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) Judge Peter J. Messitte
CONNEXUS CORP. Third-Party Plaintiff, v. JAMES JOSEPH WAGNER, *et al.*, Third-Party Defendants.	

PLAINTIFF'S POST-TRIAL MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

INTRODUCTION 1

I. THERE IS NO "BONA FIDE" REQUIREMENT IN THE MARYLAND OR CALIFORNIA STATUTE..... 3

A. Defendants Fail To Provide a Valid Reason Why This Court Should Ignore Standard Rules of Statutory Construction and Impose an Extra-Statutory Standing Requirement. 3

1. The "Absurd Results" Exception to the Plain Meaning Rule Is Exceedingly Narrow and Inapplicable Here. 4

2. Defendants' Three Propositions in Support of Their "Absurd Results" Argument Misstate the Legal Standards That Govern. 8

B. *Gordon* Does Not Control Here as a Matter of Law and Is Distinguishable as a Matter of Fact.15

1. The Standing Requirements of CAN-SPAM Are Distinguishable. 15

2. BSI Is Also Factually Distinguishable From Gordon. 20

3. BSI's Practices in Collecting Emails Do Not Disqualify it From Being an ICSP or an EMSP. 21

II. BSI DID NOT "CONSENT" TO DEFENDANTS TRANSMITTING ILLEGAL SPAM, LET ALONE TO RECEIVING IT. 23

A. Consent Is Not a Defense To Liability Under the Maryland and California Statutes. 32

B. At the Very Least, There Are Genuine Issues of Material Fact That Preclude Summary Judgment on the Issue of Consent. 35

1. BSI and Hypertouch Each Broadcast a "No UCE" Message to All Incoming Connections..... 36

2. Sending an Opt-Out Request Does Not Constitute Consent to Receive Even More Spam. 37

3. A Spammer's Transmission of Mail to a Spam Trap or to a Wildcard Entry in a Routing Table Does Not Mean That the Service Provider Consents to Receipt of the Spam.. 38

4. BSI's Filtering or Blocking of Email In No Way Means it Consented to Receive Spam 41

5. The Routing Relationship Between BSI and Hypertouch Does Not Prove That BSI Consented to Receive Spam from Defendants..... 42

CONCLUSION.....44

INTRODUCTION

Plaintiff Beyond Systems, Inc. ("BSI") opposes Defendants Kraft Foods, Inc.'s ("Kraft") and Connexus Corp.'s ("Connexus") Motions for Summary Judgment (DE 585 and 586).

In opposing BSI's standing, Defendants argue that BSI took actions that enabled it to capture Defendants' spam and to assert claims over that spam. Because of this, Defendants argue, BSI is not a "bona fide" ICSP or EMSP and has no standing under the Maryland and California anti-spam laws. Defendants concede that the statutes at issue here do not expressly require BSI to be "bona fide," but they contend that, unless the Court reads that phrase into the law, BSI will have the right to recover, and that would be an "absurd result."

Defendants are wrong. The Maryland and California statutes clearly and unambiguously set forth the requirements for standing to enforce those laws, and as BSI established in its opening brief, those requirements are the only requirements for standing. The "absurd results" exception to the plain meaning rule has no application here and, in fact, would disqualify the very kind of plaintiffs that the state legislatures rely on to enforce these anti-spam laws. BSI's aggressive pursuit of Defendants' statutory violations is entirely consistent with the Maryland and California legislatures' goals of rooting out deceptive spam.

Defendants, in a second motion, also contend that BSI's practices establish that it "consented" to receive Defendants' spam and that consent should be a complete defense to violations of those statutes. This argument, too, fails. First, BSI's claims are statutorily based. Nothing in those statutes suggests that consent is a defense to the sending of false and deceptive spam, and Defendants cannot cite any authority establishing that the defense of "consent" is applicable here. Second, even if consent were legally relevant, there are triable issues of fact as to whether BSI's conduct amounts to "consent." In particular, BSI has put in substantial

evidence – and in a trial on the merits, would adduce even more evidence – that it did *not* consent to receive Defendants' spam, including BSI's deployment of a digital "banner" that alerts all incoming mail transmissions that BSI does *not* consent to receive unsolicited commercial email. That alone establishes a genuine issue of material fact that precludes summary judgment. BSI also has introduced substantial evidence showing that BSI's collection of spam does not amount to consenting to its transmission. Defendants wrongly conflate the use of measures that are designed to catch spammers in the act and to hold them accountable with affirmatively consenting to the Defendants' illegal conduct. The two are not the same.

Defendants' "consent" theory boils down to an attempt to cast BSI as the party responsible for the Defendants' unlawful actions in sending their deceptive spam. But it is Defendants, not BSI, who chose to send their spam to BSI and to employ tactics like address harvesting and dictionary attacks to multiply their spam campaigns and inundate ICSPs and EMSPs like BSI with tens of thousands of deceptive, unsolicited emails. Those violations were complete at the moment that Defendants hit the send button, and the fact that BSI thereafter used spam traps and wildcards and the like to collect and preserve evidence of that wrongdoing – and to hold Defendants financially accountable – does not mean that BSI consented to Defendants' illegal spamming.

Defendants' Motions for Summary Judgment should be denied, and this Court should hold that BSI has standing to pursue its claims under the Maryland and California statutes.

I. THERE IS NO "BONA FIDE" REQUIREMENT IN THE MARYLAND OR CALIFORNIA STATUTE.

A. Defendants Fail To Provide a Valid Reason Why This Court Should Ignore Standard Rules of Statutory Construction and Impose an Extra-Statutory Standing Requirement.

It has been BSI's view from the outset that the time-honored "plain meaning" rule of statutory construction controls the central question whether a "bona fide" requirement should be read into the two anti-spam statutes at issue in this case. Defendants argue that the Court should depart from that basic rule of construction and impose an extra-statutory condition that would require plaintiffs to prove more than what the statutes expressly require.[1] In Defendants' view, BSI is required to prove not only that it is an interactive computer service provider and an electronic mail service provider, but also that it is a "bona fide" service provider of those services, a condition that finds no basis in the text or legislative history of the two statutes. To require any less, Defendants' argument goes, would produce "absurd results" that could not have been contemplated by Maryland or California lawmakers.

Defendants "absurd results" argument seems to rest on three propositions: 1) the anti-spam statutes are ambiguous and would make sense only if a "bona fide" requirement were imposed, 2) a "bona fide" requirement is needed so that claims will be limited to entities that are actually injured, and 3) recovery by "opportunistic plaintiffs" can be prevented only if a "bona fide" requirement is imposed. None of these propositions is supported by the "absurd results"

[1] Defendants have couched their arguments addressing BSI's standing as a Motion for Summary Judgment and have provided an accompanying statement of purportedly "undisputed facts." *See* Kraft Mot. Summ. J. 17-22; Connexus Mot. Summ. J. 2-7. However, the issue of BSI's standing has already been tried, and this Court made clear that the purpose of holding a trial was to make a record on which to base its determination of that issue. (Trial Tr. at 6/28 85:12-22). This means that only evidence from the trial record should be considered on the issue of BSI's standing and that, as far as that issue is concerned, Defendants' motion is not one for summary judgment, but rather a Post-Trial Motion for Judgment as a Matter of Law in support of Defendants' position that the jury's verdict in Phase Two should be controlling on the issue of BSI's standing. Accordingly, BSI's Opposition does not respond separately to Defendants' Statement of Facts as such and does not include citations to materials outside the trial record.

exception to the plain meaning rule. In fact, if there is an absurdity here, it is in Defendants' argument that statutes aimed squarely at stopping and punishing false and misleading spam cannot be used by ICSPs and EMSPs like BSI that vigorously and frequently use them.

1. The "Absurd Results" Exception to the Plain Meaning Rule Is Exceedingly Narrow and Inapplicable Here.

Parties seeking to evade the plain meaning of a statute under the "absurd results" exception carry a heavy burden. In *In re Sunterra Corp.*, the Fourth Circuit held that invoking the exception requires that "'literal application of the statutory language at issue results in an outcome that can truly be characterized as absurd; *i.e.*, that is so gross as to shock the general moral or common sense.'" 361 F.3d 257, 265 (4th Cir. 2004) (quoting *Sigmon Coal Co. v. Apfel*, 226 F.3d 291, 304 (4th Cir. 2000)). The court of appeals further emphasized that "'the instances in which exceptions to the Plain Meaning Rule apply are, and should be, exceptionally rare.'" *Id*. (quoting *Hillman v. Internal Revenue Serv.*, 263 F.3d 338, 342 (4th Cir. 2001)). "[I]f it is plausible that [the legislature] intended the result compelled by the Plain Meaning Rule, we must reject an assertion that such an application is absurd." *Id.* at 268.

California and Maryland law is fully in accord. "This ["absurd results"] exception should be used most sparingly by the judiciary and only in extreme cases else we violate the separation of powers principle of government. . . ." *Unzueta v. Ocean View School Dist.*, 6 Cal. App. 4th 1689, 1698 (Cal. App. 1992); *accord People v. Pecci*, 72 Cal. App. 4th 1500, 1507-08 (Cal. App. 1999) (same); *Guttman v. Wells Fargo Bank*, 26 A.3d 856, 862-63, 863 n.4 (Md. 2011) (explaining that plain meaning rule is strongly preferred rule of statutory construction and that existence of absurdity exception does not mean that "a court is wholly free to rewrite a statute merely because of some judicial notion of legislative purpose." (quoting *Kaczorowski v. Baltimore*, 525 A.2d 628, 633 n. 4 (Md. 1987))); *see also Schuster v. White Coffee Pot Family*

Inns, Inc., 43 Md. App. 550, 554, 406 A.2d 452, 454 (Md. App. 1979) (explaining absurd results rule in context of contract litigation and noting that "[w]e may not resort to that rule of construction if the contract, by its language, is susceptible of only one meaning (even if absurd)"). If it were otherwise, then the exception would quickly swallow the rule in any case in which a judge disagrees with legislative choices.

Given this high threshold, the plain meaning of a statute cannot be ignored merely because a court believes that its application would be "odd" or "unwise." *People v. Baldwin*, 189 Cal. App. 4th 991, 1004 (Cal. App. 2010) ("We recognize that as applied to a case such as this, the statutory language creates what is, at first blush, an odd result . . . Nonetheless . . . we cannot say that the result is so incongruous as to create an absurdity justifying a departure from the statutory language."); *People v. Pecci*, 72 Cal. App. 4th at 1507-08 ("There is nothing absurd about [the result dictated by the statute's plain meaning]. At most, such a [result] is unwise."); *In re Sunterra Corp.*, 361 F.3d at 268 ("In assessing whether a plain reading of a statute implicates the absurdity exception . . . the issue is not whether the result would be 'unreasonable,' or even 'quite unreasonable,' but whether the result would be absurd."); *see also Small v. United States*, 544 U.S. 385, 404 (Thomas, J., dissenting) ("[These outcomes] certainly present no occasion to employ, nor does the Court invoke, the canon against absurdities. We should employ that canon only 'where the result of applying the plain language would be, in a genuine sense, absurd, *i.e.*, where it is quite impossible that Congress could have intended the result . . . and where the alleged absurdity is so clear as to be obvious to most anyone'.") (quoting *Public Citizen v. Dept. of Justice*, 491 U.S. 440, 470-471 (1989) (Kennedy, J., concurring in judgment). Indeed, because there is so little to constrain a court's discretion once it invokes the absurdity exception, courts are understandably hostile toward its application.

In this case, it cannot be said that the legislatures in Maryland and California would never have intended to confer standing on ICSPs and EMSPs such as BSI. And that is the case even though claimants like BSI may spend a great deal of their time ferreting out spammers, collecting their violative emails, and then suing the spammers for significant statutory damages. The state legislatures knew that spammers are extraordinarily difficult to stop and that by using various means they are able to always stay one step ahead of whatever technology exists to stem the flood of spam. Indeed, the fact that private enforcement authority is expressly given to all service providers *and* recipients of false and misleading emails, and that any of these possible plaintiffs would be authorized to sue for significant statutory damages, is further proof that Maryland and California intended to encourage private attorneys general like BSI to go after illegal spammers like Kraft and Connexus.

This situation is thus nothing like the tort plaintiff, posited by the Court during trial, who intentionally steps from a curb into the path of a oncoming bus and then makes a claim for injuries because the bus negligently failed to stop in time. Perhaps it would be absurd to allow that plaintiff to recover, and there are all manner of legal doctrines and defenses that would provide the bus company with relief. Here, by contrast, it is the illegal spam itself that violates the anti-spam statutes, and it does so the moment that it is transmitted by the spammers to the intended recipients. Spammers like Kraft and Connexus send their false and misleading spam with the express desire that it will reach someone who will open it and take whatever action the email recommends. That plaintiffs such as BSI go to great lengths to gather these violative emails and then sue those who are responsible for sending them is entirely *consistent* with the goals and objectives of the Maryland and California laws. Maybe the Court thinks that it is "odd" or "unwise" to allow industrious and repeat claimants like BSI to sue spammers for tens of

millions of dollars. Maybe the Court does not like plaintiffs who avail themselves of opportunities like this. But that is no justification to disregard the plain meaning of the anti-spam statutes that confer standing on anyone who provides various Internet-related services. Indeed, it would be wholly improper for this Court to impose *any* extra-statutory standing requirement on the ground that it may disagree with the outcome when the plain meaning of the law is applied. The issue is whether conferring standing on BSI is, in the words of the Fourth Circuit, an outcome "that is so gross as to shock the general moral or common sense." That can hardly be said to be the case here. There is simply nothing absurd, shocking, immoral, or nonsensical about allowing BSI to sue spammers like Kraft and Connexus.

The few authorities on which Defendants rely do nothing to advance their argument. For example, *People v. Lundgren*, 14 Cal. 4th 294 (1996), makes clear that the "absurd results" exception should be used only as an aid in choosing between two or more legitimately susceptible constructions of a law. "'Where the language of the statutory provision is susceptible of two constructions, one of which, in application, will render it reasonable, fair and harmonious with its manifest purpose, and another which would be productive of absurd consequences, the former construction will be adopted.'" *Id*. at 305 (quoting *Western Oil & Gas Ass'n v. Monterey Unified Air Pollution Control Dist.*, 49 Cal. 3d 408, 425 (Cal. 1989)). The court in *Lundgren* premised its ruling on the existence of an ambiguity in the meaning of the phrase "source of drinking water," *id.* at 303-05, and selected the meaning that was most consistent with the legislature's expressly stated purpose "'to protect [the people] and the water they drink against chemicals that cause cancer, birth defects, or other reproductive harm.'" *Id.* at 306 (quoting the statute's preamble). *Lundgren*, and the other cases cited by Defendants,[2] are applications of the

[2] Likewise, in *Pan Am. Sulphur Co. v. State Dep't of Assessments & Taxation*, 251 Md. 620, 625-27, 248 A.2d 354, 357-58 (Md. 1968), the Court recognized the "absurdity" exception, but the result that it

"absurd results" exception in the narrow case where there is a need to make a choice between two plausible interpretations of the statutory text. That is not this case. There is no ambiguity here and thus no need to choose between differing interpretations of the law.

2. Defendants' Three Propositions in Support of Their "Absurd Results" Argument Misstate the Legal Standards That Govern.

Defendants' three arguments in support of engrafting a "bona fide" requirement onto the two anti-spam statutes – that the statutes are ambiguous; that standing should be limited to plaintiffs that are "genuinely injured"; and that "opportunistic plaintiffs" can be stopped only if a "bona fide" requirement is imposed – are not supported by the law or the facts.

First, there is no ambiguity in the definitions of an ICSP or an EMSP and thus no fear of construing or applying Maryland or California laws in a way that would lead to an absurd outcome. ICSPs and EMSPs are defined terms that are clear and understandable. Indeed, the jury had no problem with either of them or with finding that BSI satisfied the statutory definitions. The jury never asked the Court for clarification during its Phase One deliberations and never suggested that it was having any difficulty understanding what a provider of Internet services is. If an entity provides the Internet-related services that are expressly identified in the statutes, then that entity is an ICSP or an EMSP and has standing to sue.

Defendants argue that the Maryland law is ambiguous on the ground that the "definition of ICSP is circular." According to Defendants, the statute defines "service provider" simply as a "'provider that provides. . . .'" Kraft Mot. Summ. J. 26. That is not correct. In the part of the statute that Defendants omit, the services that an entity must provide to qualify as in ICSP are

---

reached was not at all comparable to the result that Defendants seek here. Instead, the court in *Pan Am. Sulphur Co.* reached the unremarkable conclusion that a tax statute that provided an exemption for property "used entirely or chiefly in connection with manufacturing" did not create an exemption for the petitioner's warehouse that was used solely for storage purposes.

expressly specified. Md. Code Ann., Comm. Law § 14-3001(c) (defining "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"). The Maryland anti-spam statute is thus nothing like the statute in *Cilecek v. Inova Health Sys. Servs.*, 115 F.3d 256, 259 (4th Cir. 1997) ("The Act defines 'employee' as 'an individual employed by an employer.' 42 U.S.C. § 2000e(f). And 'employer' is defined as a 'person ... who has fifteen or more employees' during a specified period of time. 42 U.S.C. § 2000e(b).") (cited at Kraft Mot. Summ. J. 26-27).

Likewise, there is no ambiguity in the California statute. An EMSP is defined 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.'" Defendants say that this definition "is so broad as to encompass virtually anyone with a computer and [I]nternet connection." Kraft Mot. Summ. J. 27. But a broad definition is not an ambiguous definition. Nor has BSI ever urged the Court to adopt a definition that would include "virtually anyone with a computer and an internet connection." *Id*. Once again, as with the Maryland definition of ICSP, the jury had no difficulty understanding the definition of an EMSP or in finding that BSI satisfied it. As the Supreme Court of California recently observed, "[T]he theoretical application of a statute's plain language to hypothetical extreme cases does not demonstrate that these literal words are absurd, and should therefore be disregarded or judicially modified to include a requirement the Legislature saw fit not to impose." *In re Ethan C.*, 279 P.3d 1052, 1070 (Cal. 2012).

The standing requirements of the Maryland and California statutes are clear and unambiguous. There is no room to impose a construction on them that would lead to a silly result.

Second, there is nothing "absurd" about permitting a party that purportedly has not proven a "genuine injury" to sue under a statute that does not require a "genuine injury" as a prerequisite to recovery.[3] The anti-spam statutes here do not require proof of actual damages, and nothing in the legislative histories of either law suggests otherwise. *See Maryland State Dept. of Educ. v. United States Dept. of Veterans Affairs*, 98 F.3d 165, 169 (4th Cir. 1996) ("To come within the ambit of this exception [to the plain meaning rule], however, the contrary intent must have been clearly expressed by the legislative body."). Rather, both statutes presume that a service provider or email recipient is harmed by false and misleading spam and thus confer standing on either party to recover liquidated damages. Many courts have held that state anti-spam statutes require neither proof of reliance nor damages.[4] *See, e.g., Hypertouch, Inc. v.*

[3] Although the statutes do not require proof of injury, BSI is prepared to show that it was, in fact, injured by Defendants' illegal spam. BSI produced ample evidence of actual damages and was deposed at length about those damages. *See* Ex. 1 (Pl.'s Supp. Rule 26(a)(1) Initial Disclosures to Connexus Corp.); Ex. 2 (chart of actual damages, BSI-DISCL 000001-000009); Ex. 3(Aug. 14, 2008 letter from A. Onorato to A. Rothman and accompanying production of receipts supporting actual damages (BSI-DISCL 000010-000084)); Ex. 4 (P. Wagner Depo. 984:9-1067:10 (June 16, 2009)); Ex. 5 (P. Wagner Depo. 40:3-43:5 (May 11, 2009)); Ex. 6 (Ex. 4 to the P. Wagner Depo. May 11, 2009)).

[4] Defendants raise their preemption argument once again, claiming that the Maryland and California statutes would be preempted if not construed to require plaintiffs to prove that they are "bona fide" service providers that have been "adversely effected" by illegal spam. Kraft Mot. Summ. J. at 40. This Court has twice addressed and rejected that argument, once in *Beyond Systems, Inc. v. Keynetics, Inc.*, 422 F. Supp. 2d 523, 538 (D. Md. 2006) (rejecting preemption and stating MCEMA "supplements the federal law. It does not frustrate the goals of the federal legislation; in fact it furthers them."), and then again when Defendants moved for summary judgment earlier in this case:

> That the gist of the statute is because there's misleading information in the transmission and not you have to rely on it. You don't have to show damages with regard. That's why you put statutory damages in. . . . I mean, if you have statutory damages, you clearly don't have to show damages. Why would you have statutory damages?

ValueClick, Inc., 192 Cal. App. 4th 805, 829 (Cal. App. 2011) (holding no harm required); *Asis Internet Servs. v. Subscriberbase Inc.*, No. 09–3503 SC, 2010 WL 1267763, at *7, 12 (N.D. Cal. Apr. 1, 2010) (same); *supra* note 4 (statement of J. Messitte).

Moreover, when proof of injury *is* required, both the Maryland General Assembly and the California Legislature have shown themselves perfectly capable of saying so. *See* Pl.'s Opening Br. 24-27. Thus, unlike the anti-spam statute, Cal. Bus. & Prof. Code § 17535 provides a claim for any violation of the state's general consumer protection law only when the plaintiff "has suffered injury in fact and has lost money or property as a result of a violation of this chapter." *See* Kraft Mot. Summ. J. 29, 35. But BSI's standing is not governed by § 17535, as the court

---

(June 14, 2010 Summ. J. Hrg. Tr. J. Messitte 94:22-25 & 95:22-24). That the Maryland and California statutes are not preempted by federal law is the law of this case and need not be revisited. *See also Hoang v. Reunion.com, Inc*., No. C-08-3518 MMC, 2010 U.S. Dist. LEXIS 34466, at *19 (N.D. Cal. Mar. 31, 2010) (holding CAN-SPAM "exempt[s] from preemption statutes such as § 17529.5."); *Hypertouch, Inc. v. ValueClick, Inc*., 192 Cal. App. 4th 805, 833 (Cal. App. 2011) (finding § 17529.5 not preempted by CAN-SPAM); *Asis Internet Servs. v. Consumerbargaingiveaways, LLC*, 622 F. Supp. 2d 935, 940 n.4 (N.D. Cal. 2009) (holding that "Defendants' arguments that plaintiffs . . . lack standing under the federal CAN-SPAM [Act] are irrelevant because plaintiffs' claims are based on their alleged status as email service providers under the state law."); *Asis Internet Servs. v. Subscriberbase, Inc.*, No. 09-3503 SC, 2010 WL 1267763, at *13-14 (N.D. Cal. Apr. 1, 2010) (holding that state laws that provide for broader enforcement authority than CAN-SPAM's are not preempted).

Defendants' related argument that BSI must prove that it was "adversely affected" to have Article III standing also is without merit. The Supreme Court has long recognized that a legislature "may enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute." *Linda R.S. v. Richard D.*, 410 U.S. 614, 617 n.3 (1973); *accord White v. Arlen Realty & Devel. Corp.*, 540 F.2d 645, 649 (4th Cir. 1975) (upholding plaintiff's standing to recover statutory damages under the Truth in Lending Act and explaining that "[i]t is essential to note that Congress in creating this statutory scheme did not . . . provide for suit only by debtors able to show that they were "aggrieved" by the creditor's inadequate performance. Rather, Congress gave the debtor a right to specific information and therefore defined "injury in fact" as the failure to disclose such information) (citing *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.")). Moreover, after concluding that the plaintiff in *Gordon* was not "adversely effected" under the CAN-SPAM Act and thus could not sue under that law, the Ninth Circuit proceeded to address the merits of the plaintiffs' state law claim. 575 F.3d at 1057-8. If "adverse effects" were synonymous with the "injury-in-fact" requirement of Article III, then the court could not have reached the merits of any claim, given that Article III standing is jurisdictional.

held in *Asis Internet Services v. Subscriberbase Inc.*, 2010 WL 1267763, at *7; it is governed by the anti-spam statute that does not contain a similar injury requirement:

> The problem with Defendants' argument is that section 17529.5 includes independent, non-exclusive standing and remedy provisions, which explicitly authorize "electronic mail service provider[s]" ("EMSPs") to bring a suit for liquidated damages against an entity that violates section 17529.5. Cal. Bus. & Prof. Code § 17529.5(b). *This section was not amended by Proposition 64. It contains no requirement that EMSPs suffer injury in fact, or lose money or property as a result of a violation.* By invoking this section, and by not seeking any injunctive relief under section 17535 of the FAL, or any other provision that was amended by Proposition 64, Plaintiffs have avoided the standing requirements imposed by the ballot initiative.

(Emphasis added.) *See also Hypertouch, Inc. v. ValueClick, Inc.*, 192 Cal. App. 4th at 829 (California's anti-spam statute "permits a recipient of a deceptive commercial e-mail to bring suit *regardless of whether they were actually mislead or harmed by the deceptive message*." (emphasis added)).

Third, nothing in the statutes or their legislative histories suggests that allowing an "opportunistic" plaintiff to sue would be absurd in the least. Legislatures commonly enact broad consumer protection legislation for the purpose of encouraging aggressive, private enforcement by private attorneys general. Granting enforcement rights to private individuals in this way is a powerful mechanism for states to achieve valid legislative objectives, particularly when the goal is to prevent and punish conduct that is detrimental to consumers at large, such the sending of false and misleading spam. As the Fourth Circuit explained when considering another consumer protection statute that also permitted private litigants even in the absence of economic harm,

> The scheme of the statute, as both sides agree, is to create a species of 'private attorney general' to participate prominently in enforcement. The language should be construed liberally in light of its broadly remedial purpose. . . . It invited people like the present plaintiff, *whether they were themselves deceived or not*, to

> sue in the public interest (emphasis added). Following familiar precedents, it encouraged such actions by providing, in addition to the incentive of public service, costs and a reasonable attorney's fee above the minimum recovery of $100.

White v. Arlen Realty & Devel. Corp., 540 F.2d 645, 649 (4th Cir. 1975) (quoting *Ratner v. Chem. Bank New York Trust Co.*, 329 F. Supp. 270, 280-81 (S.D.N.Y. 1971)).

As BSI has previously shown (Pl.'s Mot. Strike (DE 452-1) at 12-16) in the context of consumer protection laws, litigation by repeat plaintiffs is entirely compatible with the purpose of deterring unlawful conduct that otherwise would continue unabated. *E.g., Lemire v. Wolpoff & Abramson, LLP*, 256 F.R.D. 321, 327-28 (D. Conn. 2009) (explaining that an analogous consumer protection statute "'permits and encourages parties who have suffered no loss to bring civil actions for statutory violations,'" and holding that the plaintiff, who had brought multiple litigations over violations of the statute and was characterized by defendants as a "professional plaintiff," was nonetheless entitled to maintain suit and even to serve as class representative (quoting *Jacobson v. Healthcare Fin. Servs., Inc.*, 516 F.3d 85, 96 (2d Cir. 2008)).

The burden thus should be on *Defendants*, not on BSI, to explain why the Court should not apply the anti-spam statutes as written, and their reliance on cases like *Hsu v. Abbara*, 9 Cal. 4th 863, 872 (Cal. 1995), utterly fails to provide that explanation. Indeed, *Hsu* did not "reject [a] literal interpretation of [a] contract provision that would encourage vexatious and frivolous litigation," as Defendants contend. Kraft Mot. Summ. J. 29. The question presented in *Hsu* was a narrow one, limited to the factors that a court could consider in determining which party is the "prevailing" one for the purpose of awarding attorneys' fees. *Hsu's* holding actually *restricts* the circumstances under which a court may deviate from the plain meaning of statutory text on the basis of so-called "equitable considerations":

> We agree that in determining litigation success, courts should respect substance rather than form, and to this extent should be guided by "equitable considerations. . . . " But when one party obtains a "simple, unqualified win" on the single contract claim presented by the action, the trial court may not invoke equitable considerations unrelated to litigation success, such as the parties' behavior during settlement negotiations or discovery proceedings, except as expressly authorized by statute. . . . *To admit such factors into the "prevailing party" equation would convert the attorney fees motion from a relatively uncomplicated evaluation of the parties' comparative litigation success into a formless, limitless attack on the ethics and character of every party who seeks attorney fees under section 1717*. We find no evidence that the Legislature intended that the prevailing party determination be made in this way.

Id. at 877 (emphasis added).

Likewise, *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723 (1975), does not support Defendants' argument that this Court should effectively amend the Maryland and California standing provisions "to promote public policy against manufactured and vexatious claims." Kraft Mot. Summ. J. 29. The Fourth Circuit has held that cases such as *Blue Chip Stamps*, which involve *judicially-implied* causes of action, are inapplicable to *statutory* causes of action that expressly set forth the circumstances necessary to bring them. *Dunn v. Borta*, 369 F.3d 421, 430 (4th Cir. 2004) ("[B]ecause the causes of action under Section 10(b) and Rule 10b-5 are implied, the responsibility of defining those claims rests with the courts. In this dispute, however, the cause of action has been created by the Virginia General Assembly and codified at 13.1-522 of the Act. It would be inappropriate for us to augment a Virginia cause of action with a requirement that does not appear on the face of the statute.").

Most importantly, BSI's claims here are not manufactured or vexatious. BSI did not create the false and misleading spam at issue or otherwise convince Connexus or Kraft to send emails that they otherwise would not have sent. Defendants' spam was created and transmitted

by them for a specific purpose; it does not simply exist harmlessly in the ether. Defendants intended their spam to be received and opened by its recipients. That BSI was able to collect massive amounts of it is a function of one, and only one, thing: Defendants sent massive amounts of it to email addresses that were owned by or routed through the services that BSI provides. Had Defendants not created and transmitted false and misleading spam in the first place, there would be no claim. But they did, and although BSI's right to sue on it may be unsettling to Defendants, they have no one but themselves to blame. *Defendants* manufactured these claims, and it is their business that is vexatious. The Maryland and California statutes are intended to allow the BSIs of the world to aid in putting an end to Defendants' sharp practices.

The only "absurd" result is the one advocated by Defendants: a construction of the statutes such that each time an entity asserts its rights thereunder, it risks undermining its standing to assert those rights again in the future, leaving spammers free to continue sending their deceptive email messages. That is surely not what the legislatures of Maryland and California intended, and Defendants are incapable of citing any authority to the contrary.

B. *Gordon* Does Not Control Here as a Matter of Law and Is Distinguishable as a Matter of Fact.

1. The Standing Requirements of CAN-SPAM Are Distinguishable.

The Ninth Circuit held in *Gordon v. Virtumundo, Inc.*, 575 F. 3d 1040 (9th Cir. 2009), that a private plaintiff must be a "bona fide" provider of Internet access that is "adversely affected" by illegal spam to have standing to sue under the federal CAN-SPAM law. The court rested its decision on two grounds that are distinguishable from this case: (1) legislative history supporting the proposition that standing for private parties was limited to "bona fide" service providers, and (2) statutory language that expressly requires that a plaintiff be "adversely

affected." *Gordon*, 575 F.3d at 1052-53 (explaining that "adversely affected" requirement of standing is imposed by CAN-SPAM's text); 15 U.S.C. § 7706(g)(1); 150 Cong. Rec. E72-73 (daily ed. Jan. 28, 2004) (statement of John D. Dingell); *id.* at E73 (statement of Rep. W.J. "Billy" Tauzin)).

Neither the Maryland nor the California statutes or their legislative histories contains the phrases "bona fide" or "adversely affected" as prerequisite to standing, as a condition to obtaining relief, or in any other context. That, without more, conclusively demonstrates that *Gordon* is inapposite as a matter of law.

But this critical difference is not the only distinguishing feature. The federal CAN-SPAM statute and the Maryland and California anti-spam laws have vastly different enforcement mechanisms. CAN-SPAM was intended to be enforced primarily by the Federal Trade Commission, state attorneys general, and other federal or state authorities. 15 U.S.C. § 7706(a), (b), (f). Accordingly, the federal law allows only for a "*limited* private right of action," as described by the court in *Gordon*, 575 F.3d at 1048 (emphasis added). Only a "provider of Internet access service adversely affected" by a statutory violation can bring a civil action. *Id.* § 7706(g)(1). As the court observed, "[w]e believe that Congress's clear intention to restrict private action remains of great importance and guides the proper standing analysis." *Gordon*, 575 F.3d at 1050.

No such policy considerations underpin the Maryland or California statutes. To the contrary, the state laws in this case provide for much broader private rights and permit lawsuits by private persons and entities as the *primary* mechanism of enforcement. The Maryland law thus can be enforced by *both* an ICSP *and* an individual email recipient, the latter of which could number in the hundreds of thousands, if not the tens of millions. Md. Code Ann., Comm. Law

§ 14-3003. The California statute likewise can be enforced by both an EMSP and an email recipient. Cal. Bus. & Prof. Code § 17529.5(b)(1)(A).

The legislative histories of both state statutes also reflect the intent to *expand* standing to a broad class of private actors. Indeed, the original version of the Maryland statute in the Maryland House did not contain a provision for ICSPs or recipients to bring suit. *See* Ex. 7, House Bill 915. In reaction to this, the Maryland Attorney General sent a letter to the General Assembly to the effect that, as initially drafted, "House Bill 915 would have little impact in preventing deceptive spam." *See* Ex. 8, Letter from the Maryland Office of the Attorney General. The Attorney General urged lawmakers to "consider the approach taken by the Washington State law concerning deceptive spam, 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.* That, of course, is exactly what the General Assembly did by amending the bill to allow both ICSPs and email recipients to bring suit.

The reason that state law provides for an expanded right of action is apparent: allowing a larger class of plaintiffs to sue creates an even greater deterrent to spammers than do the relatively few cases that government agencies are able to investigate and prosecute.[5] Indeed, the wisdom of the state legislatures in expanding the class of eligible plaintiffs was prescient. The CAN-SPAM Act has proven to be uniquely ineffective and has been criticized since its creation. Maryland and California, by contrast, chose not to rely on overburdened state agencies to enforce their laws,[6] as expressly recognized by this Court:

---

[5] *See* FTC, Spam Summit: The Next Generation of Threats and Solutions (2007), *available at* http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf (noting that as of November 2007 (the most recent time data is available) the FTC has brought 90 enforcement actions total).

[6] Like Congress, some States have opted for more limited private enforcement and have limited standing under their spam laws to recipients who suffer actual injury. *E.g.*, Iowa Code Ann. § 716A.6 (West 2012) (providing a cause of action to "a person who is injured by a violation"). Legislatures are aware of these

> Getting the State Attorney General to undertake an action against one or more out-of-state spammers is much easier said than done. Inevitably political judgments must be made as to how limited resources are to be marshaled. Given competing law enforcement concerns, it is clear that only so many actions may be maintained against so many suspected offenders at any one time. More particularly, it is apparent that only so many actions can proceed against so many suspected spammers-in-state or out-of-state-at any one time. Granting individual recipients of spam the right to bring individual actions by holding out the possibility of substantial statutory damages for each transgression is a far more effective and efficient way to put the State's anti-spam policy into practice.

Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 535-36 (D. Md. 2006). By enacting statutes that allow ICSPs, EMSPs, and all recipients of illegal spam to sue for statutory damages without the need to show actual injury, Maryland and California have opted for broad private enforcement that distinguishes the state laws from federal law.[7]

This important difference in the scope of private rights of action conferred by state and federal law renders the "bona fide" and "adversely affected" elements of a federal claim under CAN-SPAM inapposite to the standing requirements under state anti-spam statutes. Indeed, *Gordon* itself acknowledges this distinction. In addition to his CAN-SPAM claim, Gordon brought suit under the Washington State anti-spam law. *Gordon*, 575 F.3d at 1057-58. Like the Maryland statute that was modeled after it, the Washington statute gives standing to both an "interactive computer service" and individual spam recipients. Wash. Rev. Code § 19.86.040.[8] Although not a topic of extended discussion in its decision, the court of appeals took no issue

---

different means for limiting standing, and the absence of any such limitation from the Maryland and California statutes is not accidental.

[7] *See also* Ex. 9, Amicus Brief of the Attorney General in *MaryCLE*, noting that MD-CEMA was adopted as a consumer protection measure; Ex. 10, Transcript of SB 538 ("You should vote for this bill to give Internet consumers a law they can use to seek damages from commercial email spammers. This law has worked effectively in the State of Washington.").

[8] Both the Maryland and Washington statutes use the same definition of "Interactive Computer Service [Provider]." *Compare* Wash Rev. Code § 19.190.010(8) *with* Md. Comm. Code § 14-3001(c)(1).

with Gordon's right to sue the state anti-spam statute: "In contrast to the more restrictive standing requirements of the CAN-SPAM Act, [the Washington statute] authorizes a recipient of a commercial e-mail message or an 'interactive computer service' to bring a private action." 575 F.3d at 1058 (noting that the defendant, who obviously had every incentive to challenge standing under *both* federal and state law, did not contest Gordon's standing to bring claims under the Washington statute). *See also Hoang v. Reunion.com, Inc.*, No. C-08-3518 MMC, 2010 WL 1340535, at *3 (N.D. Cal. Mar. 31, 2010) (recognizing that "CAN–SPAM . . . differs significantly from the Washington state [anti-spam] statute, both as to the type of conduct regulated thereby and the types of parties who may bring a suit thereunder.").

Other cases support the substantial differences between the CAN-SPAM standing requirements and those under state law. For example, in *Asis Internet Services v. Consumerbargaingiveaways, LLC*, the defendant cited the district court decision in *Gordon* and argued that the plaintiff lacked standing under California law because it did not meet the *Gordon* test. The court disagreed and held that "Defendants' arguments that plaintiffs . . . lack standing under the *federal* CAN-SPAM [Act], are irrelevant because plaintiffs' claims are based on their alleged status as email service providers under state law. 622 F. Supp. 2d 935, 940 n.34 (N.D. Cal. 2009). Another court, when analyzing the issue in terms of preemption, held that California could enact spam legislation that provides for a broader private enforcement mechanism than that of CAN-SPAM:

> The CAN-SPAM Act's preemption provision grants states the authority to regulate certain behavior . . . without regard to the methods that states may use to enforce these prohibitions. 15 U.S.C. § 7707(b)(1). It would be both unnecessary and disingenuous to attempt to impose parity in the standing provisions between the two statutes, by imposing a narrow reading on Congress's express reservation of this right for the states.

Asis Internet Servs. v. Subscriberbase, Inc., 2010 WL 1267763, at *13-14.

2. BSI Is Also Factually Distinguishable From Gordon.

Based on the Ninth Circuit's opinion, the plaintiff in *Gordon* appeared to have had a barebones operation *from the outset*, created solely for the purpose of collecting illegal spam and suing on it. Gordon appeared to provide no services whatsoever other than this. BSI, which was incorporated nearly six years before the state anti-spam laws were even enacted, is clearly distinguishable, as the evidence at trial demonstrated:

Gordon	BSI
Gordon's domain was hosted on leased server space, and he had substantial restrictions on the use of this leased server space.	BSI does not rent or access equipment remotely - its first email server was built in 1997 and it had email accounts running for various people and entities beginning in 1997, long before any anti-spam statutes had been enacted. (6/19 PM Trans. 78:17-20).
Gordon had an ordinary Internet connection	BSI has a "high speed ISP level" connection to the Internet. (6/20 AM Trans. 40:12-21)
Gordon had no physical control or access to the server hardware and had to access it virtually.	BSI's servers are physically located in its three points of presence in Silver Spring, MD Rockville, MD, and Washington, DC. (6/19 PM Trans. 66:8-67:4).
Gordon used GoDaddy to create email accounts and build web pages and did not supply those services himself.	BSI provided these and more services directly to customers including email, web, DNS, streaming media, e-commerce, Internet access, FTP and wireless access. (6/19 PM Trans. 71:25-73:23).
Gordon had no real customers	BSI had multiple customers, including the Young Women's Christian Home, St. Luke's House, Solar Electric Light Company, Barcroft Cycles, and Colorvivo Films. (*See* Pl.'s Opening Br. 3-18.

The services that BSI proved at trial and that the jury found to satisfy the definitions of ICSP and EMSP under Maryland and California law would, BSI submits, have satisfied the court in *Gordon*. In fact, given that the jury was permitted to consider (and was expressly instructed

on) virtually every extra-statutory factor that Defendants have extracted from *Gordon*, *see* Pl.'s Opening Br. 35-37, its Phase One verdict demonstrates that, even if *Gordon* had applied to this case, BSI would prevail.

3. BSI's Practices in Collecting Emails Do Not Disqualify it From Being an ICSP or an EMSP.

Finally, Defendants raise a series of arguments regarding BSI's practices, which somehow disqualify it from being a "bona fide" ICSP or EMSP. Kraft Mot. Summ. J. 33-34. Many of these contentions – including BSI's use of spam traps and wildcards, its policy of accepting all mail rather than rejecting possible spam, the separate and disputed issue of whether BSI uses spam filters, its use of litigation as a tool to combat spam, and the routing relationship between BSI and Hypertouch – are repeated in Defendants' separate argument regarding "consent," addressed below Part II.B. Whether considered in the context of "consent" or BSI's standing, however, none of BSI's practices disqualifies it from being an ICSP or an EMSP.[9] *See infra*, Part II.B.

In particular, Defendants assert that BSI and Hypertouch "target the same defendants, sue on the same emails, and share in settlement proceeds," and that such conduct should disqualify BSI from bringing suit against these Defendants. Kraft Mot. Summ. J. 34. But this argument is incorrect, both legally and factually.[10] As a legal matter, there is nothing improper about both Hypertouch and BSI suing the same defendant over the same email. If both entities received or routed that defendant's spam, it would be actionable more than once, just as would be the case if

[9] As demonstrated in the opening brief, the jury in fact considered BSI's efforts to block spam, its use of wildcard accounts, and its reasons for email archiving, and still found that BSI was an ICPS and an EMSP. Pl.'s Opening Br. 35-36. That alone disposes of Defendants' argument.

[10] As shown by Defendants' Exhibit No. 8, only 37 out of 8,945 currently at issue as to Kraft, and only 86 out of 28,137 emails at issue as to Connexus are the same emails claimed in another BSI suit. This represents only 0.33% of the total number of emails at issue in the case.

both Google and Verizon sued over the same spam after both companies' networks were implicated. Although much has been made of the routing relationship between BSI and Hypertouch, that issue is nothing but a distraction. BSI's use of Hypertouch as an intermediate routing partner does nothing to change the ultimate destination of the email at issue, because that is determined solely by the *sender* of the email (here, Defendants and their affiliates). Indeed, both statutes specifically contemplate that email transmissions involve the relay of messages by routing intermediaries.[11] Defendants cannot dispute that all of the emails at issue in this lawsuit were addressed to a domain that BSI holds as an ICSP and EMSP and that it is Defendants who are responsible for addressing the email to those domains. That is the *only* fact that matters to BSI's standing, and whatever intermediate routing path that these emails took to get to BSI is irrelevant.

There is also nothing inherently wrong with BSI suing multiple defendants over the same email. Kraft Mot. Summ. J. 15. Because both are complicit in the transmission of the unlawful email, the law permits a separate claim against advertisers and spammers.[12] *See* Cal. Bus. &

---

[11] *See* Md. Comm. Law § 14-3002(a) ("This section does not apply . . . to the extent that the interactive computer service provider . . . merely handles, retransmits, or carries a transmission of commercial electronic mail."); Cal. Bus. & Prof. Code § 17529.5 ("[T]here shall not be a cause of action under this section against an electronic mail service provider that is only involved in the routine transmission of the e-mail advertisement over its computer network.").

[12] Kraft's argument that Hypertouch's settlement with Kraft bars BSI's from suing here is defeated by the simple fact that *none of the emails for which BSI is suing Kraft was routed through Hypertouch*. Nor were any of those emails the subject of Hypertouch's settlement with Kraft. Although it is not mentioned in Defendants' brief, this Court excluded all such emails on the basis that claims over them were already settled. *See* DE 370 ¶ 3. All of the emails over which BSI is suing Kraft were thus sent directly to BSI's mail servers without any intermediate routing by Hypertouch. Hypertouch's settlement agreement with Kraft simply has nothing to do with BSI's standing to sue over these emails.

Similarly, although Defendants suggest that BSI is suing on the same MailCompanyX emails for which Hypertouch obtained a settlement against Connexus's predecessor Vendare, Kraft Br. 15, the testimony at trial made clear that Hypertouch sued on distinct emails:

> A. So, if I could be clear, the e-mails that I sued on didn't go to BSI, whatever part of BSI, those are e-mails sent to Hypertouch's domain name, hype has great food dot com.

Prof. Code § 17529(j) (West 2012) ("There is a need to regulate the advertisers who use spam, as well as the actual spammers."); *Hypertouch v. ValueClick*, 192 Cal. App. 4th at 821-22; Md. Comm. Law § 14-3002(b) (conspiring, initiating, or assisting in false or deceptive emails is prohibited).

II. BSI DID NOT "CONSENT" TO DEFENDANTS TRANSMITTING ILLEGAL SPAM, LET ALONE TO RECEIVING IT.

In a separate motion, Defendants argue that the "undisputed facts" show that BSI "consented" to receiving the underlying emails at issue and that this prevents BSI from proceeding any further with this case. This argument is fundamentally flawed.

First, this case is governed by two statutes, and nothing in those statutes states or even suggests that "consent" is a defense to liability.[13] Moreover, consent to harm should not be a defense to a statutory violation that does not require a showing of any harm. Indeed, a similar issue was raised during the debate in the Maryland General Assembly:

> Majority Whip: Well let me ask you this, an enterprise an individual wants to go about and actually start collecting a lot of monies, that could possibly be available by suing under this bill[.] [A]re they allowed to do that from home? Can they actually try to entrap someone into sending this kind of stuff?
>
> [Subcommittee Chairman]: I don't know how you entrap somebody into lying to you?[14]

(Trial Tr. at 6/27 J. Wagner Testimony 20:20-22). And while Defendants suggest that Hypertouch continued to route MailCompanyX emails to BSI at the same time that Joe Wagner was negotiating a settlement, they ignore the other side of that same coin: at the same time that Vendare was negotiating a settlement over unlawful spam with Hypertouch, it was continuing to send unlawful spam to BSI.

[13] California law does contain a reference to "consent," but that law's definition cannot help Defendants. The California statute provides in clear terms that "[d]irect 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) (West 2012) (emphasis added). Not only is there no evidence whatsoever of BSI's express consent to receive email from Kraft or Connexus, but consent does not apply to EMSPs.

[14] Maryland Commercial Electronic Mail Act: Floor Debate on Senate Bill 538, Audio Recording *available at* http://mlis.state.md.us/mgaweb/pyaudio.aspx (2002, Saturday, April 06, 2002, Session #1) (last accessed Sept. 14, 2012).

The wrong here was complete when Kraft and Connexus transmitted spam that BSI claims to have been false and misleading. Just as one cannot "entrap somebody into lying to you," one cannot "consent" to having a spammer transmit emails that violate the statute. Kraft and Connexus did that all on their own. BSI did nothing more than actively and aggressively collect evidence of Defendants' wrongdoing, and that does not equate to "consent" under any definition of that term.

Second, even if the issue of consent were legally relevant, it would merely be a *defense* to BSI's claims, and Defendants would be entitled to summary judgment only if they could demonstrate that no reasonable trier of fact could conclude other than that BSI had consented to all of the illegal emails that are at issue in this case. Summary judgment should be denied.

Response to Defendant' Statement of Undisputed Facts

Defendants include a list of "undisputed facts" purportedly relating to BSI's "consent" to receiving the disputed emails. However, Defendants do not assert that BSI took any actions to sign up to receive spam. All of the emails at issue in this case are unsolicited – *BSI never opted in or signed up for a single one*. The facts listed by Defendants regarding BSI's "consent" are genuinely disputed, and the fundamental requirement for granting a motion for summary judgment is absent:

1. Defendants assert as an undisputed fact that BSI agreed to receive spam routed to it from Hypertouch and that BSI requested more spam be sent to it from Hypertouch. Connexus Mot. Summ. J. ¶¶ 3, 4; Kraft Mot. Summ. J. 9-12, 18. BSI owns the hypertouch.com domain. Hypertouch, Inc.'s mail servers are the initial contact receipt point for BSI's incoming hypertouch.com email. Hypertouch is merely acting as the intermediate relay for BSI. (Ex. 11,

Feb. 17, 2012 Klensin Mini-Trial Report ¶ 33; Ex. 12, Jan. 24, 2012 P. Wagner Mini-Trial Report ¶ 74).[15] 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. (Ex. 12, Jan. 24, 2012 P. Wagner Mini-Trial Report ¶ 74). This routing happens automatically through a process called "routine conveyance." (Ex. 13, Feb. 17, 2012 Levine Mini-Trial Report ¶ 21; Ex. 12, Jan. 24, 2012 P. Wagner Mini-Trial Report ¶ 75). For other BSI-owned domains, such as castalia.net, those emails travel over service providers other than Hypertouch for delivery to BSI, or they might go directly to BSI. (Ex. 12, Jan. 24, 2012 P. Wagner Mini-Trial Report ¶¶ 74-75). However, the fact that messages were routed through Hypertouch does not change the party that actually authored the messages and caused them to be sent:

> [I]t cannot be legitimately claimed that Hypertouch was the sender of the message, let alone that because of the message routing that Plaintiff gave permission to receive these messages. This simply misconstrues the nature of how the email messages arrived at Plaintiff's servers and therefore incorrectly concludes that this constitutes consent to receive these messages.

(Ex. 14, Feb. 17, 2012 Resnick Mini-Trial Report ¶ 47).

2. The discussion of routing tables in Kraft's brief on page 9 does not take into account who sent the spam the emails in the first place. The routing of a message does nothing to change the originator of the message, and it does not change the end recipient to whom the sender addressed that message. (Ex. 11, Feb. 17, 2012 Klensin Mini-Trial Report ¶ 35). As Dr. Klensin stated, "the routing path has nothing to say about the addressing of the email in the first instance by the spammer to, in this case, BSI's domains. To claim that those arrangements constitute agreement on BSI's part to receive Defendant's messages, or that they somehow turn Hypertouch into the spammer, is inconsistent with good sense." (Ex. 11, Klensin ¶ 40).

[15] As noted above, references outside the trial record are included on the issue of consent, because consent was not decided by the jury during the mini-trial.

Defendants only look at the very last link in the chain (the routing from Hypertouch to BSI), but ignore how the spam was created and sent by them and their affiliates. Defendants' view of the facts gives the impression that Hypertouch is the spammer and that Defendants are innocent bystanders with clean hands. However, the destination of the message is determined entirely by the address of the recipient to whom the sender (*i.e.*, Defendants and their affiliates) chooses to send a particular email. (*Id.* ¶ 35). "The argument that BSI 'solicited' mail from Hypertouch willfully misunderstands Routine Conveyance." (Ex. 13, Feb. 17, 2012 Levine Mini-Trial Report ¶ 21).

3. Defendants claim as an undisputed fact that Paul Wagner wanted to receive emails in order to file lawsuits. Connexus Mot. Summ. J. ¶ 5. However, the quoted statement from Joe Wagner does not support this assertion. Joe Wagner was simply pointing out that he had filed actions in small claims court, which has no bearing on whether he consented to receive the emails in the first place. The trial record is clear that Joe Wagner decided aggressively to litigate against the entities that sent spam. Spammers made the decision to send BSI spam. Joe Wagner made the decision to go after them in court and found that this was a successful tactic. (Trial Tr. at 6/27 J. Wagner Testimony 73:6-7 ("And so they see the risk [of being sued] and often times they stop. I think most of the people that I've sued have stopped.")). Joe Wagner testified that when he went after an entity called AV Tech in small claims court, "[t]he day after they were in trial and they lost, no one anywhere on the Internet at all ever got anymore AV Tech spam. Stopped cold. So I guess in that sense, it's 100 percent effect spam filter." (Trial Tr. at 6/27 J. Wagner Testimony 73:22-25; *id.* 79:10-11 ("Even when I lost Stamp.com arbitration, stamp.com stopped spamming. Nobody in the world gets Stamp.com spam.")).

4. Defendants claim as an undisputed fact that Paul Wagner purchased a computer from Joe Wagner knowing it contained spam. Connexus Mot. Summ. J. ¶ 6. While it is undisputed that the sale of the "little mac" computer took place, it has no bearing on the consent. This transaction has nothing to do with consenting to receive the spam sent to the computer's mail server. Indeed, as the transcript from Connexus Exhibit 2 shows, Joe Wagner testified that the computer contained spam because "there's spam everywhere unfortunately." (Trial Tr. at 6/26 J. Wagner Testimony 154:24). Moreover, as the computer acted as a secondary mail server, there was no spam on the machine other than what incidentally might have been in the message queue, waiting to be delivered. (Trial Tr. at 6/26 J. Wagner Testimony 152:13-153:16 (stating that "there were no e-mails archived" on the machine and that "there must have been e-mails on it just in process.")).

5. Defendants claim as an undisputed fact that BSI and Hypertouch modified a setting on the CommuniGate Pro ("CG Pro") server application so that spam could be received and stored. Connexus Mot. Summ. J. ¶ 7. However, as Joe Wagner testified, the "return path" setting in CG Pro was changed because the return path verification had a number of drawbacks, including impeding delivery of desired mail as well as spam: "when it gets an incoming e-mail, it's saying, quickly says hold a second, and it goes to check to see if the from address, the return path works. And so if you're trying to exchange e-mail between servers, if, in fact, it doesn't work, CG Pro doesn't just note that it was bouncing it, so this would interrupt all e-mails, all of its users could be affected by this." (Trial Tr. at 6/26 J. Wagner Testimony 76:18-77:1; *id.* 163:7-163:14 ("You could stop receipt of ones where the return path doesn't, for example, doesn't verify, but that may mean that in fact just the other mail server is down or something.")).

6. Defendants claim as an undisputed fact that BSI and Hypertouch upgraded their equipment so that they could handle the receipt of more spam. Connexus Mot. Summ. J. ¶ 8. It is indeed an undisputed fact that both companies had to upgrade their equipment to deal with the large volumes of spam coming from Defendants and other spammers. (Trial Tr. at 6/26 J. Wagner Test. 174:4 ("We both had to have had the upgrade to handle the spam load.")). But the fact that BSI and Hypertouch needed to upgrade their equipment as a *consequence* of the massive flow of spam that they were receiving does not mean that, by doing so, they consented to that spam.

7. Defendants allege that BSI does not filter incoming email. Kraft Mot. Summ. J. 7, 18; Connexus Mot. Summ. J. ¶ 9. This is false, as has been stated many times during this litigation. BSI (and Hypertouch) filter all incoming mail. DE 295-42, P. Wagner Decl. ¶¶ 19-21, 26. Incoming mail to the hypertouch.com domain is filtered and delivered by Hypertouch to its users, and the rest of the mail is then relayed to BSI for filtering and delivery. *Id*. BSI filters using commercial filtering software, including SpamAssasin and SpamPal. *Id*. ¶ 26. BSI also relies in part on its upstream providers to assist in filtering spam, viruses and other threats. *Id*. ¶¶ 25-26. At trial, Joe Wagner discussed filtering on his domains, using "reasonabledoubt.com" as an example. (Trial Tr. at 6/26 J. Wagner Testimony 84:20-24 (discussing the spam filter on reasonabledoubt.com)). Nor was Mr. Marti, as Defendants claim, able to deny that BSI filters. Connexus Mot. Summ. J. ¶ 9. Mr. Marti was presented with BSI's interrogatory responses during his deposition that identify the several pieces of filtering software BSI employs, including Spam Assassin, Niversoft, PolluStop, Niversoft Clam AV, and SpamPal [transcribed as Spam-pow]. (Trial Tr. at 6/22 Marti Testimony 122:23-123:15; Ex. 15, 9/19/2008 BSI Response to Connexus' First Set of Interrogatories No. 1(h)). Marti conceded that he was not denying that

BSI uses spam filters, but rather that the filters were not, in his estimation, satisfactorily configured. (Trial Tr. at 6/22 Marti Testimony 123:9-15).

8. Defendants conflate email filtering and blocking. Kraft Mot. Summ. J. 7, 18. Spam filtering means detecting and flagging probable spam. (DE 295-46, Resnick Decl. ¶¶ 34, 42; DE 295-44, Klensin Decl. ¶¶ 45, 57; DE 295-42, P. Wagner Decl. ¶ 29). Kraft claims that 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." Kraft Mot. Summ. J. 18 (citing Trial Tr. at 6/21(am) Resnick Testimony 84:20-85:10). Resnick was *not* asked about "making no attempt to block or filter unsolicited mail" – a conflation by Defendants of blocking and filtering. Rather, when asked about archiving, he identified Google as a company that receives and saves email indefinitely. *Id*.

9. Defendants allege that BSI and/or Hypertouch could have blocked incoming spam. Kraft Mot. Summ. J. 7, 10, 18; Connexus Mot. Summ. J. ¶ 11. Not blocking does not equate to consent. Whether a service provider delivers spam to subscribers or sends the message back to its sender, it faces essentially the same burden: it must determine what the message is and where it should be sent. (DE 295-46, Resnick Decl. ¶ 33; DE 295-44, Klensin Decl. ¶¶ 45, 51). In short, it is entirely appropriate, if not preferable, for a service provider 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. *Id*. (DE 295-44, Klensin Decl. ¶¶ 48, 51-52; DE 295-45, Levine Decl. ¶¶ 11-13; DE 295-46, Resnick Decl. ¶¶ 32, 42). Indeed, Defendants' own expert admitted that his own institution, Texas A&M, accepts delivery of spam:

> Q: Do the users at Texas A&M have the option to view all the e-mail that is sent to them, or do you stop some of that e-mail from ever getting to them?
>
> A: We do stop, we don't block. We don't drop it. What we do is quarantine it and give them notice of the quarantine and then allow them to release it.
>
> Q: So you do accept delivery of spam?
>
> A: Yes.

(Trial Tr. at 6/22 Marti Testimony 124:12-19). At the very least, there is a dispute of material fact as to whether ICSPs and EMSPs are obligated to block spam and whether the failure to do so is tantamount to consent.

10. Defendants assert that BSI's use of spam traps was improper. Kraft Mot. Summ. J. 7; Connexus Mot. Summ. J. ¶¶ 12, 13. However, as Dr. 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." (DE 295-20, Klensin Dep. 190:23-191:17). 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.*; (DE 295-44, Klensin Decl. ¶ 50; DE 295-45, Levine Decl. ¶¶ 10, 12).

11. Defendants state that Resnick's definition of spam trap supports their position that spam traps were used to generate spam. Connexus Mot. Summ. J. ¶ 12. However, Resnick explained during the trial that "[i]f I used that phrasing, I was being very imprecise." (Trial Tr. at 6/27 Resnick Testimony 157:16-159:7). Resnick testified that in his opinion, use of spam traps by an ICSP or EMSP does not invite the sending of spam to that entity. (*Id.* 148:23-149:1.) As Resnick stated, "Not only does this not support Defendants' claim that Plaintiff consented to

receive email messages from Defendants, my opinion is exactly contrary to this claim: In my opinion, Plaintiff did not give consent to receive unsolicited commercial email messages from Defendants." (DE 295-46, Resnick Decl. ¶ 47).

12. Defendants state that BSI used wildcard addresses for the specific purpose of collecting spam. Kraft Mot. Summ. J. 8; Connexus Mot. Summ. J. ¶ 10. A "wildcard" means that a system can receive any combination of characters left of the "@[domain]. Like spam traps, wildcards do not in any way cause the sender to transmit mail to that address. Rather, they simply accept all mail addressed to the domain: "'Wild card addresses' have a long history of usage ... 'Wild cards' are not the same thing as 'spam traps . . . . what they [BSI and Hypertouch] are going [doing] is benign and passive: neither involves somehow finding, attracting, or authorizing spam that was not sent to Plaintiff's servers." DE 309-48 (Klensin Decl. ¶ 50). Kraft states that BSI's ability to accept email to an "erroneously addressed email" such as "xyz@hypertouch.com" shows its willingness to "attract" spam. Kraft Mot. Summ. J. 10 n.5. The characterization of an address containing essentially random letters and numbers as "erroneously addressed" is wrong. The only reason that these spam messages were sent to BSI in the first place is because of the mass mailings employed by Defendants. Indeed, as Levine pointed out, "In BSI's case, spammers sent a great deal of mail to invented or guessed addresses, so the catchall functioned as a spam trap, without any direct action by plaintiff to make it one." (DE 295-45, Levine Decl. ¶ 16).

13. Defendants allege that the posting of email addresses by Hypertouch on its webpage was used as a spam trap. Kraft Mot. Summ. J. at 8. As Resnick previously stated about these same allegations, "What Defendants refer to as a 'spam trap' is a web page shown to me during deposition as exhibits 257, 258, 259, and 305. As I testified in deposition, in addition to

stating a specific policy that no unsolicited commercial email be sent to addresses in the 'hypertouch.net' and 'hypertouch.com' domains, the page also lists email addresses which have been "opted out" of receiving commercial email (DE 295, Resnick Decl. Ex. 1 at 905:3-909:7). In my opinion, these exhibits appear to explicitly deny consent to receive email messages so addressed." (DE 295-46, Resnick Decl. ¶ 47). Moreover, Defendants have not identified which, if any, of the emails at issue was sent to an email address that had been "posted." In addition, at 11-12 Kraft cites communications between BSI and Hypertouch but never identifies what, if any, of the emails at issue – all dating from 2005 forward – were ever "consented to" by way of these irrelevant conversations.

14. Defendants state that BSI used opt-out requests as a means of intentionally receiving more spam. Connexus Mot. Summ. J. ¶ 13, 14; Kraft Mot. Summ. J. 8 n.3. Opting-out from receiving spam cannot be construed as seeking spam. BSI and Hypertouch attempted to use the "opt-out" mechanisms provided in spam emails they had received (typically a link to an "unsubscribe" web page) to get their domains taken off the distribution lists. They would use a unique email address that had never been used before for this purpose. (Trial Tr. at 6/26 J. Wagner Testimony 108:7-109:7). However, sending the opt-out request often resulted in even more spam being sent. *Id.* Indeed, when Joe Wagner sent an opt-out request to Kraft, he got 45,000 additional emails sent to the address. (Trial Tr. at 6/27 J. Wagner Testimony 76:10-78:7). Moreover, Defendants have not identified which, if any, of the emails at issue was sent to an email address that had opted-out.

A. Consent Is Not a Defense To Liability Under the Maryland and California Statutes.

Defendants' reliance on consent as an defense to BSI's statutory claims is flawed as a matter of law. There is nothing in the Maryland statute even suggesting that consent is a

defense. And although consent is mentioned in the California statute regarding recipients, it does not apply to EMSPs and has nothing to do with this case. Recovery in this case is a creature of state statute, and that is where the Court should look to determine whether a defense to recovery exists. *See Wang v. Massey Chevrolet*, 97 Cal. App. 4th 856,*871 (Cal. App. 2002) ("The third cause of action in the complaint was premised on violations of Business and Professions Code section 17200. [Defendant's] ground for summary judgment as to this claim was similarly based on the parol evidence rule, and on the premise that the defenses available to a common law fraud claim are applicable to a claim under Business and Professions Code section 17200. The latter contention is without merit.").

Defendants' argument also makes no logical sense. It rests on the premise that "BSI consented to the alleged harm about which it complains." Connexus Mot. Summ. J. 9. But it is hard to see how a plaintiff can consent to harm under a statute that does not even require harm. *See supra*, Part I.A.2, pgs. 8-10.

That consent is not a defense to claims under consumer protection laws like the anti-spam statutes here is supported by the case law. For example, under the Fair Credit Reporting Act, so-called "professional plaintiffs" were allowed to proceed with a claim notwithstanding that they "consented" to receiving defendant's junk mail. *See Murray v. Cingular Wireless II*, 242 F.R.D. 415, 418-19 (N.D. Ill. 2005) (holding that plaintiffs could maintain suit, even though "the named plaintiffs appear to greet the arrival of . . . junk mail . . . with joy and eagerly show their mail to lawyers at Edelman & Combs pursuant to a pre-existing agreement in the hope of finding an offer that presents a colorable FCRA claim"). Similarly, in the context of permitting "testers" to bring suit under laws like the federal Fair Housing Act, "the Supreme Court has held that standing exists to vindicate this right even when the testers 'fully expect [to] receive false

information, and [have] no intention of buying or renting a home.'" *In re Carter*, 553 F.3d 979, 989 (6th Cir. 2009) (quoting *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982)). It would make little sense – and, indeed, would frustrate the legislature's intent – to recognize standing to enforce these statutory prohibitions, only to reject the plaintiff's claim that the plaintiff "consented" to receive the defendant's illegal misrepresentations.

Moreover, it is not at all clear that Defendants are actually relying on "consent" in their motion. Rather, the cases that they cite seem to address "assumption of risk," which is typically a defense only in negligence cases. *See Hedding v. Pearson*, 173 P.2d 382, 385 (Cal. App. 1946) (discussing assumption of risk as a defense to a negligence case); *Janelsins v. Button*, 648 A.2d 1039, 1042 (Md. Ct. Spec. App. 1994) (assumption of risk is not a defense to a claim of battery). It is not normally a defense where the defendant's intentional conduct is at play. *See Janelsins v. Button*, 648 A.2d 1039, 1045 (Md. Ct. Spec. App. 1994) ("[J]urisdictions that have considered the issue of assumption of risk as a defense to an intentional tort have overwhelmingly rejected its applicability."); *Ordway v. Superior Court*, 198 Cal. App. 3d 98, 108 (1988) ("Historically, the doctrine of assumption of risk has provided a defense only to actions for negligence. It has little or no application in the case of intentional or reckless conduct."); *Aitken v. Commc'ns Workers of Am.*, 496 F. Supp. 2d 653, 660 n.4 (E.D. Va. 2007) ("Spamming is intentional."). Indeed, as one of the cases cited Defendants holds, "Because of the legitimate public policy of deterring and punishing intentional wrongdoing, the fact that a plaintiff 'assumed the risk' that such wrongdoing would occur cannot bar recovery for the wrongs perpetrated." *Janelsins*, 648 A.2d at 1046. At bottom, "[a] plaintiff could 'assume the risk' of an occurrence without consenting to it. As an example, a homeowner who leaves the front door unlocked for a few

minutes to chase an errant child may knowingly and voluntarily encounter a risk of daytime housebreaking, but does not consent to it." *Id.* at 1045 n.7.

B. At the Very Least, There Are Genuine Issues of Material Fact That Preclude Summary Judgment on the Issue of Consent.

Even if consent were a defense to liability under the two statutes here, no one can seriously contend that no genuine issue of material fact exists about this matter. Indeed, the record evidence supports the opposite conclusion – that BSI did *not* consent to receiving unsolicited emails, much less unsolicited emails that were false and misleading. As the parties moving for summary judgment on the issue of consent, Defendants bear the "initial burden of demonstrating the absence of a genuine issue of material fact." *Bouchat v. Baltimore Ravens Football Club, Inc.*, 346 F.3d 514, 527 (4th Cir. 2003) (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986)). Defendants have not carried their burden of showing that the facts to which they point are tantamount to "consent," and thus summary judgment must be denied.

Defendants contend that by 1) failing to filter and block incoming spam, 2) archiving spam, 3) sending opt-out requests to spammers, and 4) employing wildcards and spam traps to track down and identify the senders of spam, BSI somehow "invited" spam and "consented" to its receipt. As Defendants would have it, the failure to erect a fence around one's house, the decision to place a hidden camera in one's driveway, or the retention of photographs of trespassers all constitute an invitation to burglars and consent to home invasions. Ignoring the fact that Kraft and Connexus hire spammers to bombard entities and individuals with hundreds of millions of emails a day in the hope that some percentage will evade spam filters, blockers, and traps and reach their intended targets, Defendants seem to suggest that spam simply floats in the ether, and that "professional plaintiffs" like BSI affirmatively go out and trap it.

Defendants have it exactly backwards. It was they who created the emails; it was they who used harvesters and dictionary attacks to scour the Internet for targets; and it was they who sent the messages directly to those targets. There is not a shred of evidence that BSI consented to any of that. To the contrary, BSI has never consented to the receipt of illegal spam, and it presented substantial evidence at trial in support of that position.

1. BSI and Hypertouch Each Broadcast a "No UCE" Message to All Incoming Connections.

When an email message is sent, the receiving server responds with a transmission called an "SMTP banner." The SMTP banner is an electronic "greeting" identifying the receiving server and providing its domain and geographic location. Trial Tr. at 6/27 J. Wagner Testimony 68:6-69:1. The sender's email server "sees" the banner each time that it makes a connection. Trial Tr. at 6/27 J. Wagner Testimony 70:16-20; 71:21-25. Mail servers that send mail to BSI's domains must either transmit directly to BSI's mail servers, or else to Hypertouch's mail servers, which then route that mail on to BSI. (Ex. 12, Jan. 24, 2012 P. Wagner Mini-Trial Report ¶¶ 74-75). And as the evidence introduced at trial shows, Hypertouch's server answers all incoming mail transmissions with an SMTP banner that states "No UCE" (unsolicited commercial email) and that "Hypertouch has a policy against unsolicited e-mail advertisements." (Trial Tr. at 6/27 J. Wagner Testimony 71:1-18). And as shown in Exhibit 16, BSI's servers, like Hypertouch's, announce this same "No UCE" banner to any mail server sending email directly to it, along with the warning that "sending of unsolicited and/or deceptive bulk emails uses equipment of Beyond Systems located in Maryland and violates its policies." (Ex. 16, BSI SMTP banner; Ex. 17, Hypertouch SMTP banner). Thus, the evidence shows that both BSI and Hypertouch display these banners to tell all incoming connections that spam was not welcome and not wanted.

This SMTP banner is the digital equivalent of a "no trespassing" sign. That Defendants deliberately ignored it and pushed their illegal emails through does not mean that BSI ever consented to receive Defendants' messages. Indeed, it would be have been simple for Kraft and Connexus to interrupt the transmittal process as soon as their spam "saw" the SMTP banner. "Because that banner is sent before the sending site even sends its initial hello message, long before the e-mail is sent, a sending server could retrieve that banner, do that determination programmatically, look at that banner, and decide not to continue the session, basically block the spam from continuing because they could just hang up the connection." (Trial Tr. at 6/27 Resnick Testimony 145:11-16). In any event, the banner, standing alone, raises a genuine issue of material fact at the very least, and that, standing alone, should preclude summary judgment.

2. Sending an Opt-Out Request Does Not Constitute Consent to Receive Even More Spam.

Both Paul and Joe Wagner used the "opt-out" mechanisms provided in spam emails to get their domains taken off the spammer's distribution lists. It would use a unique email address that had never been used before for this purpose. Sending the opt-out request, however, often resulted in even more spam. (Trial Tr. at 6/26 J. Wagner Testimony 108:7-109:7). Indeed, when Joe Wagner sent an opt-out request to Kraft, he got 45,000 additional emails sent to the opt-out address. (Trial Tr. at 6/27 J. Wagner Testimony 76:10-78:7). Defendants have not identified which of the emails at issue were sent to an address that had opted-out beforehand.

Defendants argue that because BSI's opt-out requests resulted in more spam, and because BSI knew or should have known that opting-out might result in the receipt of more spam, BSI therefore "consented" to the spam. Connexus Mot. Summ. J. at 6. Connexus offers no authority for this position and does nothing to explain why a spammer's deceptive practices of sending even *more* spam to an email address that expressly opted *out* should result in a complete defense

to liability. There is – and there is no other way to put it – a certain "Alice in Wonderland" sensibility to that argument.

3. A Spammer's Transmission of Mail to a Spam Trap or to a Wildcard Entry in a Routing Table Does Not Mean That the Service Provider Consents to Receipt of the Spam.

Defendants next argue that BSI's use of spam traps and wildcard accounts constitutes "consent" to receive spam. But this argument fails, because it wrongly equates the use of measures designed to catch spammers in the act with affirmatively consenting to the Defendants' illegal conduct. As Defendants' concede in their brief, Kraft Mot. Summ. J. 8, spammers like Defendants often use "email harvesting" as a technique for acquiring addresses.[16] Email harvesting is a method of using an automated "crawler" to scan webpages for anything that looks like an email address and then to collect them for later use to send email marketing. (Trial Tr. at 6/26 Resnick Testimony 147:23-148:7). A "spam trap" is an email address embedded into the code of a website that is not given out to anyone. (Trial Tr. at 6/21(pm) Resnick Testimony 56:8-57:9). When an automated address harvester detects the address, it will be added to the spammer's advertising list. Id. If mail is sent to that spam trap address, then its owner knows that it must be unsolicited email. (Trial Tr. at 6/21(pm) Resnick Testimony 56:9-57:9; 6/27 P. Wagner Testimony 111:9-16).

The record showed that BSI uses spam traps as a way to track down spammers and to catch them red-handed when they engage in tactics like "email harvesting" – a tactic that, as noted above, is specifically outlawed by the California statute. Indeed, spam traps are commonly used by ICSPs and EMSPs. (Trial Tr. at 6/27 Resnick Testimony 147:6-11; *supra* ¶ 10).

[16] "Harvesting" email addresses and sending spam to them is a violation of the California statute. Cal. Bus. & Prof. Code § 17529.4 (specifically prohibiting the collection of emails posted on the Internet when used for spam and obtaining addresses "by using automated means based on a combination of names, letters, or numbers.").

Companies like Microsoft have set up spam traps that they have used in litigation against spammers. (Trial Tr. at 6/20(am) P. Wagner Testimony 48:23-49:8; *supra* ¶ 10). Indeed, Kraft's own email marketers use a company called LashBack which sets up a series of spam traps to monitor Kraft's compliance with CAN-SPAM. *See* DE 309-35, ¶¶ 23, 41. Connexus also uses spam traps and has itself filed suits for emails sent to such addresses. *See Vendare v. Liquid Marketing et al*. (Florida 05-80916) and *Vendare v. Does 1-10* (California 06-2479). As Connexus stated in its own complaint, the spam traps "do not appear anywhere else and have not been used for any purpose other than unsubscribing to future marketing emails from Plaintiffs or the Advertisers." Connexus saw the utility of using spam traps for the many of same reasons as BSI. As Connexus alleged, such emails "can identify or aid in the identification of [spammers'] true names and contact information." Ex. 18, Ex Parte Application ¶ 4 in *Vendare v. Does 1-10*.

A spam trap cannot itself create email, deliver email, or cause email to be sent. It is simply a receptacle for incoming spam that is used to identify sources of unwanted messages. *Id*. As Resnick testified:

> Q: In your professional expert opinion, sir, does the use of spam traps by an interactive computer service provider or an e-mail service provider invite the sending of spam to that entity?
>
> A: Absolutely not.
>
> Q: If I put a hidden camera on the outside of my house, am I inviting people to break into my house?
>
> A: I think that analogy is exactly right. In the same way that a spam trap is used to identify the person sending the spam, that camera on the outside of your house isn't asking someone to break in. It's if someone breaks in, you can identify them. If someone sends the spam, you can identify them because they used one of the addresses in the spam trap.

(Trial Tr. at 6/27 Resnick Testimony 148:23-149:10).

Like spam traps, the use of wildcard addresses or catch-all entries in a routing table did not "invite" the sending of spam to BSI ore equate to consent to receive that spam. (Trial Tr. at 6/27 Resnick Testimony 149:11-21; *supra* ¶ 12). As Defendants acknowledge in their brief, "Wildcard accounts capture e-mails that are sent to a domain name, but are not addressed or destined for any specific customers." Connexus Mot. Summ. J. ¶ 10. But Defendants' statement raises three crucial questions:

1. How is it that these emails come to be sent to a domain name, but not addressed to any specific customer?;
2. What gives spammers like Defendants the right to bombard the domains owned by an ICSP or an EMSP with deceptive spam in the hope of landing on a handful of "specific customers"?; and
3. If spammers engage in such tactics, why should they later be allowed to complain that their spam was received in an ICSP's or EMSP's wildcard entry?

As BSI's experts have explained, wildcards are merely passive receptacles that accept all email addressed to a domain; they do nothing to "cause" or "invite" the spammer to send that mail. *Supra* ¶ 12. "'Wild cards'" are not the same thing as 'spam traps' . . . what they [BSI and Hypertouch] are [doing] is benign and passive: neither involves somehow finding, attracting, or authorizing spam that was not sent to Plaintiff's servers." *Id*. They certainly do not provide any manifestation of "consent" on which Defendants can rely as a defense to their conduct. As the evidence in this case shows, spammers like Defendants commonly engage in a tactic known as "dictionary attacks," by which spammers send hundreds or thousands of messages to randomly-generated email addresses at particular domains, in the hope that some portion of these randomly-generated addresses will belong to active customers. (Ex. 11, Feb. 17, 2012 Klensin

Mini-Trial Report ¶ 29). BSI's use of wildcards does not force the Defendants to engage in such tactics, nor does it constitute consent to their spam. *Supra* ¶ 12. But wildcards *do* allow BSI to preserve a record of all unlawful spam sent to its domains, and to use that evidence to hold the senders of that spam accountable. At bottom, the only thing Defendants have shown is that the thousands of deceptive emails that they addressed to BSI's domains successfully arrived there. They have not explained how this fact equates to "consent." At the very least, in light of the statements of BSI's experts that the use of wildcards is not equivalent to consent, there is a genuine issue of material fact as to whether Defendants' have established BSI's consent that must be resolved by the finder of fact.

4. BSI's Filtering or Blocking of Email In No Way Means it Consented to Receive Spam

Defendants argue that BSI consents to receive spam because it does not filter or block email. *First*, the allegation that BSI does not filter incoming email is false, as has been stated many times in this litigation. BSI (as with Hypertouch) does, in fact, filter incoming email using professional, commercial filtering software, and always has. *Supra* ¶ 7. Counsel for Kraft admitted as such to the Court: "BSI had spam filters on its servers, Your Honor. It had spam filters." (Trial Tr. at 6/27 169:5). As such, to the extent that this argument is relevant to consent, it is disputed.

Second, Defendants conflate the concepts of filtering and blocking. *Id.* ¶ 8. Spam filtering means detecting and flagging probable spam. *Id.* BSI filters all incoming email, but it does not block incoming email. The reasons for not blocking are several. *Id.* ¶ 9. As an initial matter, though, there is no obligation for an ICSP/EMSP to block any email. *Id.* As the California legislature observed, one of the problems with spam is that it shifts costs from spammers to recipients or EMSPs. Cal. Bus. & Prof. Code § 17529(h) (West 2012) ("The 'cost

shifting' from deceptive spammers to Internet business and e-mail users has been likened to sending junk mail with postage due or making telemarketing calls to someone's pay-per-minute cellular phone."). The primary flaw, then, with Defendants' argument is that it assumes that service providers are required to take active measures to block spam, even though the point of these anti-spam laws is to put the burden of illegal spam on the *spammers*.

Further, BSI's experts have made abundantly clear that there is no obligation to filter or block spam. *Supra* ¶ 9. As they have stated, it is entirely appropriate, if not preferable, for a service provider 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. *Id*. (citing DE 295-44, Klensin Decl. ¶¶ 48, 51-52; DE 295-45, Levine Decl. ¶¶ 11-13; DE 295-46, Resnick Decl. ¶¶ 32, 42). Indeed, Defendants' own expert admitted that his institution, Texas A&M, accepts delivery of spam. *Id*. Defendants' argument that BSI's choice (like most ICSPs/EMSPs) not to block incoming email (and instead to flag probable spam so that recipients can make the decision what to do with it) has no bearing on consent.

5. The Routing Relationship Between BSI and Hypertouch Does Not Prove That BSI Consented to Receive Spam from Defendants.

As an initial point, the entire issue of the "routing relationship" should not even be relevant. There are no longer any emails at issue in this case as to Kraft that were routed from Hypertouch to BSI. This Court excluded all such emails on the basis that claims over them were already settled. DE 370 ¶ 3. The only Kraft emails left in the case are those that Defendants sent directly to BSI's domains.

As described above, Hypertouch's mail servers are the initial receipt point for BSI's incoming hypertouch.com email. Hypertouch is merely acting as the intermediate relay for BSI.

(Ex. 11,Feb. 17, 2012 Klensin Mini-Trial Report ¶ 33; Ex. 12, Jan. 24, 2012 P. Wagner Mini-Trial Report ¶ 74). Incoming mail to those addresses is filtered and delivered by Hypertouch to its users, and the rest of the mail is then automatically relayed to BSI for filtering and delivery. *Supra* ¶¶ 1, 2, 7. Defendants imply that none of this mail would wind up at BSI's servers were it not for Hypertouch. But as Klensin states unequivocally: "even if Hypertouch never existed, mail directed to BSI-held addresses by the senders, such as Defendants, would still arrive at its destination – BSI – over some other ISP's network." (Ex. 11, Feb. 17, 2012 Klensin Mini-Trial Report ¶ 36). The notion that BSI "consented" to receive spam because it went through Hypertouch on its way to BSI and this completely absolves Defendants from all responsibility for sending the spam in the first instance is wrong on both counts. "The unsolicited mail that BSI received was addressed to BSI by spammers, and its route through Hypertouch didn't change that." (Ex. 13, Feb. 17, 2012 Levine Mini-Trial Report ¶ 21).

Indeed, both statutes confirm that the violation occurs during the initial transmission of the message by the sender. *See* Cal. Bus. & Prof. Code § 17529.2 (unlawful to initiate an unsolicited commercial email); Md. Comm. Law § 14-3002(b) (a person may not "initiate the transmission" of unlawful email). "[T]o claim that an ISP that receives email routed through another ISP's systems somehow has consented to receive the email on the basis of that routing relationship is simply a misunderstanding of how Internet email works." (Ex. 14, Feb. 17, 2012 Resnick Mini-Trial Report ¶ 48). The routing of a message does nothing to change the originator of the message, and it does not change the end recipient to whom the sender addressed that message. (Ex. 11, Feb. 17, 2012 Klensin Mini-Trial Report ¶ 35).

CONCLUSION

For the reasons stated in BSI's opening brief and in this opposition to Defendants' post-trial motions, the Court should (1) hold that BSI has standing to sue under the Maryland and California statutes, and (2) deny Defendants' motion for summary judgment on the issue of "consent."

Date: October 22, 2012 Respectfully submitted,

/s/

Thomas M. Barba (D. Md. Bar No. 28487)
Roger W. Yoerges (D. Md. Bar No. 14088)
Jeffrey E. McFadden (D. Md. Bar No. 8738)
John J. Duffy (D. Md. Bar No. 28613)
STEPTOE & JOHNSON LLP
1330 Connecticut Ave., NW
Washington, D.C. 20036
T: 202-429-3000
F: 202-429-3902
tbarba@steptoe.com
ryoerges@steptoe.com
jmcfadden@steptoe.com
jduffy@steptoe.com

Anthony A. Onorato (D. Md. Bar No. 28622)
STEPTOE & JOHNSON LLP
1114 Avenue of the Americas
New York, NY 10036
T: 212-506-3900
F: 212-506-3950
tonorato@steptoe.com

Counsel for Plaintiff Beyond Systems, Inc. and Third-Party Defendants James Joseph Wagner and Hypertouch, Inc.

Of Counsel:

Stephen H. Ring (USDC-MD Bar No. 00405)
Law Offices of Stephen H. Ring, P.C.
506 Main Street, Suite 215
Gaithersburg, Maryland 20878
T: 301-563-9249
F: 301-563-9639
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.

TABLE OF EXHIBITS

1. BSI's Supplemental Rule 26(a)(1) Initial Disclosures to Connexus Corp.
2. BSI-DISCL 000001-000009, Chart of Actual Damages
3. August 14, 2008 Letter to A. Rothman and enclosed BSI-DISCL 000010-000084, Production of Actual Damages Receipts
4. Excerpts of Deposition of Paul A. Wagner, June 16, 2009
5. Excerpts of Deposition of Paul A. Wagner, May 11, 2009
6. Exhibit 4 to May 11, 2009 Deposition of Paul A. Wagner (BSI Responses to Defendants' First Set of Interrogatories)
7. Maryland House Bill 915 Text
8. Letter from Maryland Office of Attorney General Regarding House Bill 915
9. Brief Amicus Curiae of the Maryland Attorney General, MaryCLE
10. Press Release Regarding Senate Bill 538
11. February 17, 2012 Minitrial Report of John Klensin
12. January 24, 2012 Minitrial Report of Paul Wagner
13. February 17, 2012 Minitrial Report of John Levine
14. February 17, 2012 Minitrial Report of Peter Resnick
15. September 19, 2008 BSI Response to Connexus' First Set of Interrogatories, No. 1
16. BSI SMTP Banner Disclosure
17. Hypertouch SMTP Banner Disclosure
18. Ex Parte Application in *Vendare v. Does 1-10*

CERTIFICATE OF SERVICE

I hereby certify that on this 22nd day of October, 2012, the foregoing PLAINTIFF'S POST-TRIAL MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT was filed electronically in accordance with the Court's CM/ECF procedures, and served electronically on the below-named parties by the Court's electronic notification system:

Barry J. Reingold
John M. Devaney
John K. Roche
PERKINS COIE LLP
700 Thirteenth Street N.W.
Washington, D.C.
20005-3960
(202) 654-6200 (Telephone)
(202) 654-6211 (Facsimile)
jroche@perkinscoie.com
breingold@perkinscoie.com
jdevaney@perkinscoie.com

Darrell J. Graham
Peter S. Roeser
John E. Bucheit
ROESER, BUCHEIT & GRAHAM LLC
20 N. Wacker Dr., Ste. 1330
Chicago, IL 60606
(312) 922-1200
dgraham@rbglegal.com
proeser@rbglegal.com
jbucheit@rbglegal.com

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

J. Douglas Baldridge
Lisa Jose Fales
Ari N. Rothman
VENABLE LLP
575 7th Street NW
Washington, D.C. 20004
(202) 344-4000 (Telephone)
(202) 344-8300 (Facsimile)
jdbaldridge@venable.com
ljfales@venable.com
anrothman@venable.com

Counsel for Defendant Connexus Corp.

/s/
Jennifer M. Newton