April 20, 2004

VIA ELECTRONIC SUBMISSION

CAN-SPAM Act
P.O. Box 1030
Merrifield, VA 22116-1030

RE: CAN-SPAM Act Rulemaking, Project No. R411008

Dear Federal Trade Commission members:

We have reviewed the effects the CAN-SPAM Act has had on curtailing spam. Go Daddy Software, Inc., offers domain name registration, web site hosting, email service, and related products and services. We receive numerous complaints every day from our customers who have received spam, as well as complaints from others who believe that our customers are using our email services to send spam. We submit the following responses to your questions.

A. Criteria for Determining Whether "The Primary Purpose" of an Electronic Mail Message is Commercial.

1. The term "the primary purpose" could be interpreted to mean that an email's commercial advertisement or promotion is more important than all of the email's other purposes combined. Does this interpretation provide relevant criteria to help determine the primary purpose of an email? Why or why not? When an email has more than one purpose, what determines whether one purpose is more important than all other purposes combined?

> The term "primary purpose" is insufficiently vague, and does not clarify how much of an email must be commercial in order to be considered a commercial email under the CAN-SPAM Act. (Similarly, "primary purpose" does not clarify how much of an email must be transactional or relationship in order to be considered transactional or relationship under the CAN-SPAM Act) We recommend that "primary purpose" be defined as "constituting 51% or more of the total visible text and code within the email," and whether a recipient would "reasonably believe it was a commercial email."

2. The term "the primary purpose" could be interpreted to mean that the email's commercial advertisement or promotion is more important than any other single purpose of the email, but not necessarily more important than all other purposes combined. Does this interpretation provide relevant criteria to help determine the primary purpose of an email? Why or why not? When an email has more than one purpose, what determines whether one purpose is more important than any other purpose?

This interpretation of "primary purpose" is also too vague, and even worse, it would allow a majority of an email to consist of unwanted portions, because it would allow "UBE," or unsolicited bulk email, to make up a portion of the email, and that combined with a portion of unsolicited commercial email could potentially make up more than 50% of an email, as long as there was a clear portion dedicated to a relationship or transactional purpose that was ostensibly the most "important" part of the email.

3. In other contexts, the FTC has stated that marketing material is to be judged by the net impression that the material as a whole makes on the reasonable observer. The "net impression" standard has been used to assess the meaning of an advertisement and the adequacy of disclosures. This standard takes into account placement of disclosures within the marketing material, the proximity of disclosures to the relevant claims, the prominence of the disclosures, and whether other parts of the marketing material distract attention from the disclosure. Should this "net impression" analysis be applied to determining whether the primary purpose of an email is a commercial advertisement or promotion? Why or why not? Are there considerations unique to electronic mail that would influence the application of such analysis, and if so, how?

The "net impression" standard is a good start, and we recommend that the definition include whether a recipient would "reasonably believe it was a commercial email," which we addressed above in Question (1).

4. The term "the primary purpose" could be interpreted to mean that a commercial advertisement or promotion in an email is more than incidental to the email. Does this interpretation provide relevant criteria to help determine "the" primary purpose of an email? Why or why not?

See our discussion above in Question (1). "More than incidental" is insufficiently vague.

5. In determining whether a commercial advertisement or promotion in an email is the primary purpose of the email, one approach could be to base the analysis on whether the commercial aspect of the email financially supports the other aspects of the email. For example, an electronic newsletter may be funded by advertising within the newsletter. Such advertising arguably would not constitute the primary purpose of the newsletter. Does the issue of whether the commercial aspect provides the financial support for non-commercial content provide relevant criteria to help determine the primary purpose of an email? Why or why not? Is this an appropriate way to approach the question of whether an email's primary purpose is commercial? Why or why not?

Allowing the commercial part of an email to dominate a transactional or relationship email if that is how the email is being funded would allow virtually anyone to claim that their ads are financially supporting their emails, hence giving them a free pass to make advertising the majority of their transactional or relationship emails.

6. Should the identity of an email's sender affect whether or not the primary purpose of the sender's email is a commercial advertisement or promotion? Why or why not? For example, if a professional sports league sends email promoting its involvement with a charitable organization, should that email be considered to have a commercial "primary purpose" under the Act based on the league's "for-profit" status?

No, because there is too much room for abuse. Furthermore, we believe the CAN-SPAM Act should be expanded to restrict UBE as well as UCE, which would include charitable organizations and make this distinction irrelevant.

7. Are there other ways to determine whether a commercial advertisement or promotion in an email is the primary purpose of the email? Do these approaches provide relevant criteria to help determine the primary purpose of an email? Why or why not?

We have addressed this in Question (1).

B. Modifying What Is a "Transactional or Relationship Message"

1. Have any changes in electronic mail technology or practices occurred since the CAN-SPAM Act became effective on January 1, 2004, that would necessitate a modification of the CAN-SPAM Act's definition of "transactional or relationship message" to accomplish the purposes of the Act?

Not that we are aware of.

2. Email messages that facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender are considered transactional or relationship messages under the Act. Are the terms "facilitate, complete, or confirm" clear, or is further clarification needed to prevent evasion of the Act's requirements and prohibitions?

The language is too vague. We recommend adding that a recipient would "reasonably expect to receive such notifications."

3. Email messages that provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient are considered transaction or relationship messages under the Act. Should the Commission modify or elaborate on this definition? Why or why not?

See our answer in this section to Question (2). Additional language should be added here specifying that the frequency the emails are sent to each customer must be reasonable.

4. Email messages that provide notice concerning a change in the terms or features of a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender are considered transactional or relationship messages under the Act. Should the Commission modify or elaborate on this definition? Why or why not?

See our answer in this section to Question (2).

5. Email messages that provide notification of a change in the recipient's standing or status with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender are considered transactional or relationship messages under the act. Are the terms used in this subsection of the act (Sec. 3(17)(A)(iii)) clear, or is further clarification needed to prevent evasion of the Act's requirements and prohibitions?

See our answer in this section to Question (2).

6. Email messages that provide, at regular periodic intervals, account balance information or other types of account statements with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender are considered transactional or relationship

messages under the Act. Should the Commission modify or elaborate on this definition? Why or why not?

> See our answer in this section to Question (2). This definition should be expanded to state that the account or membership must still be active, the recipient must have initially clearly agreed to receive periodic emails, and the frequency of the emails must be reasonable in light of what the recipient agreed to.

7. Email messages that provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled are considered transactional or relationship messages under the Act. Should the Commission modify or elaborate on this definition? Why or why not?

> See our answer in this section to Question (2). Additional language should be added here specifying that the frequency they are sent to each customer must be reasonable.

8. Email messages that deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender are considered transactional or relationship messages under the Act. Should the Commission modify or elaborate on this definition? Why or why not?

> See our answer in this section to Question (2). Additional language should be added here specifying that the frequency the emails are sent to each customer must be reasonable.

9. Some transactional or relationship messages may also advertise or promote a commercial product or service. In such a case, is "the primary purpose" of the message relevant? If so, what criteria should determine what is "the primary purpose?" Should such messages be deemed to be commercial email messages? Should they be deemed transactional or relationship messages? Why?

> See our answer in this section to Question (1).

C. Modifying the 10-Business-Day Time Period for Processing Opt-Out Requests

1. Is ten (10) business days an appropriate deadline for acting on an opt-out request by deleting the requester's email address from the sender's email directory or list? Why or why not? If not, what time limit would be appropriate? Why?

> Ten (10) business days is more than enough time for senders to remove a recipient from their database, because email marketing is generally all electronically automated. It is very easy to remove an email address from a database of email addresses. Plus, a 10 day time limit leaves 10 days for an alleged spammer to continue spamming a complaining recipient, and it also makes it more likely the alleged spammer will not respond to the complaining recipient right away but may put it off for a few days, which can escalate nerves. Therefore, five (5) business days would be preferable to 10.

2. What procedures are required to delete a person's email address from the sender's email directory or list? What reasons, if any, prevent such deletion in a time period shorter than ten (10) business days? What burdens, including costs, would be borne by senders if the time period were shortened? What benefits to consumers would result from a time deadline shorter than ten (10) business days for effectuating an opt-out request?

There should be a confirming email sent to the complaining recipient stating that their email address has been removed from their database, and that their email address will not be distributed. The benefit to consumers of a shorter time span to effectuate an opt-out request is that there would be less spam.

3. What costs are associated with deleting a person's email address from a sender's email directory or list? What costs does the recipient bear from unwanted electronic mail during the period from submission of the request to the effectuation of that request?

There are very little costs associated with deleting a person's email address from a database, since mailing lists are almost always electronically automated.

4. What currently is the average time to create and implement procedures to delete a person's email address from a sender's email directory or list following that person's opt-out request? What factors affect the length of time necessary to create and implement these procedures?

It takes a few seconds to delete a name out of a mailing list, and most mailing list programs are already set up with delete procedures already in place for the removal of email addresses, and many also already have procedures in place so complaining recipients can automatically click on a link and be removed, without having to ever go through a live person for assistance. Since most email campaign software programs already have opt-out features built into them, compliance with CAN-SPAM simply means making sure that the email program a sender selects has those minimal options.

5. What currently is the average time in which a request to be removed from an email list is processed once these procedures have been created and implemented? What factors affect the length of time necessary to process such a request?

At Go Daddy, it takes a few seconds to remove a complainant's email address from an email campaign database, since the process for removing email addresses is fully automated; recipients simply click on a link to remove their address.

6. What is the industry standard, if any, regarding the time frame to create and implement procedures for processing opt-out requests? What is the industry standard, if any, regarding the time frame to process opt-out requests once procedures have been created and implemented?

Not known.

7. How are lists of email addresses used for electronic mail marketing maintained, distributed, and used? What impact, if any, do the maintenance, distribution, and use of these lists have on the time it takes to effectuate an opt-out request?

Lists of email addresses are frequently sold by unscrupulous spammers to others for commercial use involving unsolicited email campaigns. It can be difficult for a recipient to opt out, because the senders who purchase and use these lists may disguise their origin and may not honor a recipient's request to opt out. Often, instead of removing a complaining recipient's email address from a database, the complainant's email address is labeled "a live one," and the email address becomes even more targeted for unsolicited email.

8. How do the size and structure of the sender's business, the use of third-party e-mailers, and the manner in which opt-out requests are received affect the time it takes to effectuate an opt-out request?

> Most senders, whether small or large, use automated email campaign programs (see our answer to Question 4 in this section). These programs are very inexpensive, so even one-person businesses use them. If a third party is used to actually send the emails, we recommend that an additional five (5) days be given to process an opt-out request. If there are multiple companies sending advertisements within one email, the burden should be on the sender who initiates the email to provide an opt-out link at the bottom of the email. Since it would be nearly impossible to have recipients opt out of every advertisement within the email (it would be quite difficult for an advertiser to keep track of which customers of *other* companies have opted out of emails that involve their ads, since that would involve sharing customer information between companies, which violates many of their privacy policies), we recommend clarifying that advertisers who are not the primary sender of an email are not responsible for providing an opt-out link. If a company is composed of more than one entity, we recommend that the law clarify that both the opt-in option and opt-out link state whether or not a recipient is opting in and out of all of the affiliate companies.

D. Identifying Additional "Aggravated Violations"

1. Section 5(c)(2) of the Act gives the Commission authority to "specify additional activities or practices to which [Sec. 5(b)] applies if the Commission determines that those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under [Sec. 5(a)]." Section 5(b) identifies four "aggravated violations." What additional activities or practices, if any, should be treated as "aggravated violations" under the Act? Why should these activities or practices be considered "aggravated violations?" How do these activities or practices contribute substantially to the proliferation of commercial e-mail that violates Sec. 5(a)? Do these activities or practices have any use other than initiating e-mail that violates the Act?

> Harvesting or mining of email addresses and "mail bombing," sending hundreds of thousands of emails to one recipient in order to crash their email program or system, should also be treated as aggravated violations under the CAN-SPAM Act; since they involve situations where the recipients clearly did not opt-in. Harvesting and mining includes obtaining email addresses from WHOIS searches, Web site crawling, scanning Usenet postings, querying finger daemons, and can also be obtained using manual methods. Since these senders know they are going to receive many complaints because the email addresses were not obtained through opt-in choices, these senders tend to falsify their header information and "from" lines, which violates Section 5(a) of the Act. Their opt-out links, if there are any, tend to be false or do not work properly, because the senders do not want to have their real identity traced. We are aware of no legitimate reason for harvesting or mining email addresses and in many cases, such harvesting is likely to violate proposed database protection statutes. The definition of harvesting email addresses should also include buying or selling email addresses, if the email addresses are of recipients who did not previously opt in to having their email addresses sold to other companies.

2. Are there new technologies that have been developed or are in development that would contribute substantially to the proliferation of commercial e-mail that is unlawful under Sec. 5(a)? If so, what are they? Should they be added to the list of "aggravated violations" under Sec.

5(b)? Why or why not? What are the costs and benefits to industry in implementing procedures to overcome these technologies? What are the costs and benefits to consumers? Do these new technologies have any use other than initiating e-mail that violates the Act?

Not known.

E. Issuing Regulations Implementing the Act.

1. Section 3(16) of the Act defines when a person is a "sender" of commercial e-mail. The definition appears to contemplate that more than one person can be a "sender" of commercial e-mail; for example, an e-mail containing ads for four different companies. In such a case, who is the "sender" of the e-mail? What costs or burdens may be imposed on such entities if all are determined to be "senders"? What costs or burdens may be imposed on consumers if only the entity originating the e-mail is determined to be the "sender?" If a consumer previously has exercised his or her rights under Sec. 5(a)(3) by "opting out" from receiving commercial e-mail from one of the companies advertised in the e-mail example above, has Sec. 5(a)(4) of the Act been violated? If so, by whom?

See our answer to Question (8) in Section C. We recommend that the definition of "sender" be, "the entity most responsible for putting the email together, arranging for its transmission, and appearing to be the entity sending the email." There should be a burden on the advertisers within the email, or the entity that physically sent the email, to notify the "sender" if they receive an opt-out request from a recipient. The "participating advertisers" should be defined as, "companies represented in commercial email that could be reasonably considered as benefiting from the email, and that knowingly participated in the email." If a recipient has opted out from one of the participating advertisers, Section 5(a) of the Act has not been violated, unless there are extenuating circumstances demonstrating that a participating advertiser was actually a sender. The definition of "sender" should not include a company's affiliates, unless the companies are so closely intertwined that a reasonable person would conclude they were the same entity.

2. Should the Commission use its authority in Sec. 13 to issue regulations clarifying who meets the definition of "sender" under the Act? If so, how? If not, why not?

Yes. See our answer in this section to Question (1).

3. The Act defines "initiate" to mean originate or transmit, or procure the origination or transmission of, a message. In turn, the term "procure" means to pay, provide consideration, or "induce" a person to initiate a message on one's behalf.

(a). Do "forward-to-a-friend" and similar marketing campaigns that rely on customers to refer or forward commercial e-mails to someone else fall within the parameters of "inducing" a person to initiate a message on behalf of someone else?

No.

(b). Are there different types of such "forwarding" marketing campaigns? What forms do these campaigns take?

These types of email marketing campaigns do take different forms. The most nefarious ones involve advertisers that continue to send email messages that appear to be from the original "friend," well after the original friend first agreed to forward an email on. This should be prohibited, or at a minimum, a requirement should be added that the advertiser put in prominent writing that

emails will continue to be sent out under their name, and there should be an opt-out link within the email. Each "friend" who forwards an email on to another friend should not be held liable under the Act, unless it is clear that they are sending the email to someone they do not know.

(c). Should these marketing campaigns have to comply with the Act? Why or why not? If so, who should be considered a person who "initiates" the message when one recipient forwards the message to another person? Who should be required to provide an "opt-out" mechanism for the message? Should each person who forwards the message be required to comply with the Act? Should the original sender of the message remain liable for compliance with the Act after the original recipient forwards the message to someone else? Why or why not?

The forward-a-friend types of email campaigns should have to comply with the Act to the extent that the emails should contain opt-out links. They should also contain clear and conspicuous notice of which friend forwarded the email.

(d). Do the Act's requirements and prohibitions reach e-mail messages containing advertisements sent by using a Web site that urges or enables individuals to e-mail articles or other materials to friends or acquaintances? How, if at all, does the Act apply to this situation when recipients have previously "opted-out" of receiving e-mails from the advertised entities?

A less offensive form of forwarding emails from a friend is the "send this article to a friend" feature, where advertisers sometimes slip in ads at the end of the email, or elsewhere within the email. A restriction should be placed on this practice to prevent advertisers from sneaking advertisements into these emails, unless the advertisements already appear on the web page next to the article. If a recipient has previously opted out of receiving emails from that entity, but a friend is the one initiating the email, the CAN-SPAM Act should not apply.

(e). Should unsolicited commercial e-mail campaigns that rely on having customers refer or forward the e-mail to other parties be treated differently from other unsolicited commercial e-mail? Why or why not? If there are different types of these campaigns, should the different types be treated differently? Why or why not?

See our prior answers in this section. If the emails are legitimately forwarded by one friend to another, then the only provision of the CAN-SPAM Act that should apply is the requirement for an opt-out link at the bottom, which will apply to the advertiser. There should also be a requirement that no additional ads may be added to the email, which don't already appear next to the article on the web site.

(f). If referrals or forwarding of e-mails should be distinguished from other types of e-mail, how should they be distinguished? What, if any, restrictions should be placed on them? Why? What disclosures, if any, should be required? Why? Should the Commission distinguish between different types of "forwarding" campaigns? Why or why not?

See our answer to Question (3)(b) in this section. If an advertiser continues to send out additional emails, ostensibly from the initiating friend, that situation is different from a friend simply sending one email.

(g). What are the costs and benefits of forwarded commercial e-mail campaigns to consumers? To businesses? Are the costs and benefits to consumers and industry different for forwarded commercial e-mail campaigns than for other types of unsolicited commercial e-mail? Why or why not?

No comment.

4. Section 5(a)(5)(A)(iii) requires the disclosure of "a valid physical postal address of the sender" in each commercial electronic mail message. How should this required disclosure be interpreted? Should a PO Box be considered a "valid physical postal address?" Why or why not? Should a commercial mail drop be considered a "valid physical postal address?" Why or why not?

We have no objection to using a P.O. Box or commercial mail drop as a valid physical postal address. However, if a commercial mail drop is used, it must be capable of receiving mail of this type. For example, a sender cannot use his employer's address if his email list is part of his personal business, and his employer has a policy against accepting employees' personal mail.

5. Section 5(a)(1), regarding false or misleading transmission information, addresses information displayed in a message's "from" line. Is the Act sufficiently clear on what information may or may not be disclosed in the "from" line? What "from" line information should be considered acceptable under the Act? Why? If a sender's e-mail address does not, on its face, identify the sender by name, does that e-mail address comply with Sec. 5(a)(1)?

This section of the Act needs to further clarify what a "materially misleading" email address constitutes. For example, if a company named Brown's Electronics is sending out a newsletter purportedly from newsletter@brownselectronics.com, but the email address isn't technically a valid working email address, although everything else is CAN-SPAM compliant, including containing an opt-out link, is the email address considered "materially misleading?" It is not clear from the Act. If a sender's email address doesn't on its face identify the sender by name, this should not be a violation of 5(a)(1) of the Act unless there are additional circumstances demonstrating intent. For example, if the rest of the email makes it clear which entity is sending the email, the rest of the email is CAN-SPAM compliant, contains a valid opt-out link, and the email address isn't pretending to be someone else, then the email address shouldn't be required to specifically name the sender.

F. National Do Not E-Mail Registry Report
past deadline to respond

G. System for Rewarding Those Who Supply Information About CAN-SPAM Violations.
1. What kinds of information would be most useful in facilitating enforcement of the Act? What kinds of information can the FTC reasonably expect to receive? Would such information likely be received in a form and manner that would make it useful in an enforcement action to prove violations of the Act? How would this information advance the Commission's ability to identify and locate people who violate the Act? How could a system for rewarding those who supply information about violations of the Act be structured? What are the relative costs and benefits?

The information that should be reported in order to facilitate enforcement of the CAN-SPAM Act includes: complete and unaltered emails with full headers, a description of how and where the email was received, logs of any previous requests to opt-out by the recipient(s), a list of all known complaints received regarding that particular email or entity, and any other relevant history or information available. The best way for the FTC to efficiently receive this information is to allow the submitter to copy and paste the information into a form online. Receiving email information in electronic form is equal to printing out an email and physically emailing it; it is generally considered equally admissible. This process would considerably advance the FTC's ability to find

violators, because it would allow the FTC to communicate directly with the parties who encounter the violators, instead of having to seek out violators using its own methods. There should be very little cost, since most of the process will involve ISPs and others copying and pasting the relevant information into an automated electronic form.

2. What procedures would be necessary to determine who is "the first person that identifies the person in violation of the Act, and supplies information that leads to the successful collection of a civil penalty by the Commission," as specified by the Act? What other procedures would be necessary to implement a reward system, e.g., to resolve disputes among competitors seeking to be "the first person that identifies the person in violation of the Act"?

We recommend that the FTC establish criteria to address these situations, and establish a small panel for adjudication of these disputes.

3. Is the phrase "identifies the person in violation of the Act" sufficiently clear to provide a bright line with respect to who will be entitled to a reward? If not, how can deciding this issue be made more certain?

See our answer to Question (1) in this section above. Not only must the violator be identified adequately, but the violation must be adequately identified.

4. How would the prospect of receiving a portion of civil penalties collected by the FTC affect existing incentives for persons who have information about the identity of spammers to come forward with such information?

Giving a portion of the civil penalties collected by the FTC to those who report violations would be an excellent incentive for reporting violations, since there is currently very little incentive to report violations. Most laws against spamming that provide civil penalties require the offended party to initiate the prosecution on their own, and provide very small monetary penalties, so it is not worth it for most people to pursue violators.

5. How would a reward system affect the behavior of ISPs and other industry participants with regard to initiating and conducting investigations of spammers, and other approaches to addressing unsolicited commercial email? Under what circumstances, if any, would ISPs and other industry participants likely submit information under a proposed reward system? What factors would be relevant to an ISP's choice whether to proceed under a reward system as opposed to proceeding under the private right of action for ISPs created by Sec. 7(g) of the Act? Specifically, what kind of information would ISPs and other industry participants likely supply, and in what format? Would such information likely be received in a form and manner that would make it useful in an enforcement action to prove violations of the Act?

ISPs and others would be more likely to report violators to the FTC if the process was quick and easy, and provided a large enough monetary reward. See our answers to Questions (1) and (2) above.

6. How successful have been the efforts of private entities or others to establish and operate reward programs similar to the one contemplated in the Act? Have such reward programs been successful in eliciting information otherwise unavailable to support enforcement or other legal action? Have such reward programs been successful in achieving the goal of reducing or deterring certain conduct?

We have never heard of any successful reward programs.

7. How might the Commission implement "procedures to minimize the burden of submitting a complaint to the Commission concerning violations of [the CAN-SPAM Act], including procedures to allow the electronic submission of complaints to the Commission," as provided by the Act?

> The FTC should set up an easy online form on their web site for the submission of complaints. See our answer to Question (1) above.

H. Study of Effects of the CAN-SPAM Act.

1. The Commission is required to write a report providing a detailed analysis of the effectiveness and enforcement of the provisions of the Act and the need (if any) for the Congress to modify such provisions. What measures of the effectiveness of the Act should the Commission consider?

> The FTC should consider the overall reduction in spam, and the number of violators who have been prosecuted under the CAN-SPAM Act.

2. Are there any developments likely to reach the market in the next two years that are likely to affect the effectiveness of the Act? How should the Commission monitor these developments?

> The FTC should monitor the increasing usage of digitally signed emails as their usage develops and becomes more popular. The FTC should monitor how effective digitally signed emails are in reducing spam.

3. This report must include an analysis and recommendations concerning how to address commercial email that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy provisions that the Federal government could pursue through international negotiations, fora, organizations, or institutions. Given the ease of falsifying header information, how can the Commission determine the extent to which email originates in or is transmitted through or to facilities or computers in other nations? How should the Commission conduct this analysis?

> The ISPs and other entities that report violators to the FTC often employ experts who can easily trace the headers from unsolicited emails. The FTC should work in conjunction with these entities to trace the originations of these emails.

4. This report must include an analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial email that is obscene or pornographic. How should the Commission conduct this analysis?

> The FTC should solicit testimony from recipients of unsolicited pornographic or obscene email.

I. Study of Subject Line Labeling

1. Prior to the enactment of the CAN-SPAM Act, many states required that unsolicited non-adult commercial email have an "ADV" label. How was this provision enforced by the States? What obstacles to enforcement did the States encounter? What, if any, limitations were found in these laws that the Commission should consider addressing in the required report regarding subject line labeling?

> Consumers who use Microsoft Outlook as their email program, and use its "preview pane," see the top part of the body of emails in their inbox, even if they have not double-clicked on an email. If an email does not get filtered directly to their Trash (and many emails slip through filters unfortunately), the consumer

must click on the email then drag-and-drop it to their Trash folder. When they click on the email to do this, they see a "preview" of the top portion of the email. Because of the risk of children seeing these images, we recommend that adult emails include a space at the top 5 inches of their emails that does not contain any adult material.

2. How effective is labeling?

Labeling can be effective if used, since recipients can set up filters in their email programs that send all email with a particular word in its subject line to their trash, so that type of unsolicited email never appears in their inbox.

3. Should the Commission recommend that all unsolicited non-adult commercial email be labeled "ADV "? Why or why not?

No.

4. Would labeling, as part of a regime that includes other technological or law enforcement approaches, be an appropriate and effective tool to help control spam? Why or why not?

No comment.

5. What are the costs and benefits to industry of labeling?

Not known.

6. What are the costs and benefits to consumers of labeling?

Not known.

7. If the Commission recommends that non-adult commercial email have an "ADV" label, should it also recommend that senders be allowed to provide additional explanatory information in the subject line; e.g., "ADV: Automobiles?" Why or why not?

No comment.

J. Regulatory Flexibility Act.

1. What burden to small business does the Act impose in the Act's requirements that certain disclosures be made in commercial electronic mail messages? How, if at all, may the burdens associated with required disclosures be minimized?

As has been stated in prior answers, the burden imposed to small businesses is minimal, since email marketing is generally an electronic automated process, and there are very inexpensive programs available that contain the features the Act requires, such as opt-out links within the emails and a mechanism that puts the advertiser's physical address at the end of each email.

2. Does the Act impose any disparate impact on small businesses? If so, how may this disparate impact be minimized?

We do not believe there is a disparate impact on small businesses, as stated in our answer to Question (1) above.

3. Describe and, where feasible, estimate the number of small entities to which the Act applies.

Unknown.

Additional Comments:
Private, non-binding regulatory organizations (in the nature of TRUSTe) could maintain general "opt-in" lists of consumers who have opted in to receive "all commercial email regarding boats," or "all bulk email regarding politics," for example. We believe that this would be the optimal solution for combating spam. The UK and Australia currently have opt-in systems, which have significantly curtailed the amount of spam, and some states such as California passed opt-in laws, which were pre-empted by the passage of the CAN-SPAM Act.

Very truly yours,

Go Daddy Software, Inc.