related lawsuits in December 2003. Hypertouch, in turn, filed its first suit under CAN-SPAM (the first of at least 45 other suits filed by Joe and Hypertouch) in March 2004, against celebrity handyman Bob Vila and BlueStream Media. (DX 4.9; DX 130; 6/26, J. Wagner at 113-16.) It appears to have been in the context of the Vila case

that Paul and Joe decided to coordinate their future litigation efforts by targeting the same defendants and suing on the same emails. Paul wrote to Joe:

Since this may turn out to be an important lawsuit and press release, why not include in your statement the key elements of your earlier piece on the 6+ problems with CAN-SPAM. Couple of questions: 1. How many spams has Hypertouch received from them? 2. Which email addresses were the recipients, and doesn't Beyond Systems own most of the email accounts provided by Hypertouch? (*Should I look for Blue Stream spam? Not sure if there'd be added value if Beyond Systems were to participate . . .*)

\* \* \* \* \*

Oh yeah, I forgot momentarily that Beyond Systems, the recipient, is powerless under "I CAN SPAM." *Maybe as Hypertouch is finishing up with them, Beyond Systems can step in under the Maryland law "Ding. Dong. Another package for Mr. Vila.*

(DX 130.1 (emphasis added); *see also* 6/26, J. Wagner at 116: "Q: And Paul is saying as soon as your suit gets done, I can bring a suit, ding dong, Mr. Vila's going to get sued again; correct? A: Yes.")

The Wagners concluded that they could multiply their claims and maximize their damages by routing emails through both California and Maryland. (DX 154, 130, 176, 247.1; 6/26, J. Wagner at 54-56 (explaining the brothers' belief that they could pursue at least three separate claims for each email routed to BSI through Hypertouch). At some point, they decided that the best way to maximize their recovery would be to bring separate lawsuits in different jurisdictions. Hypertouch would sue on the emails they collected in California first. BSI would then sue on the same emails in Maryland, seeking two sets of statutory damages for each email under California and Maryland law. (DX 154; 6/26, J. Wagner at 54-56.)

To shield their efforts from discovery, BSI and Hypertouch entered into a joint-defense agreement under which they shared litigation strategy and acted as consultants on each other's cases. (DX 349.2, ¶¶ 8-9; 6/26, Steve Wagner at 144, 147-49, 151.) Over the next five years,

they brought separate claims in California and Maryland against several of the same defendants, asserting claims on the same emails. These defendants included Kennedy-Western University, World Avenue, Connexus and, of course, Kraft.<sup>6</sup>

**1. Kennedy-Western University**

The Wagners identified Kennedy-Western University as a potential defendant sometime in 2004. Initially, the brothers debated whether to file the claim together, or in separate lawsuits. (DX 174; DX 176; 6/26, J. Wagner at 125-27.) Joe expressed concerns that separate suits would “double[] the work” without increasing their recovery. (DX 174.2.) Paul on the other hand opined that separate cases – one in Maryland, the other in California – made sense because: (i) “Maryland has no [] reduction of statutory damages, even if the defendant could show he implemented a serious anti-spam policy;” (ii) BSI had received a handful of Kennedy Western emails “without Hypertouch involvement – some possibly because Hypertouch’s services were down”; and (iii) costs could be shared because BSI had “much of the work product of filing in [Maryland] already. One team could forgo deposing the defendant all together, or do a follow up the first team’s depo. If one team were denied supplemental discovery, the other might hopefully be granted it.” (DX 174.1; 6/26, Wagner at 119-123.)

Ultimately, Hypertouch filed suit against Kennedy-Western first. (DX 4.9.) BSI filed its own complaint against the University in Montgomery County Circuit Court five months later. (DX 4.6.)

---

<sup>6</sup> Other companies against whom Joe and Paul considered filing duplicative suits over the same emails included ValueClick (which Hypertouch sued in 2008, *see* DX 4.8; 6/27, J. Wagner at 13), Experian and Ameriquest Mortgage Co. (DX 247.)

**2. World Avenue**

Joe Wagner sued World Avenue in 2007, recovering a judgment against the company in California state court. (6/27, J. Wagner at 15, 17.) BSI then sued World Avenue in this Court over emails Hypertouch had delivered to BSI. (*Id.*, DX 4.13) That case settled for \$1.1 million, of which \$600,000 was paid to BSI. Although not a plaintiff in the case, Hypertouch received \$475,000 of the settlement proceeds. Joe Wagner was paid the remaining \$25,000. (6/27, J. Wagner at 16-17.)

BSI is suing Kraft and Connexus for many of the same emails Joe Wagner sued on and settled in *World Avenue*. (DX 8; 6/27, P. Wagner at 124.)

**3. Connexus**

In 2005, Joe Wagner threatened to sue Connexus' successor, Vendare, in California state court. The case settled before a complaint was filed. The last email Wagner determined Hypertouch received from marketing affiliate, MailBox X, was sent before January 31, 2006. (6/27, J. Wagner at 13-14.)

While settling his claim against Vendare, Joe continued to route Mailbox X emails from Hypertouch to BSI. (*Id.* at 20-22.) In a 2006 prospectus of potential litigation, BSI identified Connexus/Vendare as one of several companies against whom BSI and Hypertouch "would have parallel claims for most of the emails below – i.e., those [Hypertouch] helped deliver to BSI." (DX 247.1, 3.)

Two years later, in 2008, BSI filed the present case against Connexus. The emails over which BSI is suing include the Mailbox X emails Hypertouch forwarded BSI three years earlier in 2005 while Joe Wagner was threatening to sue and then settling his claim against Vendare. (*Id.* at 20-22.)

4. **Kraft**

The Wagners' claims against Kraft are perhaps their most brazen attempt to manipulate the system. The Wagners began contemplating their Kraft lawsuits in 2004, in conjunction with their claims against Kennedy-Western. (DX 174; DX 178F; 6/26, J. Wagner at 123-28.) As with their other cases, Hypertouch filed the first complaint in April 2005. (6/26, J. Wagner at 129; DX 4.9.)

Kraft and Hypertouch settled that case on June 29, 2006. (DX 239.) The settlement agreement included what Joe Wagner characterized as a "broad release," under which Hypertouch agreed to release all known and unknown claims against Kraft. (DX 239.2, ¶¶ 2; 6/26, J. Wagner at 130.) The agreement also included a release of future claims intended to ensure the parties' cooperation in the event Hypertouch received any Gevalia emails post-settlement. In such an event, Wagner agreed to notify Kraft of the emails within 20 days of their receipt. (DX 239.4 ¶ 3(c).) Kraft, in turn, agreed to help Hypertouch identify the sender(s) of the emails. (*Id.*) If Kraft failed to do so, only then could Hypertouch bring a new claim against Kraft. (*Id.*; 6/26, J. Wagner at 131-32: "Q: So the understanding was, [Kraft was] going to get a release from you, we're going to buy peace, but if you have problems with spam in the future, you're going to let us know promptly, and we'll help you identify the spammers, and then you can pursue them if you want . Do you recall that? A: Yes.")

It is clear from the evidence that Wagner had little intention of complying with the parties' agreement even before he signed it. (6/26, J. Wagner at 136-37.) A week before the agreement was executed, Wagner sent an email to Hypertouch's lawyers suggesting they include a stipulation by Kraft of an agency relationship between Kraft and its marketing affiliates. The reason, Wagner explained, was he believed it would be "a very valuable admission *for anyone*

*else* who might sue them, especially under their own state’s spam laws, *e.g. Maryland* or *WA.*” (DX 237.1; 6/26, J. Wagner at 133-34 (emphasis added).)

The same day Kraft and Hypertouch signed their agreement, Joe and Paul’s brother Steve Wagner informed Paul that he and Joe “are having Dan Balsam prepare a draft Complaint and MSJ for ‘BSI v. Kraft’ in Maryland” and that [i]deally this will make his case all the more attractive to Chadbourne (DC).” (DX 238.1.) Balsam sent Steve and Joe the draft complaint two weeks later, which Steve forwarded to Paul with the comment that: “I don’t have much time to devote to this. Maybe between the 3 of us we can come up with universal comments over the weekend.” (DX 243.1; 6/26, J. Wagner at 137-38.)

Two months later, the Wagners began marketing to prospective law firms their “top 5 potential spam suits,” which included a potential suit by BSI against Kraft. (DX 248.) The prospectus stated that almost 10,000 of the emails on which BSI intended to sue had been delivered through Hypertouch to BSI, including 381 emails *after* “Hypertouch’s Settlement Agreement was signed.” (DX 247.2.) As he admitted, Joe knew that he and Paul were receiving Gevalia emails following his settlement agreement with Kraft, but he chose not to notify Kraft of this fact. (6/26, J. Wagner at 140.)

## **II. BSI’s Alleged Business Operations.**

In contrast to BSI’s well-organized litigation operation is the rudimentary and haphazard operation it portrays as an ICSP/EMSP. In Phase I, Defendants presented the expert testimony of Willis Marti, the Director of Networking and Information Security at Texas A&M University. Mr. Marti has over 30 years of experience working with internet and email service providers, having developed and managed the installation, operations, engineering, security and support of several large computer networks since 1978. (6/22, Marti at 38-42.) Marti described for the jury the typical characteristics of *bona fide* internet and email service providers with respect to their

customary practices, policies, and infrastructure. He concluded that BSI's operations are not consistent with and, in many instances directly contrary to, the industry-wide customs and practices of legitimate providers. (*Id.* at 49.)

**A. BSI Makes No Attempt To Block Its Receipt Of Spam.**

As discussed above, BSI refuses to take even the most minimal of steps to block or filter unsolicited emails. None of BSI's witnesses could identify another email provider who does not filter spam.

For example, BSI's expert witness, Dr. Peter Resnick, testified that his expertise in the area of email practices and protocol is virtually unparalleled. (6/21M, P. Resnick at 57.) According to Resnick, there are "only a couple dozen people" in the world who "know as much about the details of e-mail protocols as I do." *Id.*

As one of the world's leading experts regarding email practices, Resnick was unable to identify a single email provider that, like BSI, accepts all incoming email, makes no attempt to block or filter unsolicited mail, or archives all mail indefinitely. (6/21A, Resnick at 84.) Neither could the Wagner brothers. (6/20A, P. Wagner at 48; 6/26, J. Wagner at 179.) Marti testified that no legitimate ISP engages in this practice. (6/22, Marti at 64-67, 71.)

**B. BSI's Routing Relationship With Hypertouch.**

According to Resnick, BSI's routing relationship with Hypertouch is also uncharacteristic. (6/21A, Resnick at 77-79) Resnick described BSI's routing of emails as "an uncommon arrangement" and a "strange historical set of facts." (*Id.* at 78.) Again, Resnick could not identify any other email service provider that configures the delivery of emails like BSI. (*Id.* at 80.)

**C. BSI's Email Services.**

BSI does not connect customers to the internet. At most, it installs or provides equipment such as cabling, routers, or “air cards” that carry or transmit the internet connection provided by a customer’s ISP, such as Comcast or Verizon. (DX 31.1; 6/20A, J. Clark at 86, 100; 6/21M, L. Sykes at 32, 33-34.)

Although Wagner claims that BSI offers several internet-related services, none other than email service bears any relevance to the case. Wagner testified that BSI “hosts” email for only four customers. (6/20M, P. Wagner at 77.) Of the two customers BSI called to testify, it provides no email services to one (Thompson-Markward Hall), and with the other (St. Luke’s House) it provided only secondary and DNS service. (6/20, J. Clark at 83-84.) BSI provided these services to St. Luke’s free of charge as a “volunteer.” (*Id.* at 98-100.)

**D. BSI's Infrastructure.**

Office Space. Internet service providers of the type BSI claims to be customarily invest in a dedicated office space with the type of infrastructure and security measures necessary to provide a robust and reliable service. BSI’s offices are located in private residences owned by Wagner and his parents. (6/20M, P. Wagner at 55-58, 60, 71-72; 6/27, P. Wagner at 129.) Two of the locations at which BSI keeps its email servers are owned by Wagner’s parents in Silver Spring and Rockville, Maryland. (6/20M, Paul Wagner at 55-58, 60, 71-72.) The third is Wagner’s own residence in Washington, D.C., which he shares with several housemates. (*Id.* at 71-72, 79-80.)

The owner of BSI’s Maryland “offices” – Wagner’s father, William Wagner – was unaware Wagner was operating a business out of either of his homes. William Wagner testified that he did not know why Paul stored computers in his Maryland homes, whether the computers were operational, who used the computers, or why BSI received mail at the Silver Spring

address. (Ex. 3, W. Wagner Dep. at 31-33, 38-39, 78-79, 86.) Wagner never asked his father if he could operate a business out of his Maryland residences, and William Wagner testified that he would be “surprised” to learn that BSI had offices at his residences. (*Id.*)

Equipment. The nerve center of any email service provider is the email servers and software used to deliver and store client emails. BSI has two active email servers. (6/19A, P. Wagner at 75.) For several years, if not still today, one of BSI’s email servers was an antiquated “mini” McIntosh computer Wagner purchased from his brother Joe for \$1. Joe testified that Paul “overpaid” for the machine.” (6/26, J. Wagner at 152-158.)

For its email delivery software, or “mail transfer agent,” BSI uses a free “trial” or “beta” version of CommuniGate Pro. As Marti explained, beta software is often unreliable given it has not been fully tested. (6/22, Marti at 77-78.). Such software can cause service disruptions, delivery delays, and lost emails. (*Id.* at 77.) For this reason, legitimate email service providers customarily use robust, well-tested and well-supported mail transfer software to avoid service disruptions and loss of client data. (*Id.* at 77-78.) Neither Marti nor Resnick were aware of an email provider other than BSI that used beta software for its mail transfer agent. (6/22, Marti at 77-79; 6/21A, Resnick at 86.)<sup>7</sup>

Physical and Digital Security Measures. BSI also lacks the physical infrastructure and security measures customary of legitimate email service providers. Physical security measures necessary to ensure the continuity of a robust service typically include: (i) housing servers in wire cages (6/22, Marti at 56); (ii) proper cable structuring to ensure quick and easy identification and access in the event of system failure (*id.* at 53-55); (iii) appropriate fire prevention measures (*id.* at 50, 96); and (iv) appropriate redundancy measures and incident

---

<sup>7</sup> Another mail transfer agent BSI used at various points, Eudora, was according to Resnick also unstable, “buggy”, and unreliable. (6/21A, Resnick at 84-85.)

response plans to protect against disruptions in service and lost customer data in the event of equipment or software failure. (*id.* at 58-60, 81-82, 101.)

BSI does not employ even the most basic of these measures. Its email servers are housed haphazardly in basement and bedroom home offices on the floor, in closets, and on tables. (6/22, Marti at 50-56; 6/19A, P. Wager at 66-67.) Its cabling is unstructured and disorganized, and it does not maintain a functional diagram. (6/22, Marti at 74-75.)<sup>8</sup> Its machines run unattended 24-hours a day, and are at risk of overheating if their cooling components failed. The only fire prevention measures BSI has available, however, are a garden house and household fire extinguisher. (6/20M, P. Wagner 56-57.)

BSI also lacks redundancy measures or an incident response plan to protect customer data and avoid service disruptions in the event of equipment failure. (6/22, Marti at 58-60, 80-82, 99.) Wagner often leaves the servers unattended for days and sometimes weeks at a time. (*Id.* at 59; DX 25) On one occasion, BSI's servers crashed and were down for a period of time while Wagner was out of the country. (*Id.*) On another, Wagner had to ask his mother to reboot BSI's servers to correct an equipment failure and service disruption. (6/22, Marti at 75-77; DX 173.)

Nor does BSI have in place the standard policies and agreements customary of internet or email service providers. Contrary to industry practice, BSI does not maintain a privacy policy, customer agreements, acceptable use policies, terms of service agreements, or uptime policies. (6/22, Marti at 79-84; 117.)

---

<sup>8</sup> Marti testified that BSI's attorneys showed him PX16 at his deposition, which purports to be BSI's "functional diagram." As Mr. Marti described it, the diagram consists of 64 boxes, 10 of which are left blank, with a "meaningless" line connecting them. (6/22, Marti at 74-75.) According to Marti, he would have "flunked" any student who turned this in to him as an example of a functional diagram.

**E. BSI's Business Operations Generally.**

BSI also lacks the usual indicia of any business, large or small:

Business Plans. BSI has no business plan, marketing plan, does not maintain customer or pricing lists, and does not use standard customer agreements. (6/22, Marti at 79-84.)

Marketing. BSI does not advertise, market, or promote its services. It instead relies entirely on "word of mouth around town." (6/20M, P. Wagner at 24.)

BSI's website consists of a single page of text that does not provide prospective customers the company's address (or even the city where it is located), phone number, or the name of anyone at BSI to contact to discuss BSI's services. It does not offer prospective customers the ability to open an account online. (Ex. 4.) The only contact information given is a generic email address, info2011@beyondsystems.net. In lieu of other information one might expect to find on a business website, the page posts links to two pages that identify the spam-related lawsuits BSI has filed and documents presumably filed therein. (*Id.*) The pages invite anyone with "additional information" about the lawsuits to "please contact us at info2011@beyondsystems.net, the same email address given to prospective customers. (*Id.*)

Source of Revenue. BSI has only "roughly ten" paying customers, most of whom are family, friends, including one of its attorneys in this case. (6/20M, P. Wagner at 76-81.) Since 2005, at least seventy-five percent of BSI's total revenue has come from repeated litigation. (6/27, P. Wagner at 125-26.)

## ARGUMENT

### **I. PROPERLY CONSTRUED, THE MARYLAND AND CALIFORNIA STATUTES REQUIRE THAT TO HAVE STANDING A PLAINTIFF MUST BE A *BONA FIDE* ICSP OR EMSP ADVERSELY AFFECTED.**

#### **A. General State And Federal Standing Requirements.**

We begin with an overview of the general principles underlying the central issue to be decided, whether BSI has proven standing to pursue its claims.

It is axiomatic that a plaintiff must have “constitutional standing to invoke the authority of an Article III court.” *See, e.g., Fla. Audubon Soc’y v. Bentsen*, 94 F.3d 658, 664 (D.C. Cir. 1996). Article III requires plaintiffs to satisfy three elements: (i) they must have suffered a concrete “injury-in-fact”; (ii) the injury must be “fairly traceable to the challenged action of the defendant;” and (iii) “it must be likely . . . that the injury will be redressed by a favorable decision.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

Maryland and California standing requirements are in accord. *See Norman v. Borison*, 192 Md.App. 405, 420 (2010) (“In order to have standing, a party must demonstrate an ‘injury-in-fact’ . . .”). Indeed, the standing requirements imposed by the Cal. Bus. & Prof. Code are even more stringent. Following Proposition 64, passed by California voters in 2003 to prohibit previously-allowed actions by “private attorneys general,” plaintiffs suing under the unfair competition and false advertising provisions of that statute must have “suffered injury in fact *and* [] lost money or property as a result of a violation of this chapter.” CAL. BUS. & PROF. CODE § 17535 (emphasis added); *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322, 324 (2011) (“because economic injury is but one among many types of injury in fact, the Proposition 64 requirement that injury be economic renders standing under section 17204 substantially narrower than federal standing under [A]rticle III . . . which may be predicated on a broader range of injuries” (citations omitted)).

In addition, it is well-established that to have standing under federal diversity jurisdiction, a plaintiff must satisfy both state *and* federal standing requirements. *See, e.g., Mid-Hudson Catskill Rural Migrant Ministry, Inc. v. Fine Host Corp.*, 418 F.3d 168, 173 (2d Cir. 2005) (“Where [] jurisdiction is predicated on diversity of citizenship, a plaintiff must have standing under both Article III of the Constitution and applicable state law in order to maintain a cause of action”); *Cantrell v. City of Long Beach*, 241 F.3d 674, 683 (9th Cir. 2001) (“California’s lenient taxpayer standing requirements do not relieve the [plaintiffs] of the obligation to establish direct injury under the more stringent federal requirements.”); *Metropolitan Express Serv., Inc. v. City of Kansas*, 23 F.3d 1367, 1369 (8th Cir. 1994) (same).

Accordingly, even where a diversity plaintiff may have standing under state law, its claim must be dismissed if Article III standing is lacking. *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 804 (1985) (“Standing to sue in any Article III court is, of course, a federal question which does not depend on the party’s [] standing in state court.”); *Goode v. City of Philadelphia*, 539 F.3d 311, 321 (3d Cir. 2008) (“[E]ven if Pennsylvania state law would have afforded appellants standing if they had brought this action in state court, we must ensure that they satisfy the federal requirements for standing as well.”).

**B. Applicable Rules Of Statutory Construction.**

While the starting point of any statutory analysis is the statute’s plain meaning, “[a] cardinal rule of statutory construction is that a literal meaning of a statute may be disregarded to avoid an absurd result.” *Woodliff v. California Ins. Guarantee Assn’n*, 110 Cal. App.4th 1690, 1705 (2003) (rejecting the literal interpretation of statute because “realistically, such a conclusion is not acceptable”); *see also People v. Pan Am. Sulphur Co. v. State Dept. of Assessments & Taxation*, 251 Md. 620, 627 (1968) (“It may be contended that this Court is reading something into [the statute] which is not there . . . However, if the ordinance is not so

construed, an almost absurd result is reached . . . One of the cardinal rules of statutory construction is that wherever possible an interpretation should be given to statutory language which will not lead to absurd consequences.”) Courts, therefore, “should reject a proposed statutory interpretation if its consequences are inconsistent with common sense.” *Forster v. State, Office of Public Defender*, 426 Md. 657, 592-93 (2012); *see also S.D. Myers v. City and County of San Francisco*, 336 F.3d 1174, 1179 (9th Cir. 2003) (California rules of statutory construction require that statute ““under scrutiny must be given a reasonable and common sense interpretation consistent with the apparent purpose and intention of the lawmakers, practical rather than technical in nature, which, upon application will result in wise policy rather than mischief or absurdity.”” (citations omitted)); *Gordon*, 575 F.3d at 1049 (“[c]ommon sense not dogma is what is needed in order to explore the actual meaning of legislative enactments.””)

Accordingly, when presented with competing statutory interpretations, courts are to reject the construction that would lead to an absurd or “unwise” result in favor of the interpretation that is reasonable, fair, and consistent with legislative intent. *See, e.g., People v. Lungren*, 14 Cal.4th 294, 305 (1996); *U.S. v. Ryan*, 284 U.S. 167, 175 (1931) (“A literal application of a statute which would lead to absurd consequences is to be avoided whenever a reasonable application can be given which is consistent with the legislative purpose.”)

**C. BSI’s Expansive Definition of ICSP And EMSP Is Unreasonable And Should Be Rejected In Favor Of A *Bona Fide* Requirement.**

**1. The Statutes’ Definitions of ICSP and EMSP Are Ambiguous.**

The Maryland and California statutes grant ICSPs and EMSPs a private right of action for the receipt of unsolicited email containing false or misleading information. *See* MD. CODE COM. LAW § 14-3001, *et seq.*; CAL. BUS. & PROF. CODE § 17529, *et seq.* The Maryland Act defines “interactive computer service provider” as “an information service, system, or access software

provider that provides or enables computer access by multiple users to a computer service.” MD. CODE COM. LAW § 14-3001. The Cal. Bus. & Prof. Code, in turn, defines “electronic mail service provider” as “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.

Accordingly, the Maryland and California statutes require that plaintiffs seeking to sue as an ICSP or EMSP satisfy two requirements. First, both require that the plaintiff be a “service provider.” Second, it must be a service provider which: in Maryland, “enables computer access by multiple users to a computer service;” or, in California, acts as “an intermediary in sending or receiving email or [] provides to end users of the electronic mail service the ability to send or receive email.”

Although BSI pretends otherwise, the intended meaning of “service provider” is far from evident from the statutory language used to define it. *See, e.g., Gordon*, 575 F.3d at 1049, 1051 (finding that CAN-SPAM’s analogous definition of “Internet Access Service” provider as “a service that enables users to access content, information, electronic mail, or other services offered over the Internet” to be ambiguous.) While both statutes distinguish between “recipients” and “service providers,” the text of neither draws a clear distinction between the two. For its part, the Maryland Act does not define “recipient,” and its definition of ICSP is entirely circular. It defines “service provider” simply as a “provider that provides.” *See* MD. CODE COM. LAW § 14-3001 (defining ICSP as “an information service, system, or access software provider that provides . . .”). The Act therefore leaves the term essentially undefined. *Cf. Cilecek v. Inova Health Sys. Serv.*, 115 F.3d 256, 259 (4th Cir. 1997) (by adopting a “circular

definition” of “employee” under Title VII, “Congress has left the term [ ] essentially undefined”).

The Cal. Bus. & Prof. Code, in turn, defines recipient as “the addressee of an unsolicited email advertisement.” CAL. BUS. & PROF. CODE. § 17529(m). Although the California statute avoids the circularity of Maryland Act, it suffers from its own ambiguity. Read literally, its definition of EMSP as “any person” who acts as “an intermediary in sending or receiving electronic mail,” or who “provides to end users . . . the ability to send or receive electronic mail,” is so broad as to encompass virtually anyone with a computer and internet connection. *Gordon*, 575 F.3d 1040 at 1051 (observing that literal interpretation of CAN-SPAM’s definition of IAS could cover “any person who allows another person to use their computer to access the Internet.”)

Given these ambiguities, the Court must therefore consider the consequences of giving the statutes’ language literal effect. The absurdities that would result from construing the definitions literally are amply demonstrated by the testimony of BSI’s own witnesses. As Paul Wagner opined, a literal interpretation of the Maryland Act would mean that Mr. Baldrige could qualify as an ICSP if he allowed neighbors to access the Internet through his Wi-Fi router. (6/20M, P. Wagner at 41-42.) According to Dr. Resnick, Mr. Graham would be both an ICSP and EMSP if he provided others an internet connection through a Bluetooth-enabled computer or cell-phone. (6/21A, P. Resnick at 49-52.) Any Starbucks, Holiday Inn, or other wireless “hotspot” that provided patrons an internet connection would also qualify. Indeed, Paul Wagner went so far as to suggest that “plugging in cords” for his father was providing “computer access to a computer service” under Maryland law, which under the plain meaning of the California

statute would also constitute “provid[ing] . . . the ability to send or receive” email. (6/21M, P. Wagner at 79.)

This is plainly not what the Maryland or California Legislatures reasonably intended. By distinguishing between “recipients” and “service providers,” it is clear that the State Legislatures intended an ICSP and EMSP to be something different than what BSI claims. Indeed, the legislative histories of both statutes reflect that both Legislatures granted services providers a remedy specifically to address the operational and economic impact of spam that is unique to them, but not experienced by average email users. *See* DX 10, Md. Senate Letter Re: Electronic Mail – Prohibitions (noting that statutory damages are greater for ICSPs “whose servers can be clogged to the point of being shut down by arge amounts of ‘spam’”); DX 11 (Cal. legislative findings that “spam will cost United States organizations more than ten billion dollars [] this year, including lost productivity and the additional equipment, software and manpower needed to combat the problem.”) The Maryland statute expressly recognizes this by granting ICSPs the right to twice the statutory damages per violation as recipients. MD. CODE COM. LAW § 14-3003(3). The nebulous definition of “service provider” BSI advocates in this case would distort the boundaries of this distinction in the best of cases, and abolish it all together in the worst. *See, e.g., Palos Verdes Faculty Assn. v. Palos Verdes Peninsula Unified Sch. Dist.*, 21 Cal.3d 659, 659 (1978) (in construing statute, courts must into account “the various parts of a statutory enactment must be harmonized by considering the particular clause or section in the context of a statutory framework as a whole.”); *Ford Motor Land Dev. V. Comptroller*, 68 Md. App. 342-346-47 (1986) (“a statute must be read so that no part of it is ‘rendered surplusage, superfluous, meaningless or nugatory.’”)

As discussed in more detail below (*see* Arg. § I.C.2.), a literal application of the statutory language would confer standing on plaintiffs in no way injured by the receipt of spam, a result directly at odds with this statutory distinction, as well as the Cal. Bus. & Prof. Code's requirement that plaintiffs must suffer an economic injury in fact to have standing under the Code's false advertising provisions, of which the anti-spam provisions are a part. CAL. BUS. & PROF. CODE § 17535. Construing either statute to allow plaintiffs not genuinely harmed by a statutory violation accomplishes neither statutes' objective of providing those most harmed by unlawful spam – legitimate internet and email service providers – the ability to redress their injuries. *See, e.g., Rincon Del Diable Mun. Water Dist. v. San Diego Water Auth.*, 121 Cal. App.4th 813, 818-19 (4th Dist. 2004) (in construing statute court “should take into account matters such as context, the object in view, [and] the evils to be remedied . . .”).

Finally, if BSI's conduct in this case is any indication, a literal interpretation of the Maryland and California provisions would invite and encourage litigation on manufactured claims contrary to public policy. *See, e.g., Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, (1975) (construing standing provisions of Securities Exchange Act narrowly to promote public policy against manufactured and vexatious claims); *Hsu v. Abbata*, 9 Cal. 4th 863, 872 (1995) (rejecting literal interpretation of contract provision that would encourage vexatious and frivolous litigation). Absent some implied limitation on the meaning of “service provider,” anyone with a computer, internet connection, and ability to receive and forward emails would be incentivized, as Wagner himself observed in DX 55, to intentionally seek out and collect spam on which to sue. There is nothing to indicate that the Maryland or California Legislatures intended to confer standing to such opportunistic plaintiffs.

**D. The Court Should Construe The California & Maryland Statutes Consistent With The Parallel Provisions Of CAN-SPAM.**

When faced with ambiguities in their own statutes, Maryland and California courts will routinely look to analogous federal law for guidance. *See, e.g., Solano County Emp. Assn. v. County of Solano*, 130 Cal. App.3d 256, 259 (1st Dist. 1982) (“[I]t is well settled that California courts will look to federal law for guidance in interpreting state statutes whose language parallels that of federal statutes,” *citing Social Workers’ Union, Local 535 v. Alameda Co. Welfare Dept.*, 11 Cal.3d 382, 391 (1974)); *DuBois v. City of College Park*, 280 Md. 525, 528-29 (1977) (looking to federal law for guidance in determining voter standing in Maryland redistricting litigation); *Davidson v. Microsoft Corp.*, 143 Md. App. 43, 50-51 (2002) (interpreting the Maryland Consumer Protection Act in accordance with federal law to prohibit claims by indirect purchasers who did not sustain an anti-trust injury). This leads here to CAN-SPAM’s analogous definition of “Internet Access Service” provider, and the Ninth Circuit’s holding in *Gordon* that to have standing under CAN-SPAM a plaintiff must show that it (i) is a *bona fide* service provider (ii) “adversely affected” by statutory violations. *Gordon*, 575 F.3d at 1049; 15 U.S.C. § 7706(g)(1).)

At issue in *Gordon* was whether CAN-SPAM granted standing to a plaintiff who, among other things: (i) configured his computers to collect spam in “unused inboxes” (*id.* at 1046); (ii) “refuse[d] to implement spam filters in a typical manner or otherwise make any attempt to block allegedly unwanted spam” (*id.* at 1052, 1055); (iii) instead created “spam traps” for “the sole purpose of snagging as many e-mail marketing messages as possible” (*id.* at 1056); (iv) devoted his time and resources to “accumulating spam . . . for the purpose of facilitating litigation” (*id.* at 1052); (v) coordinated his efforts to collect spam with “clients” who “sen[t] to Gordon in enormous unsorted batches of 10,000 to 50,000 messages to fuel his various anti-spam lawsuits,”

and with whom Gordon then shared his settlement proceeds (*id.*); (vi) “created a cottage industry where he and his ‘clients’ set themselves up to profit from litigation” (*id.* at 1057); (vii) derived “substantial financial benefit but endure[d] no real ISP-type harm from commercial email” (*id.*); and (viii) “suffered no harm related to bandwidth, hardware, Internet connectivity, network integrity, overhead costs, fees, staffing or equipment costs.” (*id.* at 1055-56.)

**1. The Compelling Rationale For Adopting A *Bona Fide* Requirement Under The State Statutes.**

At the heart of *Gordon’s* analysis was the court’s conclusion that a reasonable, common-sense construction of CAN-SPAM’s analogous and equally ambiguous definition of “IAS” provider necessarily included a *bona fide* requirement. 575 F.3d at 1049 (“While over time courts have developed various canons to assist with statutory interpretation, this ‘is an area in which absolutist rules do not [always] lead to sensible or accurate results . . . Therefore, especially in this highly technical and evolving field, ‘common sense not dogma is what is needed in order to explore the actual meaning of legislative enactments.’” (citations omitted).)

To give meaning to the statute’s imprecise definition of “IAS provider,” *Gordon* looked first to the overall structure and purpose of the statute. The court began by observing that “the purpose of the CAN-SPAM Act was not to stamp spam out of existence,” but rather to balance the need for protection against fraudulent email practices, with the social and economic benefits of commercial email generally. 575 F.3d at 1049. To strike this balance, Congress drew a distinction between mere recipients of email – for whom it did not provide a remedy – and those entities and individuals most affected by unlawful spam and in the best position to prosecute statutory violations – internet service providers – for whom it did. *Id.* at 1051-52, 1053-54, 1057.

On this point, the Act's legislative history expressly reflected Congress' intent that standing be limited to a narrow class of private plaintiffs it characterized as "*bona fide* Internet service providers." As *Gordon* explained:

It is perhaps a sad reality that Congress must specify a *bona fide* IAS provider, as possibly distinct from a non-genuine IAS provider. But this demonstrates to us that lawmakers were wary of the possibility, if not the likelihood, that the siren song of substantial statutory damages would entice opportunistic plaintiffs to join the fray, which would lead to undesirable results.

*Id.* at 1050.

Gordon's argument (similar to BSI's argument here) that the definition of IAS provider should be given literal effect would render it almost meaningless: "[i]n the most general terms, a 'service that enables users to access' online content or email could encompass the proprietor of an Internet coffee shop or, as one district court suggested, 'any person who allows another person to use their computer to access the Internet' . . . Without question, this was not what Congress intended when it was the defining the private right of action." *Gordon*, 575 F.3d at 1051. Thus, although Congress did not intend to limit standing exclusively to "fee-for-service operations," it *did* intend to exclude plaintiffs who, "despite certain identifying characteristics, did not provide the actual, *bona fide* service of a legitimate operation." *Id.* at 1050, 1057 ("The CAN-SPAM Act was enacted to protect individuals and legitimate businesses – not to support a litigation mill for entrepreneurs like Gordon.")

Agreeing with the majority's analysis and holding, Justice Gould wrote separately to emphasize that he "would presume a *bona fide* requirement even without this legislative history," *Gordon*, 575 F.3d at 1068:

[S]tatutory standing should be denied to plaintiffs such as Gordon who purposely structure themselves to look like one of the limited entities eligible to sue but do so for the primary purpose of collecting damages and settlements from litigation. Such individuals trying to game the system do

not fall into the limited class to which Congress made available a private remedy, and ordinarily should be denied statutory standing. That the legislative history specifies *bona fide* IAS providers strengthens our conclusion that Gordon's suit should be dismissed, but the legislative history is not necessary to reach this conclusion in light of the common-law antecedents that do not favor manufactured claims.

*Id.* at 1066-67

For Judge Gould, “the most pertinent conclusion [ ] in this case . . . is that Gordon was seeking to use the CAN-SPAM Act to build a litigation factory for his personal financial benefit . . . the ways in which Gordon inserted himself into legal controversy here require conclusions that he is not an IAS and that he was not adversely affected by spam. Each of these conclusions is independently sufficient to deny Gordon statutory standing to assert his claims.” *Id.* at 1066-67.

The undisputed record in this case closely parallels that at issue in *Gordon*, and presents an equally compelling basis for the Court to interpret the Maryland and California statutes to include a *bona fide* requirement. Any nominal differences between the facts in *Gordon* and those presented to the jury here – namely, that BSI uses its *own* servers to intentionally seek out and capture spam – are immaterial. All other aspects of the two cases are virtually identical.

Like *Gordon*:

- BSI lacks the customary indicia of a legitimate internet or email service provider, *see pp. 17-22, above; Gordon, supra, at 1052, 1055*
- BSI refuses to take even nominal steps to block, filter, or otherwise mitigate its receipt of spam. Instead, it accepts and archives indefinitely all incoming email contrary to the industry-wide custom and practice of other internet and email service providers, *see pp. 7-9, 18, above; Gordon, supra, at 1055-56.*
- It employs “spam traps” to attract and collect spam on which to then sue, *see pp. 7-9, above; Gordon, supra, at 1056.*

- It routes spam to abandoned or otherwise unused email accounts or “inboxes,” *see* pp. 7-9, above; *Gordon, supra* at 1046.
- Paul Wagner can be aptly described as a “professional” litigant. BSI has filed approximately 25 spam-related lawsuits, and its sole employee spends 40 or more hours a week on litigation, *see* pp. 4-5, 12-15, above; *Gordon, supra* at 1052, 1056.
- Paul Wagner coordinates BSI’s spam collection and litigation efforts with his brother Joe and his company Hypertouch. Joe automatically forwards to BSI spam emails captured by Hypertouch’s servers by the tens of thousands, which Paul archives and then later sues on, sometimes years later, *see* pp. 5-11, above; *Gordon, supra*, at 1052.
- Paul and Joe target the same defendants, sue on the same emails, and share in settlement proceeds, *see* pp. 12-17, above, *Gordon, supra*, at 1052.
- BSI’s primary source of revenue are its litigation proceeds, *see* pp. 4, 22, above; *Gordon, supra*, at 1056.
- All of BSI’s activities relate to litigation, *see* pp. 4, above. *Gordon, supra*, at 1055-56.

There is no evidence that the Maryland or California statutes were enacted to provide a remedy to plaintiffs like BSI, whose nominal provision of internet-related services primarily to family and friends is incidental to the full-time pursuit of statutory damages on claims manufactured by their own intentional actions. To the contrary, as discussed above, the legislative intent of both statutes was to limit standing to legitimate service providers genuinely affected by statutory violations, as reflected by the statutes’ legislative findings, the overall

structure of the statutes, and underlying public policy. *See* DX 10; DX 11; CAL. BUS. & PROF. CODE § 17535 (limiting standing for false advertising claims to plaintiffs who suffer economic injury-in-fact); MD CODE COM. LAW § 14-3003(3) (granting service providers double the statutory remedy as recipients”). Allowing BSI to proceed with its claims on the undisputed record here would be contrary to this intent, contrary to public policy, and contrary to well-established canons of statutory construction, *see* Arg. § I.B, above. Accordingly, any reasonable and common-sense interpretation of the Maryland and California statutes compels the conclusion that, like Congress, both State Legislatures intended to limit the right to sue to *bona fide* service providers genuinely affected by unlawful spam in the ordinary course of a legitimate operation.

**2. BSI Cannot Establish On The Undisputed Record That It Was “Adversely Affected.”**

Although neither State statute expressly states an “adversely affected” requirement, it is implicit under the “injury-in-fact” standing requirements of state and federal law, as well as the enormity of the remedy the statutes provide. *See* Arg. § I.A., above; CAL. BUS. & PROF. CODE § 17535 (limiting standing for false advertising claims to plaintiffs who suffer economic injury-in-fact caused by violation); *Shutts*, 472 U.S. at 804 (“Standing to sue in any Article III court is, of course, a federal question which does not depend on the party’s [] standing in state court.”); *Goode*, 539 F.3d at 321 (“[E]ven if Pennsylvania state law would have afforded appellants standing if they had brought this action in state court, we must ensure that they satisfy the federal requirements for standing as well.”).<sup>9</sup>

---

<sup>9</sup> Indeed, it would be unreasonable to presume that the State Legislatures intended to impose such onerous statutory penalties on defendants in favor of plaintiffs not genuinely injured by a statutory violation. To that end, the Fourth Circuit’s opinion is *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348, 352 (4th Cir. 2006) is in accord. There, the Fourth Circuit found that CAN-SPAM preempted Oklahoma’s anti-spam statute to the extent that it allowed a

In defining “adversely affected” in the context of CAN-SPAM, *Gordon* emphasized two points that comport with the “injury-in-fact” requirement of both state law and Article III standing. First, the injury alleged must be both “real” and “uniquely encountered by IAS providers.” *Gordon*, 575 F.3d at 1053-54; *Lujan*, 504 U.S. at 560-61 (injury necessary to support standing must be concrete and particularized). Such harm in this context includes “network crashes, higher bandwidth utilization, and increased costs for hardware and software upgrades, network expansion and additional personnel.” *Id.* at 1053 (citations and internal quotations omitted). Second, a plaintiff must be able to show causation – *i.e.*, that the harms alleged must be attributable to violations of the statute. *Id.* at 1054 (“there must be, at bare minimum, a demonstrated relationship between purported harms and the type of e-mail practices regulated by the Act); *Lujan*, 504 U.S. at 560-61 (injury alleged must be traceable to purported misconduct). Stated differently, a plaintiff must demonstrate that it was “*adversely affected by misconduct.*” *Gordon* at 1054 (emphasis in original).

For this reason, “[c]ourts must of course be careful to distinguish the ordinary costs and burdens associated with operating an Internet access service from actual harm”:

After all, network slowdowns, server crashes, increased bandwidth usage, and hardware and software upgrades bear no inherent relationship to spam or spamming practices. On the contrary, we expect these issues to arise as a matter of course and for legitimate reasons as technology, online media, and Internet services continue to advance and develop. Therefore, evidence of what could be routine business concerns and operating costs is not alone sufficient to unlock the reassurance trove of . . . statutory damages.

---

cause of action for immaterial misrepresentations inconsistent with CAN-SPAM’s requirement that “falsity” and “deception” be construed in the nature of tort which, among other things, requires as an element of proof that plaintiff suffered injury as a result of the fraudulent misrepresentation alleged. *Id.* at 354 (“Since the word ‘falsity’ considered in isolation does not unambiguously establish the scope of the preemption clause, we read ‘falsity’ in light of the clause as a whole. Reading ‘falsity’ as referring to traditionally tortious or wrongful conduct is the interpretation most compatible with the maxim of *noscitur a sociis*, that a word is generally known by the company it keeps.”)

*Id.* at 1054 (“to secure adequate bandwidth and storage capacity and take reasonable precautions, such as implementing spam filters, as part of its normal operations.”)

Ultimately, *Gordon* concluded that whether a plaintiff is a *bona fide* service provider adversely affected calls for a sliding-scale approach applied on a case-by-case basis:

[i]n some civil actions – where, for example, well-recognized ISPs or plainly legitimate Internet access service providers file suit – adequate harm might be presumed because any reasonable person would agree that such entities dedicate considerable resources to and incur significant financial costs in dealing with spam . . . Where, by comparison, a private plaintiff’s status as an IAS provider is questionable and reasonably contested, courts should not only inquire into the plaintiff’s purported Internet-related service operations but also closely examine the alleged harms attributable to spam.

*Id.* at 1054, 1055 (“Courts should take an especially hard look at the cited harm if it suspects at the outset that a plaintiff is not operating a *bona fide* Internet access service, as is the case here.”)

Accordingly, a plaintiff in the business of manufacturing claims by seeking out and capturing spam is not a *bona fide* service provider. *Gordon*, 575 F.3d at 1040 (“The CAN-SPAM Act was enacted to protect individuals and legitimate businesses – not support a litigation mill for entrepreneurs like *Gordon*.”) If a plaintiff is not a *bona fide* provider, it is unlikely able to establish any genuine, adverse effect caused by a statutory violation. *Id.* at 1057 (“The fact that *Gordon* derives substantial financial benefit but endures no real ISP-type harm from commercial e-mail, coupled with his unusual efforts to seek out and accumulate – rather than avoid or block – spam, demonstrates that he has not been adversely affected by alleged violations of the federal act in any cognizable way.”)

Here, the undisputed evidence plainly establishes that BSI’s alleged harm was the self-inflicted and avoidable consequence of its own conduct, unrelated to a legitimate operation or its provision of a legitimate service. For that matter, BSI presented no evidence that it was required to invest in new equipment, increase its bandwidth utilization, increase its storage capacity, buy

new servers, incur additional costs to block or filter spam, hire additional staff, or otherwise invest in resources necessary to combat spam in order to maintain a robust and legitimate service for its customers. Nor is there any evidence that BSI's receipt of spam in the ordinary course affected any service it provides customers, or otherwise negatively impacted its customer relationships. Instead, the record is clear that BSI's alleged "harm" was the result of its own intentional efforts to attract and capture spam to support its litigation activities. This is not the type of "injury" on which standing should be allowed, under either state or federal law. *Gordon*, 575 F.3d at 1056 ("Gordon's claimed harms almost exclusively relate to litigation preparation, not to the operation of a *bona fide* service.")

**E. BSI's Interpretation Of The State Statutes Raises Issues Of Preemption.**

Moreover, a contrary interpretation of the State statutes would create an inevitable conflict between state and federal law inconsistent with CAN-SPAM's express preemption of state law. 15 U.S.C. § 7707(b)(1) (providing that CAN-SPAM "supersedes any statute, regulation, or rule of a State or political subdivision of that 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.")

The Supreme Court has "long recognized that state laws that conflict with federal law are without effect," and that "a statute's pre-emptive effect is guided by the rule that the purpose of Congress is the ultimate touchstone in every pre-emption case." *Altria Group, Inc. v. Good*, 129 S. Ct. 538, 543 (2008) (citations and internal quotations omitted). Thus, "Congress may indicate pre-emptive intent through a statute's express language or through its structure and purpose." *Id.* In addition, "[p]re-emptive intent may also be inferred if the scope of the statute indicates that

Congress intended to occupy the legislative field, or if there is an actual conflict between state and federal law.” *Id.* (citations omitted.); *Omega World Travel, Inc.*, 469 F.3d at 352 (“Instead of imposing the narrowest possible construction on preemptive language when read in isolation, we seek ‘a fair understanding of congressional purpose,’ looking to ‘the language of the pre-emption statute and the statutory framework surrounding it,’ while also considering “the structure and purpose of the statute as a whole” (emphasis, citations, and internal quotations omitted)).

The scope of Congress’ preemptive intent under CAN-SPAM is clear from both the text of the statute and legislative history. Congress enacted CAN-SPAM to create “one national standard” to replace the inconsistent patchwork of state laws governing commercial email. As its legislative history explained: “Given the inherently interstate nature of e-mail communications, the Committee believes that this bill’s creation of one national standard is a proper exercise of the Congress’s power to regulate interstate commerce . . . this is particularly true because . . . a sender of e-mail has no easy way to determine with which State law to comply.” S. Rep. No. 108-102, at 21 (2003). So central was this intent to the purpose of the Act that Congress expressly stated it in the statute itself:

Many states have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.

15 U.S.C. § 7701(a)(11); *see also Gordon*, 575 F.3d at 1063 (absent a national standard “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, whose

location is often unknown”); *Omega*, 469 F.3d at 356 (absent preemption, “one state’s Internet laws may impose compliance costs on businesses throughout the country.”)

Interpreting the State statutes to allow non-*bona fide* service providers to bring claims under state law that are prohibited under CAN-SPAM would frustrate Congress’ clear intent that CAN-SPAM supplant conflicting state regulation of commercial email generally and, specifically, its intent to limit standing under CAN-SPAM to a narrow group of plaintiffs who qualify as “*bona fide* internet service providers.” *Gordon*, 575 U.S. at 1050; *cf.*, *Anderson v. Sara Lee Corporation*, 508 F.3d 181, 194-95 (4th Cir. 2007) (conflict preemption bars plaintiff from circumventing the exclusive remedies and procedures of the FLSA by pursuing the same FLSA claims through state common law claims). Stated differently, it would completely frustrate the express intent of Congress if States were allowed to expand upon an identical class of claimants Congress intentionally limited to *bona fide* ISPs, thereby creating an inconsistent standard contrary to the objective of creating a uniform standard for email regulation. *Gordon*, 575 F.3d at 1063 (“It would be logically incongruous to conclude that Congress endeavored to erect a uniform standard but simultaneously left states and local lawmakers free to manipulate that standard.”); *Omega*, 469 F.3d at 356; *Columbia Venture, LLC v. Dewberry & Davis, LLC*, 604 F.3d 824, 830 (4th Cir. 2010) (obstacle preemption applies “where state law ‘stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress’”).

When presented with two plausible interpretations of a statute, courts should adopt the construction that avoids preemption. *See, e.g., Adams Fruit Co., Inc. v. Barrett*, 494 U.S. 638, 647 (1990) (rejecting interpretation of state law that would create a conflict with federal law). While we dispute that BSI’s interpretation of the Maryland or California statutes is plausible, the point remains. Interpreting the State statutes in a manner consistent with CAN-SPAM gives

effect to Congress' objective of creating a national standard for the regulation of email by avoiding any conflict between state and federal law.

\* \* \* \* \*

For all of the foregoing reasons, the Court should interpret the Maryland and California definitions of ICSP and EMSP to require BSI to establish that it is a *bona fide* service provider adversely affected by the statutory violations it alleges. The Court should therefore adopt the jury's Phase II verdict and enter judgment in Defendants' favor.

**II. DEFENDANTS ARE ENTITLED TO SUMMARY JUDGMENT ON THE UNDISPUTED RECORD THAT BSI CONSENTED TO RECEIVE THE EMAILS AT ISSUE.**

Kraft joins in Defendant Connexus Corp's Motion for Summary Judgment regarding the second issue on which the Court ordered briefing – whether Defendants are entitled to judgment as a matter of law given that BSI consented to the “harm” it alleges. Although Connexus' motion focuses on emails routed from Hypertouch to BSI that BSI expressly agreed to accept, the same doctrine of consent similarly bars any claims on emails sent directly to BSI's servers.

BSI's claims are in the nature of tort, and therefore subject to the same defenses. *MaryCLE, LLC. v. First Choice Internet, Inc.*, 166 Md. App. 481, 528 (2006) (claims brought under CEMA are tort in nature). It is a fundamental principle of tort law that “[o]ne who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it.” Restatement 2d of Torts § 892A; Cal. Civ. Code § 3515 (“He who consents to an act is not wronged by it.”) The Restatement defines consent as “willingness in fact for conduct to occur.” Restatement 2d of Torts § 892(1). Consent need not be express, but “may be manifested by action or inaction and need not be communicated to the actor.” *Id.* Accordingly, “subjective beliefs as to [] consent are not determinative; consent is measured from [p]laintiff's manifested action or inaction.” *Jones v.*

*Corbis Corp.*, 815 F. Supp.2d 1108, 1114 (C.D. Cal. 2011), (dismissing claim for commercial misappropriation on ground that plaintiff impliedly consented to photographs of her likeness for commercial purposes).

A defendant is entitled to summary judgment where the evidence shows “that there is no genuine issue as to any material fact, and that the moving party is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c); *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986). The undisputed facts here plainly establish BSI’s consent to the alleged wrongdoing for which it seeks recovery. Contrary to industry custom and practice, BSI intentionally accepted and archived indefinitely all incoming emails, knowing that 99% of them were spam. It purposely made no effort to block, filter, or otherwise mitigate spam generally, or its receipt of the emails at issue in this case specifically, despite the relative ease and nominal expense of implementing such measures. *Jones*, 815 F. Supp.2d at 1114 (plaintiff consented to use of her photographs for commercial purposes because not only did she understand that photographs would be used commercially and did not object, but her argument to the was contrary to well-established industry custom and practice); *Gordon*, 575 F.3d at 1054 (legitimate email service providers are expected “to secure adequate bandwidth and storage capacity and take reasonable precautions, such as implementing spam filters, as part of its normal operations). In fact, BSI purposely avoided taking such preventative measures precisely so that it would receive spam. Tellingly, when the filtering feature on BSI’s email software was blocking spam, Wagner turned it off to avoid rejecting “fraudulent” emails on which the brothers could sue. (DX 135; 6/22, J. Wagner at 163-65.)

Moreover, it is undisputed that BSI intentionally sought to attract spam by posting on websites thousands of fictitious email addresses with the understanding and expectation that

“spammers” would find the addresses and send emails to them. (DX 360, 361; 6/26, J. Wagner at 82-83, 109-13.) Spam sent to these addresses was routed directly to BSI’s servers. (6/26, J. Wagner at 112-13.) That Paul Wagner intended for spam to be sent to these addresses is evident. Wagner has an advanced degree in artificial intelligence from MIT, and has been involved in the field of internet and email technology for more than 20 years. (6/19A, P. Wagner at 55, 56-59.) He is actively involved with several anti-spam groups and has filed approximately 25 spam-related lawsuits over the last eight years. Wagner certainly knew that most, if not all, of the emails sent to the “spam traps” he and his brother posted would contain spam. (6/21A, Resnick at 56-57; 6/27, P. Wagner at 111; Ex. 2, Levine Dep. at 631-32.)

As Joe Wagner admitted at trial, BSI wanted to collect spam. (6/26, J. Wagner at 80-81, 170.). This admission, while alone a sufficient basis for granting Kraft’s motion, merely summarizes what all other undisputed evidence in the case demonstrates. BSI deliberately invited and collected spam for purposes of bringing cases such as this one, a practice from which it has profited handsomely. The law does not allow such gratuitous conduct as the basis for asserting a claim. For this additional reason, Defendants are entitled to judgment as a matter of law.

### CONCLUSION

For all of the foregoing reasons, Kraft respectfully requests that the Court enter judgment in Defendants’ favor and dismiss BSI’s complaint in its entirety.

Dated: October 1, 2012

/s/

---

Darrell J. Graham (*pro hac vice*)  
John E. Bucheit (*pro hac vice*)  
ROESER BUCHEIT & GRAHAM LLC  
20 N. Wacker Dr., Ste. 1330  
Chicago, IL 60606  
(312) 621-0301  
(312) 621-0306 (facsimile)  
dgraham@rbglegal.com  
jbucheit@rbglegal.com

John K. Roche (USDC-MD Bar No. 17531)  
John M. Devaney (*Pro Hac Vice*)  
PERKINS COIE LLP  
700 13<sup>th</sup> St., N.W., Suite 600  
Washington, D.C. 20005-3960  
(202) 434-1627  
(202) 654-9106 (facsimile)  
jdevaney@perkinscoie.com  
jroche@perkinscoie.com

*Attorneys for Defendants Kraft Foods Inc.,  
Kraft Foods Global Inc., and Vict. Th.  
Engwall & Co., Inc.*

I hereby certify that on October 1, 2012, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following individuals:

---

Anthony Cavanaugh  
Thomas M. Barba  
John J. Duffy  
Anthony A. Onorato  
STEPTOE & JOHNSON LLP  
1330 Connecticut Ave., NW  
Washington, D.C. 20036  
(202) 429-3000  
(202) 429-3902 (facsimile)  
[acavanaugh@steptoe.com](mailto:acavanaugh@steptoe.com)  
[tbarba@steptoe.com](mailto:tbarba@steptoe.com)  
[jduffy@steptoe.com](mailto:jduffy@steptoe.com)  
tonorato@steptoe.com  
Stephen H. Ring  
Law Offices of Stephen H. Ring, P. C.  
506 Main Street, Suite 215  
Gaithersburg, Maryland 20878  
301-563-9249  
301-563-9639 (fax)  
shr@ringlaw.us

Mike Rothman  
Law Office of Michael S. Rothman  
401 E. Jefferson St., Suite 201  
Rockville, MD 20850  
(301) 251-9660  
(301) 251-9610 (facsimile)  
mike@mikerothman.com  
*Attorneys for Plaintiff Beyond Systems, Inc.*

J. Douglas Baldrige  
Lisa Jose Fales  
Ari N. Rothman  
VENABLE LLP  
575 7th Street, N.W.  
Washington, DC 20004-1601  
(202) 344-4000 (phone)  
(202) 344-8300 (fax)  
[jdbaldrige@venable.com](mailto:jdbaldrige@venable.com)  
[ljfales@venable.com](mailto:ljfales@venable.com)  
[anrothman@venable.com](mailto:anrothman@venable.com)

*Attorneys for Defendants Connexus Corp.*

/s/

---

John E. Bucheit (*Pro Hac Vice*)  
Roeser Bucheit & Graham llc  
20 N. Wacker Dr., Ste. 1330  
Chicago, IL 60606  
(312) 621-0302  
(312) 621-0306 (facsimile)  
[jbucheit@rbglegal.com](mailto:jbucheit@rbglegal.com)

*Attorneys for Defendants Kraft Foods Inc., Kraft Foods Global Inc., and Vict. Th. Engwall & Co., Inc.*