



**Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580**

**COMMENTS OF
THE INTERNET COMMERCE COALITION**

**CAN-SPAM ACT RULEMAKING
Project No. R411008**

(Advance Notice of Proposed Rulemaking)

I. Introduction

The Internet Commerce Coalition ("ICC") submits these comments in response to the Commission's ANPRM on various topics related to the CAN-SPAM Act, Pub. L. No. 108-187. ICC members include leading Internet and e-commerce companies and trade associations, including AT&T, BellSouth, Comcast, eBay, MCI, SBC Communications Inc., TimeWarner/AOL, Verizon, the U.S. Telecomm Association, CompTel, and the Information Technology Association of America.

Our members work very hard to protect consumers from spam, suing more than 150 spammers, operating 24x7 response teams to respond to spammer attacks, implementing a wide

range of spam filtering technologies, working on more secure e-mail systems of the future and, in many cases, offering consumers flexible self-help filters to combat spam.

These comments address eight issues raised by the ANPRM:

- The “transactional or relationship” messages definition should be interpreted to include a narrowly defined exception for e-mails sent within the scope of affirmatively expressed consent of the recipient.
- The “primary purpose” test in the definition of commercial e-mail means that promotion of a commercial product or service must be “*the* primary purpose” of the e-mail, measured objectively.
- It is important that the Commission clarify the meaning of the term “sender” under the CAN-SPAM Act. When it does so, the Commission should specify that a website or online service that offers tell-a-friend e-mail technology to its users is not a “sender” of those messages for purposes of the CAN-SPAM Act.
- It is equally important that the Commission clarify that, except in situations where e-mail marketers provide others with financial incentives to send e-mail messages on the marketer’s behalf in order to evade opt-out requirements under the Act, there is no more than one sender of a commercial e-mail message.
- The Commission should clarify that aggravated violations include the violations set forth in § 5(b) and encompass each of the violations set forth in 18 U.S.C. § 1037(a) and conduct described in 28 U.S.C. § 994 note (b)(2)(A)(ii).
- The 10-business-day deadline for honoring opt out requests should be extended substantially to 31 calendar days.
- The valid “physical postal address” element of notice required by § 5(a)(5)(A)(iii) should be interpreted as inclusion of a street address at which the sender may be contacted.
- An ADV labeling requirement would not be effective in protecting Internet users against spam.

In our members’ experience, there are two very different sorts of commercial e-mail activity. The first, which we refer to as “outlaw” spam, is sent using falsification or hacking techniques and fails to identify the sender of the message or the sender’s physical location. It often makes the false claim that a consumer opted in to receiving the message and offers falsified

opt-out information, or uses a network of “affiliate senders,” dummy corporate names, a chain of bank accounts, or other methods to frustrate efforts to prove who sent and who paid for the message. These outlaw spam messages frequently advertise illegal or objectionable products or services, and generate the overwhelming majority of consumer complaints about spam.

The second category of e-mail is sent by legitimate businesses who do not falsify the source of the message, accurately identify themselves in the e-mail message, and make serious efforts to respect recipient opt-out preferences. In our members’ experience, these e-mailers generate very few consumer complaints, burden ISP networks far less, and raise far fewer public policy problems.

The ICC urges the Commission to be mindful of the practical differences between these two categories of senders and implement tough regulation of the first category of e-mail, while clarifying several ambiguities in the statute that affect senders of commercial e-mail who fall within the second category.

II. Specific Issues Raised in the ANPRM

A. Transactional or Relationship Messages

The categories of transactional or relationship messages do not appear to raise potential for abuse, and accordingly should not be narrowed.

The Commission should clarify ways in which the transactional or relationship message exception applies to communications with existing customers who have affirmatively consented to receive communications from the sender. In particular, ICC members engage in frequent one-to-one e-mail communications with high-volume current customers with the customer’s consent. We are concerned that application of a notice and opt-out requirement could significantly impede

use of e-mail for such spontaneous one-to-one communications in order to service an existing account.

At a minimum, the Commission should clarify that the transactional or relationship message exception in § 3(17)(A)(i) of the Act for e-mails sent to “facilitate, complete or confirm a commercial transaction” permits commercial e-mail communications within the scope of an agreement between the sender and an existing customer for a “product update” service that informs existing customers of new products or services with their affirmative consent.

More generally, where the sender has an ongoing, existing business relationship with the recipient involving payment for a product or service provided by the sender, the sender has a strong incentive to respect customers’ preferences regarding receiving commercial e-mail. In this context, the Commission should seriously consider clarifying that a transactional or relationship exception applies to e-mail messages sent with the affirmative consent of recipients in this limited context.

Question B.9. of the ANPRM asks whether the “primary purpose test” applies to determining whether a message is a transactional or relationship message. The statute specifically provides that the primary purpose test applies. See § 3(17)(A).

B. Primary Purpose Test

The ANPRM asks a number of questions regarding how to interpret the primary purpose test for determining whether an e-mail is a commercial e-mail. Congress’ choice of the phrase “*the* primary purpose” compels the conclusion, as the ANPRM suggests in Question A.1., that commercial advertisement or promotion “is more important than all of the e-mail’s other purposes combined.” Congress could have used terms such as “a primary purpose,” “a non-

incidental purpose,” or “a partial purpose” to determine whether an e-mail is commercial, but did not do so. Accordingly, this interpretation best effectuates congressional intent.

Moreover, by choosing the term “purpose,” Congress made the intent of the sender/initiator the central issue in determining whether the an e-mail is commercial. However, the sender’s intent may be established through objective evidence, such as the content of the message, the context in which it was sent, how the message compares to other e-mails by the same sender, and other similar factors. Above all, it is important that this test be clear so that senders, ISPs, and law enforcement know what the statute covers and when it can be enforced.

The Commission also should clarify in its proceeding that e-mails sent for commercial purposes other than those described in the statutory definitions of commercial e-mail message and transactional or relationship message are not regulated by the Act. It would be helpful if the Commission provided specific examples of such commercial messages—for example, e-mail messages sent for the purpose of negotiating an agreement with the recipient, or e-mail surveys sent to improve the sender’s products or services.

C. Clarifying the Meaning of the Term “Sender”

It is important that the Commission clarify the meaning of the term “sender,” as it is one of the most complex definitions in the CAN-SPAM Act, it is central to defining the scope of the recipient opt-out right under the statute, and the complexity of applying this term creates significant operational challenges for companies that send commercial e-mail and for ISPs that are occasionally called upon to evaluate whether senders of commercial e-mail over their networks are honoring opt-out requests. This complexity has led some senders to include opt-out notices from multiple advertisers in a single commercial e-mail message. Under the plain language of the Act, “senders” must “initiate” e-mail messages and have their product or service

advertised in those messages. § 3(16)(A). “Initiators” include entities that originate or transmit e-mail messages, or procure origination or transmission. § 3(9). Actions of ISPs used by senders are exempt from the initiation definition as “routine conveyance.” § 3(9) & (15).

The key statutory term bearing on whether a third party is a sender of an e-mail message transmitted or originated by someone else is the definition of “procure.” To “procure” a message, an entity must intentionally pay or provide other consideration to, or induce another person to initiate an e-mail message “*on one’s behalf*.” § 2(12) (emphasis added). This test hinges on whether the e-mail message is actually sent “on behalf of” an entity.

Interpretation of this provision is guided by one of only three statements of policy in the CAN-SPAM Act, that: “recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from *the same source*.” § 2(b)(3) (emphasis added). This statement reflects Congress’ intent that opt-outs apply to e-mail from the same entity who sent the message, rather than multiple entities. It thus supports a “single sender” interpretation, even though there may be multiple initiators of the same message. See § 3(9).

The Senate Commerce Committee report regarding the meaning of the term “procure” states that “[t]he intent of this definition is to make a company responsible for e-mail messages that it hires a third party to send . . .” S. Rep. No. 108-102, 108th Cong. 1st Sess. at 15 (2003). Significantly, even though the version of the “procure” definition reported by the Senate Commerce Committee contained the same operative terms as the final definition—“pay, or provide other consideration to, or induce, another person to initiate a message on one’s behalf”—the report language provides no indication that the definition covers multiple entities.

Accordingly, Congress’ intent in crafting this provision is best reflected in an interpretation of the terms “procure” and “sender” that covers affiliate and related programs used

by spammers to hire or pay others in attempts to evade opt-out responsibilities for their e-mail marketing campaigns. However, these terms should not be interpreted so as to produce more than one sender unless a procurer attempts to evade opt-out obligations under the statute by providing compensation to a third party to initiate messages on the procurer's behalf, and both the initiator's and the procurer's products or services are advertised in the message.

Whatever test the Commission adopts should clearly distinguish between legitimate commercial offerings that bundle more than one service together and those that are designed to evade the requirements of the Act. Furthermore, the Commission should make clear that an entity that specifically prohibits, makes good faith efforts to prevent, and does not know of violations by affiliate marketers does not "procure" their messages.

Should the Commission wish to consider in its Notice of Proposed Rulemaking an interpretation that would create multiple senders in other contexts, we suggest that it request comment on whether multiple senders should be deemed to exist only where:

- both senders' products or services are advertised in the message;
- all non-transmitting senders have paid or provided consideration to the transmitter to send the message;
- the message appears to be sent by both senders;
- the message is sent "on behalf of" both senders, rather than primarily for the benefit of one sender who, for example, may send a message on its own behalf containing content from multiple advertisers; and
- both senders are actively involved in formulating the marketing appeal (rather than simply allowing use of a company's marks subject to the company's approval) and in providing or selecting the e-mail addresses used in the marketing campaign.

1. Tell-A-Friend Messages

The ANPRM asks at Questions E.3.a. through f. whether “forward-to-a-friend” e-mail marketing should be subject to regulation under the Act. “Tell-a-friend” features, which many ICC members employ, taken as a whole are a good example of e-mails that are sent by consumers solely on their own behalf. The consumer who transmits the message exercises total control over whether the message is sent and what it recommends. The consumer also selects and controls the recipients to whom the message is sent. And the message comes from the consumer—typically without any collection of the e-mail addresses by the website or service that supplies the tell-a-friend functionality.

In fact, treating the provider of the tell-a-friend function as a “sender” would require the provider to capture where such messages are being sent and to scrub messages for opt-outs, increasing costs and potentially encouraging monitoring and tracking of such messages, which would itself raise privacy concerns. It also would run counter to consumer expectations because when consumers send an e-mail to their friends and family, they expect their friends and family to receive it. If consumers attempted to send an e-mail to friends who had opted out of messages from the provider of the tell-a-friend technology, the consumers would be informed that they were not allowed to e-mail their friends through this service.

2. Multiple Advertiser E-mails

Similarly, where multiple advertisers’ products are advertised in an e-mail circular that an initiator, such as Circuit City or Buy.com, assembles and controls, only the initiator is the “sender” of the e-mail message. The initiator is sending the communication on its own behalf, not on behalf of advertisers whose products it is promoting, and is the only entity required to provide an opt-out under the CAN-SPAM Act.

Clarifying that multiple advertisers within a message do not need to provide consumers opt-outs is fully consistent with the purpose of the Act, which states in Section 2(b)(3), as one of three congressional policies advanced by the statute, that “recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail *from that same source.*”

It also avoids creating serious disincentives to e-mails promoting multiple advertisers’ products or services because, under a contrary rule, those e-mails would need to be run against the opt-out lists of *every single advertiser*. This would encourage the sending of more e-mail, as advertisers’ communications would have to be separated and sent in separate e-mails, thereby increasing the total number of e-mails recipients receive. It also would increase the cost of and delay the sending of such messages, and prevent recipients who had opted out of e-mail contacts by one company whose product or service was advertised in an e-mail circular from receiving e-mail regarding any of the other companies whose products or services were advertised.

In ICC members’ experience, it is legitimate Internet retailers who send e-mails containing advertisements from a large number of advertisers, not outlaw spammers, who generally advertise a single website. Furthermore, the sender of the e-mail circular must honor consumer opt-out requests and generally sends more commercial e-mail than the advertisers themselves, and is thus the more effective “funnel” for opt-out requests from consumers who do not want to receive such e-mails.

D. Aggravated Violations

As explained in the introduction to these comments, ICC members have unparalleled experience trying to block spam and bringing civil enforcement actions against spammers. From this difficult experience on the front lines of the battle against spam, the ICC has reached the

conclusion that each of the spamming techniques prohibited in Section 4(a) or listed as a possible sentencing enhancement criterion in Section 4(b) of the Act are “contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection [5](a).” § 3(c)(2).

These methods are the tools through which spammers hide their identities, penetrate the technology defenses that ISPs and consumers erect to protect against spam, or illicitly obtain e-mail addresses. Each should be subject to strong civil penalties—as well as criminal prosecution.

The statutory aggravated violations specified in § 5(b) of the Act cover: (1) harvesting, which is a serious deterrent to users posting their e-mail addresses in a public location, and dictionary attacks, which seriously burden networks and create enormous numbers of bounce-backs; (2) automated e-mail account registration; and (3) use of open proxies and open relays to “relay or retransmit” spam.

However, § 5(b) does not cover sending spam by means of: (1) hacking into a computer and originating spam, (2) falsifying header or routing information in spam, (3) materially falsifying header information, (4) materially falsifying registration information for 5 or more e-mail accounts or two or more domain names, or (5) falsely representing the right to 5 or more Internet protocol addresses. 18 U.S.C. § 1037(a)(1), (3)-(5). Nor does it cover sending spam knowing that the messages involved in the violation contained or advertised a URL for which the registrant for the name provided false registration information—which hide the identity of the owner of the site advertised through the spam. § 4(b)(2)(A)(ii).

All are important tools of spammers and methods that significantly contribute to the proliferation of spam by hiding spammers’ tracks and frustrating efforts to filter out or bring

enforcement actions against spam. No company defended any of these practices during the development of and consideration of S. 877 or S. 1293 (the criminal spam bill that was merged with S. 877 on the Senate floor and became Section 4 of the CAN-SPAM Act). To our knowledge, no legitimate company engages in any of these behaviors, and these behaviors have no legitimate use in connection with sending commercial e-mail.

Congress decided that each of these activities was so serious that it should be criminalized or be considered as a possible enhancing factor by the U.S. Sentencing Commission. All should be aggravating factors for purposes of civil penalties in the Act.

E. 10-Business-Day Time Frame for Honoring Opt-Out Requests Should Be Extended

In ICC members' experience, although opt-outs may be effectuated very quickly in some instances, a 10-business-day time frame is too short to effectuate opt-outs for companies with multiple e-mail databases, companies that use third-party e-mail service providers to send commercial e-mail, and for companies involved in joint marketing arrangements if both companies are deemed to be "senders" for purposes of the CAN-SPAM Act.

We suggest that the Commission establish a 31-calendar-day opt-out period, which is consistent with the time frame under the Telemarketing Sales Rule. Because we expect that database compatibility and technologies for implementing opt-out requests will improve over time, we suggest that the Commission adopt this extended opt-out period on an interim basis and consider shortening the period at a later date.

F. "Valid Physical Postal Address" Should Require a Street Address

Because the ability to serve process on outlaw spammers is very important to the integrity of commercial e-mail, the ICC believes that the Commission should interpret the term "valid physical postal address" in § 5(a)(5)(A)(iii) as requiring that senders supply a street address

where the sender may be found, and a separate mailing address (if the sender's mailing address is different).

Outlaw spammers and procurers of outlaw spam who use falsified e-mail that violates the criminal provisions of the CAN-SPAM Act and § 5(a)(1) routinely list only a P.O. Box in their commercial e-mails and in registering for domain names—often a P.O. Box for which the registrant has supplied falsified information. Although convenient and appropriate for legitimate senders of commercial e-mail, we are concerned that allowing listing of only a P.O. Box to suffice under the statute would lead to abuse by outlaw spammers.

Furthermore, requiring that the sender merely list a valid P.O. Box on its e-mail would effectively write the term “physical” out of the phrase “valid physical postal address” because P.O. Boxes are mailing addresses. To give some meaning to the word “physical,” something more than a mere P.O. Box listing is required. We submit that Congress' intent can best be advanced by providing that a street address is a “physical” address. This result would not significantly burden legitimate senders of commercial e-mail, while assisting significantly in enforcement of the Act.

G. A Subject Line Labeling Requirement Would Not Measurably Reduce Objectionable Commercial E-mail

Before passage of the CAN-SPAM Act, more than 20 state laws, including laws of major states such as California, imposed ADV labeling requirements. Spammers routinely flouted this requirement, as evidenced by an FTC study of commercial e-mail that found that only 2% of e-mail bore this label. *False Claims in Spam*, A Report by the FTC's Division of Marketing Practices, April 30, 2003, at 11.

We are not aware of any state enforcement of those laws. We suspect that this is because spammers falsified other aspects of many of the e-mails that violated this requirement, frustrating enforcement.

Although labeling in theory would be somewhat effective in helping to filter out spam, in practice, professional spammers almost never label their messages. Simply enforcing the requirements in § 5(a)(1) and 18 U.S.C. § 1037 that spammers not falsify the origin of their messages and bringing enforcement actions for aggravated violations would be sufficient to allow users and ISPs to protect themselves from the overwhelming majority of unwanted commercial e-mail.

A simple ADV labeling requirement likely would have costs to commercial e-mailers, because programs keyed to block e-mails with that label would block all such e-mails, effectively presenting only an all-or-nothing choice to Internet users regarding whether to receive unsolicited commercial e-mail when consumers may desire a more nuanced choice.

Subject line labeling requirements may also raise compelled speech issues under the First Amendment, whereas prohibitions against falsification do not.

We thank you for considering our views, and would be pleased to answer any questions you may have.

Respectfully submitted,



James J. Halpert
General Counsel
(202) 861-3938