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

In the Matter of:	)	
	)	
CAN-SPAM Act Rulemaking	)	Project No. R411008

COMMENTS OF VERIZON[1]

Verizon is a leader in the fight against spam, and strongly supports efforts to stop unsolicited and misleading commercial e-mail. Verizon also believes that legitimate businesses have a right to communicate with their customers, however, and urges the Commission to reject rules that would limit these legitimate business messages. As Congress has recognized, these communications are valuable to both companies and consumers; indeed, if anything, the Commission should consider expanding the category of e-mails that will be deemed "transactional or relationship" and thus outside the scope of the prohibitions on unsolicited e-mails. The Commission's final rules should provide legitimate businesses with a bright-line test for determining whether e-mails will be regulated as "commercial," "transactional or relationship," or "other," so that companies can tailor their behavior to ensure they are complying with the rules. The Commission should also create a "safe harbor" rule, similar to the do-not-call safe harbor rules, so that legitimate businesses with effective controls are not penalized for sending commercial e-mails to persons on do-not-spam lists if they reasonably could have believed the e-mails were non-commercial, or if they have in place normally effective

---

[1] These comments are filed on behalf of Verizon Internet Services Inc. and GTE.Net LLC d/b/a Verizon Internet Solutions (which operate under the trade name Verizon Online), and Verizon's affiliated local exchange carriers and long distance companies (collectively referred to herein as "Verizon"). Some of these companies are service providers subject to regulation under the Communications Act of 1934, as amended, and therefore are subject to the enforcement jurisdiction of the Federal Communications Commission, not the Federal Trade Commission. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699, § 7(b)(10) (2003) ("CAN-SPAM Act").

protections against sending such e-mails. Finally, the Commission should educate consumers both about the types of legitimate e-mails they should continue to expect to receive, and the types of e-mail scams that are prominent.

I. THE COMMISSION SHOULD PROVIDE AN OBJECTIVE, BRIGHT-LINE TEST FOR DETERMINING THE PRIMARY PURPOSE OF AN E-MAIL

The CAN-SPAM Act undoubtedly will be a valuable tool in combating the proliferation of fraudulent and misleading e-mails. However, in adopting the Act, Congress recognized that e-mail is "an extremely important and popular means of communication" for both personal and commercial purposes. CAN-SPAM Act, § 2(A)(1). Recognizing this, the Commission should adopt a clear, bright-line test to assist legitimate businesses in determining whether the Commission will deem the "primary purpose" of an e-mail to be "commercial," "transactional or relationship," or something else. The rules also must reflect the Act's intent not to impinge upon normal, constitutionally protected communications between a business and its customers.

The Commission correctly has proposed to reject tests that would deem the primary purpose of an e-mail to be "commercial" if the e-mail were unsolicited, or if *any* portion of the e-mail contained an advertisement or promotion of a commercial product or service.[2] As the Commission recognized, such rules would be contrary to the plain language of the Act.[3]

---

[2] *See* FTC, Notice of Proposed Rulemaking, Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act, Project No. R411008, 69 Fed. Reg. 50091, at 50099, § II.C.3.c (Aug. 13, 2004) ("Notice").

[3] *See id.*, at 50099, § II.C.3.c (rejecting the argument that all "unsolicited" e-mails be deemed commercial, because "[i]t is clear from the Act that Congress did not intend for the primary purpose of an e-mail message to be determined based on whether a message was unsolicited"); *see also id.* (rejecting proposals to treat an e-mail as commercial if it contained any commercial content, since the "primary purpose" language of the Act "establishes that mere inclusion of any commercial content is not enough by itself to bring an e-mail message within the ambit of the Act's coverage").

Congress expressly recognized the value that e-mail has in commercial transactions.[4] The Act specifically states that the rules regulating commercial e-mail will apply only if the *primary* purpose of the e-mail is commercial. CAN-SPAM Act, § 3(2), § 5(a)(4). It also defined "transactional or relationship" messages between businesses and their customers as falling outside the scope of these prohibitions. *Id.*, § 3(2), § 3(17). But the line between commercial and transactional/relationship limits can be blurred when an email is between two parties with an already existing commercial relationship.

To add clarity to the requirements, the Commission should consider expanding the definition of "transactional or relationship" messages to include e-mails sent as part of a pre-existing relationship between the sender and the recipient.[5] For example, Verizon customer service personnel may send e-mails to customers discussing security alerts regarding phishing scams or an operational update. These communications may also include information about new security products or services that the customer may wish to consider or inform the customer of an upcoming promotion. Such e-mails are a part of normal interactions between a business and its customers, and they benefit both parties. They are not the type of "bulk unsolicited" messages that Congress intended to target. CAN-SPAM Act, § 2(a)(10); *see also* Verizon Advanced NPRM Comments, at 3-5. Expanding the definition of "transactional or relationship

---

[4] *See* CAN-SPAM Act, § II.A (Finding that e-mail is "an extremely important and popular means of communication" that consumers rely upon for personal and "commercial purposes," and that "[i]ts low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce").

[5] *See* Verizon Comments, Advanced Notice of Proposed Rulemaking, Project No. R411008, at 3-5 (FTC, filed April 20, 2004) ("Verizon Advanced NPRM Comments"); Comments of the Internet Commerce Coalition, Advanced Notice of Proposed Rulemaking, Project No. R411008, at 3-4 (FTC, filed April 20, 2004).

messages" as proposed above is within the Commission's authority,[6] and consistent with the goals of the Act.

II. THE COMMISSION SHOULD CLARIFY THAT WHEN E-MAILS CONTAIN ADVERTISEMENTS BY MULTIPLE PARTIES, THE ONLY "SENDER" IS THE ENTITY THAT CAUSES TRANSMISSION OF THE MESSAGE

The rules regulating the sending of commercial e-mails generally regulate activities of the "sender" of the e-mail. *See* CAN-SPAM Act, § 5(a)(4). The Advanced Notice[7] asked whether there would be more than one "sender" if an e-mail contains "ads for four different companies." *See* Advanced Notice, 69 Fed. Reg. at 11781. The proposed rules contained in the further Notice simply adopt the statutory definition of "sender," without clarifying the answer to that question. *See* Notice, 69 Fed. Reg. at 50094, § I.B, n.25.[8] As Verizon explained in comments to the Advanced Notice, the Commission should clarify that normally, there will be deemed only one sender of an e-mail – the party that causes its transmission. *See* Verizon Advanced NPRM Comments, at 6-8.

Under the language of the Act, an entity is not deemed the "sender" of a commercial e-mail message unless it *both* "initiates" the message and is the person whose product or service is being advertised. *See* CAN-SPAM Act § 3(16)(A). Thus, in the Commission's example, none

---

[6] The Commission has the authority to modify the definition of the term "transactional or relationship message" "to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and to accomplish the purpose of [the] Act." Notice, § I.A (quoting 15 U.S.C. 7702(17)(B)).

[7] *Definitions, Implementation and Reporting Requirements Under the CAN-SPAM Act*, Advanced Notice of Proposed Rulemaking, Project No. R411008, 69 Fed. Reg. 11776 (Mar. 11, 2004) ("Advanced Notice").

[8] The Act defines the term "sender" as a "person who initiates such a [commercial electronic mail] message and whose product, service, or Internet web site is advertised or prompted by the message." *See* CAN-SPAM Act, § 3(16)(A). To "initiate" a message means "to originate or transmit such message or to procure the origination or transmission of such message ...." *Id.* § 3(9). To "procure" means "intentionally to pay or provide other consideration to, or induce, another person to initiate such message on one's behalf." *Id.* § 3(12). Ordinarily, only one entity can be the "sender" of an e-mail.

of the four companies would be the sender, unless it also was the initiator of the e-mail under the language of § 3(9).

The plain language of the Act supports defining the sender as a single entity. Indeed, Congress expressly defined "sender" as "a person." *See* CAN-SPAM Act, § 3(16)(A). If Congress intended for the "sender" of an individual e-mail to be multiple entities, then it would have defined "sender" as "any person" or "persons" who initiate a commercial electronic mail message, or expressly stated that the definition was intended to cover multiple persons. *See* CAN-SPAM Act, § 3(9)(defining "initiate" and setting forth clear direction as to the inclusion of multiple persons: "For purposes of this paragraph, more than one person may be considered to have initiated a message").

Moreover, a contrary interpretation would cripple common (and entirely permissible) forms of advertising. For example, if all advertisers included in an e-mail were considered "senders," and a newspaper transmits an e-mail that contains an advertisement for Verizon, Verizon would be considered a "sender" of this e-mail. Yet, it would be virtually impossible for Verizon to determine to whom the newspaper, or any other advertiser with which Verizon does business, will send such e-mails. Although the Commission partially proposes to address this problem by deeming newspaper and newsletter transmittals not to be primarily "commercial" e-mails,[9] there exists subjectivity in interpretation of those rules. *See* Section III, *infra*. Thus, advertisers who do not transmit e-mails would face the choice of forgoing all such advertising in third party e-mail sources, which raises First Amendment concerns, or risk being later found to have violated the Act. *See* Verizon Advanced NPRM Comments, at 6-8.

---

[9] *See* Advanced Notice, 69 Fed. Reg. at 50099-50100, § 3(C)(3).

In addition, the Commission should confirm that, in the context of a bundled service offering, only the line of business that transmits the commercial e-mail is considered the "sender." This is consistent with the plain language of the Act, which states that "[i]f an entity operates though separate lines of business or divisions and holds itself out to the recipient throughout the message as that particular line or business or division ..., then the line of business or division shall be treated as the sender of such message for purposes of this Act." *See* CAN-SPAM Act, § 3(16)(B).

Of course, the Commission should not allow outlaw spammers to use misleading practices to avoid penalties under the Act by claiming they are not the true "senders" of the message. However, this is best accomplished by making clear rules that prohibit false and misleading headers or "sham" senders designed to evade the Act's requirements.

III. THE COMMISSION SHOULD CREATE A "SAFE HARBOR" RULE SO THAT LEGITIMATE BUSINESSES WITH EFFECTIVE CONTROLS ARE NOT PENALIZED FOR INADVERTENTLY SENDING COMMERCIAL E-MAILS TO PERSONS ON DO-NOT-SPAM LISTS

Even with the clarifications contained in the Commission's proposed rules, several ambiguities will still exist. For example, the proposed rules for determining the "primary purpose" of an e-mail focus in several instances on what a "recipient reasonably interpreting" the message would believe to be the primary purpose. *See, e.g.*, Notice, 69 Fed. Reg. at 50106, § IX, proposed rule 316.3(a)(3). A subjective test of this sort creates ambiguity in compliance and enforcement as reasonable minds may differ on what they interpret to be the "primary purpose" of an e-mail. If the Commission retains this subjective standard, it should also adopt a rule providing that companies that undertake a good-faith effort to comply with the rules, but have adopted interpretations with which the Commission later disagrees, should not be penalized for inadvertently sending commercial e-mails to people on the do-not-spam list. In addition, if the

Commission later determines that there can be multiple "senders" of commercial e-mails (*see* Section II, *supra*), entities should not be punished for problems resulting from errors in coordinating the do-not-spam lists of multiple parties.

More specifically, the Commission should adopt rules, similar to those enacted in connection with the do-not-call regulations, to ensure that businesses which have adopted an effective compliance program and are undertaking a good-faith effort to comply with the rules are not penalized if the Commission later determines they sent a commercial e-mail to someone on the do-not-spam list. Such rules should state that companies will not be penalized for such e-mails if they have established written procedures to comply with the Act, trained personnel in the compliance procedures, and employed generally effective methods to prevent unsolicited, commercial e-mail messages to customers who have opted out of receiving such messages.[10]

The CAN-SPAM Act already states that companies will not fail to satisfy the Act's requirements based on technical problems that lead to a temporary inability to process opt-out messages.[11] This reflects a Congressional recognition that companies that employ generally effective compliance programs should not be penalized for temporary problems with the systems. The Act also grants the Commission authority to modify the ten-business-day period in which businesses have to comply with opt-out requests, which allows the Commission to adopt the safe harbor rules proposed above.[12] Modifying the rules to include a safe-harbor provision similar to the one contained in the do-not-call rules will encourage businesses to adopt effective

---

10 *See, e.g.,* 16 C.F.R. § 310.4(b)(3) (similar safe harbor adopted for do-not-call rules).

11 *See* CAN-SPAM Act, § 5(a)(3), 15 U.S.C. § 7704(a)(3)(C).

12 *See* CAN-SPAM Act, § 5(c)(1)(A)-(C), 15 U.S.C. § 7704(c)(1)(A)-(C)

programs to comply with the Act, and ensure that Commission resources are focused on e-mail scammers, not inadvertent violations by legitimate businesses.

IV. THE COMMISSION SHOULD EDUCATE CONSUMERS ABOUT PERMISSIBLE E-MAILS, AS WELL AS POTENTIAL SCAMS

Regardless of the rules that the Commission adopts, many consumers will remain confused about the nature of protections provided by the CAN-SPAM Act. When the Commission announces the final rules, it should use the opportunity to identify forums available to educate consumers about how to distinguish between the legitimate e-mails they may continue to receive from businesses and those that violate the Act. In addition, the Commission should use this opportunity further to educate consumers about the many email-based scams that unscrupulous emailers use every day to commit fraud and other crimes on the Internet.

One area of likely consumer confusion is recognizing the difference between "commercial electronic mail messages" and the standards that apply to them, and e-mails that have a primary purpose that is "transactional or relationship" or otherwise not "commercial." Adopting the "existing business relationship" rule and providing a clear explanation about the requirements for permissible commercial and transactional relationship emails, as well as advice for "unsubscribing" to commercial e-mails, will both instill a greater confidence in the law's effectiveness, as well as limit the filing of unwarranted complaints that are based on a misunderstanding of the law, rather than any violation by the e-mail sender.

The Commission also should use this opportunity to alert consumers to the types of e-mail scams they may face from unscrupulous scammers, particularly when the scammers falsely purport to act on behalf of legitimate businesses. Such scams undermine consumer confidence in e-mail communications and seriously impair the credibility or the businesses whose names or websites are falsified. One common and particularly harmful scam, as the Commission is well

aware, involves "phishing." In phishing scams the scammer poses as a known, legitimate business in order to trick consumers into submitting confidential information such as account numbers, passwords, credit card information, or financial data.[13] The scammer then uses this information to steal the identity of the unwitting consumer or to commit other acts of fraud. Verizon has warned consumers about such scams,[14] and other companies are doing the same. However, the nature of the scams means that these warnings often can come only after legitimate businesses and their consumers already have become victims, because the scam is not known to the affected business until it is already out on the Internet.

The Commission should encourage businesses that operate online to educate their customers about how they will request personal information (and how to avoid the scammers). The Commission should also lead a nationwide educational campaign to warn consumers to be wary of unsolicited e-mails that ask them to provide personal or financial information online, even if the e-mails appear to come from legitimate companies with which they do business. When there is any doubt, customers should be directed not to respond to the e-mail until they have independently verified the e-mail by calling the business' customer care center or similar trusted source. Any educational effort should also remind consumers of existing online resources, sponsored by the Commission or reputable third party organizations, where they can go for information or to report suspected scams.

---

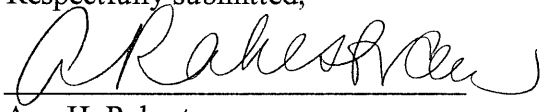
[13] *See* Anti-Phishing Working Group Website, *available at* www.antiphishing.org (describing phishing, and identifying scams that have plagued various businesses).

[14] *See, e.g.*, News Release, "Verizon Warns Consumers: Beware of On-Line 'Phishing' Scam," (April 21, 2004) (attached as Exhibit A).

V. CONCLUSION

For all the foregoing reasons, the Commission should set clear, bright line rules that give guidance to businesses about permissible behavior, and should educate consumers about legitimate e-mails as well as potential scams.

Respectfully submitted,



Ann H. Rakestraw
Edward Shakin

1515 North Courthouse Road
Suite 500
Arlington, VA 22201
(703) 351-3174

Thomas M. Dailey
Verizon Legal Department
1880 Campus Commons Drive
Reston, VA 20191
(703) 295-4285

Attorneys for Verizon

Michael E. Glover
Of Counsel

September 13, 2004

Verizon Warns Consumers: Beware of On-Line 'Phishing' Scam

Newest Scam Involves Attempts to Collect Credit Card Numbers And Other Sensitive Information Through Fake Web Site

April 21, 2004

Media contacts:
Mark Marchand, 518-396-1080
Bobbi Henson, 972-718-2225

NEW YORK - Verizon customers should be aware of a new wave of scams that try to pry personal information from consumers, which can lead to identity theft and other crimes.

The newest scam involves an authentic-looking e-mail from someone posing as a Verizon representative. The e-mail asks Verizon customers to update their personal billing information - such as credit-card or social security numbers -- and directs them to a Web site that is designed to look like a Verizon Web site. The phony Web site is actually operated by the scammers. The e-mail falsely warns the consumer that in order to continue receiving Verizon services, he or she must visit the fake Web site and avoid paying a "processing" fee by updating personal and account information. Verizon does not do business in this fashion, nor does the company charge consumers to update their information.

This latest wave of scams directing consumers to phony Web sites -- known as "phishing" -- has targeted a number of other industries and companies over the past year.

"Consumers should be wary of any e-mail or phone call asking that they reveal credit card or other sensitive information," said Jim Trainor, Verizon vice president-security. "Verizon customers can call us via the phone number on their bills, or they can visit our real home page - www.verizon.com or our Verizon Online home page, www.verizon.net if they have any suspicions about an e-mail, phone call or letter.

"The bottom line is there are many scam artists out there willing to do anything to trick consumers into giving up personal information or money," Trainor said. "Take the extra step and ask a question or call us if you have any doubt at all."

Other Scams Also Threaten Consumers

In issuing its warning about "phishing," Verizon also made consumers aware of several other scams:

- **Pop-up ad questions -** This is another relatively new issue. Verizon Online customers and other Internet access-provider consumers should carefully scrutinize what they agree to when they click on Web site pop-up ads and are asked to respond to a series of questions. In some cases, dial-up consumers who clicked "yes" to several pop-up ad questions have found their computer modems re-programmed to make expensive long-distance calls. Pop-up ads are a legitimate way of advertising on Web sites - but

consumers should read the fine print and make sure they know what they're agreeing to when they click the "yes" button in response to questions in such an ad. It could be a costly mistake.

- **Collect calls from unknown callers -** This is a relatively old scam that has been surfacing again recently in several areas of the country. Under this scam, a caller - sometimes an inmate from a correctional facility - calls people through an operator and asks them to accept a collect call by convincing them someone they know is in jail. In the relatively rare circumstances where the called party accepts the call and associated charges, the caller hangs up and the consumer is stuck with a charge for the collect call. In some cases, the scammer stays on and tries to convince the consumer to program his or her incoming calls to be forwarded to another destination. In some cases, this can then lead to the scam artist making additional long-distance calls that are then charged to the unsuspecting consumer. The bottom line is: Never accept a collect call unless it is from someone you know or from someone whose identity you can verify.

- **Callers or letter-writers masquerading as Verizon employees -** Verizon has seen many different variations on this scam over the years, but the overall purpose remains the same: trick an unsuspecting consumer into giving up personal information that can be used to commit identity theft or other crimes. In one variation of this scenario, the caller identifies himself as a Verizon representative and says the consumer in his or her most recent payment to Verizon paid more than the balance due. In order to process a refund check, the scammer says, the customer should provide some personal information that can be used to speed the processing of the check. Again, Verizon does not do business in this fashion. Any overpayments are automatically credited to the next month's bill - without Verizon having to contact the consumer or the customer having to call Verizon. In general, if you receive such a phone call, ask the caller for a callback number or simply hang up and call Verizon via the business office phone number listed on your bill.

"By simply taking that one extra minute to consider whether something is a legitimate communication from a trusted source, consumers can save themselves both a lot of headaches and maybe a lot of money," Trainor said. "Usually just one extra question or taking a minute to check out an e-mail or online ad is enough for a consumer to stop the scammers dead in their tracks."

A Fortune 20 company, Verizon Communications (NYSE:VZ) is one of the world's leading providers of communications services, with approximately $68 billion in annual revenues. Verizon companies are the largest providers of wireline and wireless communications in the United States. Verizon is also the largest directory publisher in the world, as measured by directory titles and circulation. Verizon's international presence includes wireline and wireless communications operations and investments, primarily in the Americas and Europe. For more information, visit www.verizon.com.

####