Prepared Statement of the Federal Trade Commission on

"Unsolicited Commercial Email"

Before the
Committee on Energy and Commerce
Subcommittee on Commerce, Trade and Consumer Protection
Subcommittee on Telecommunications and the Internet
U.S. House of Representatives

Washington, D.C.
July 9, 2003

Mr. Chairman, the Federal Trade Commission appreciates this opportunity to provide information to the Committee on the agency's efforts to address the problems that result from bulk unsolicited commercial email ("spam"). This statement discusses the Commission's law enforcement efforts against spam, describes our efforts to educate consumers and businesses about the problem of spam, and focuses particularly on the Commission's recent Spam Forum and several studies on the subject that the Commission's staff has undertaken in recent months. It also discusses legislative ideas to enhance the Commission's effectiveness in fighting spam.[(1)]

As the federal government's principal consumer protection agency, the FTC's mission is to promote the efficient functioning of the marketplace by acting against unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. To fulfill this mission, the Commission enforces the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(2)] Online commerce, including unsolicited commercial email, falls within the scope of this statutory mandate.

The problems caused by unsolicited commercial email go well beyond the annoyance spam causes to the public. Indeed, these problems include the fraudulent and deceptive content of most spam messages, the offensive content of many spam messages, the sheer volume of spam being sent across the Internet, and the security issues raised because spam can be used to disrupt service or as a vehicle for sending viruses.

FTC Spam Forum

Building upon our research, education, and law enforcement efforts, the FTC held a three-day public forum from April 30 to May 2, 2003 on spam email. This was a wide-ranging public examination of spam from all viewpoints. The Commission convened this event for two principal reasons. First, spam is frequently discussed, but facts about how it works, its origins, what incentives drive it, and so on, are not widely known. The Commission anticipated that the Forum would generate an exchange of useful information about spam to help inform the public policy debate. This could help the Commission determine what it might do to more effectively fulfill our consumer protection mission in this area. Second, the Commission sought to act as a potential catalyst for solutions to the spam problem. Through the Forum, the Commission brought to the table representatives from as many sides of the issue as possible to explore and encourage progress toward potential solutions to the detrimental effects of spam.

Virtually all of the panelists at the Commission's recent Spam Forum opined that the volume of unsolicited email is increasing exponentially and that we are at a "tipping point," requiring some action to avert deep erosion of public confidence that could hinder, or even destroy, email as a tool for communication and online commerce. In other words, as some have expressed it, spam is "killing the killer app." The consensus of all participants in the workshop was that a solution to the spam problem is critically important, but cannot be found overnight. There is no quick or simple "silver bullet." Rather, solutions must be pursued from many directions - technological, legal, and consumer action. The Forum explored and helped to suggest paths to follow toward solving the spam problems. Such solutions will depend on cooperative efforts between government and the private sector.

Law Enforcement

The Forum is only the most recent example of the FTC's role as convener, facilitator, and catalyst to encourage that activity. But the Commission also plays another important role - that of law enforcer. For example, the Commission has pursued a vigorous law enforcement program against deceptive spam, and to date has brought 54 cases in

which spam was an integral element of the alleged overall deceptive or unfair practice. Most of those cases focused on the deceptive content of the spam message, alleging that the various defendants violated Section 5 of the FTC Act through misrepresentations in the body of the message.[3] More recently, the Commission has expanded the scope of its allegations to encompass not just the content of the spam but also the *manner* in which the spam is sent. Thus, *FTC v. G. M. Funding*[4] and *FTC v. Brian Westby*[5] allege (1) that email "spoofing" is an unfair practice,[6] and (2) that failure to honor a "remove me" representation is a deceptive practice. In each of these cases, the defendants' email removal mechanisms did not work and consumers' emailed attempts to remove themselves from defendants' distribution lists were returned as undeliverable.

Westby is also the first FTC case to allege that a misleading subject line is deceptive because it tricks consumers into opening messages they otherwise would not open. In other cases, the Commission has alleged that the defendants falsely represented that subscribing to defendants' service could stop spam from other sources[7] or that purchasers of a spamming business opportunity could make substantial profits.[8] Accordingly, these law enforcement actions demonstrate that the Commission has attacked and will continue to attack deception and unfairness in every aspect of spam.

In May 2003, the FTC joined the Securities and Exchange Commission, United States Postal Inspection Service, three United States Attorneys, four state attorneys general, and two state regulatory agencies to file 45 criminal and civil law enforcement actions against Internet scams.[9] As part of this sweep, the FTC brought five federal court actions alleging the deceptive use of spam. In one case, the defendants allegedly used spam with deceptive representations that the email came from well-known entities, such as Hotmail or MSN, to market a "100% Legal and Legitimate"work-at-home opportunity. Although the spam promised consumers they could earn as much as $1,500 a week stuffing envelopes supplied by the defendants, consumers ended up paying $50 for a set of instructions on how to market a deceptive credit-repair manual.[10] In another case, the defendant allegedly used spam to make false and deceptive income claims for a chain-letter scheme dubbed "Instant Internet Empire."[11] A third complaint alleged that defendants used deceptive spam to market an advance-fee credit card scam.[12] In each of these cases, the FTC was able to obtain preliminary injunctive relief and to shut down the operations.[13]

In addition to the law enforcement actions, in this sweep, the FTC and 17 other federal and state consumer protection and law enforcement agencies initiated an effort to reduce deceptive spam by urging organizations to close "open relays."[14] Fifty law enforcers from 17 agencies identified 1,000 potential open relays, 90 percent of which were in 16 countries: U.S., China, Korea, Japan, Italy, Poland, Brazil, Germany, Taiwan, Mexico, Great Britain, Chile, France, Argentina, India, Spain, and Canada. The agencies drafted a letter, translated into 11 languages and signed by 14 different U.S. and international agencies, urging the organizations to close their open relays to help reduce spam.

Approaches to Solving the Spam Problem

Solutions to the problems posed by spam will not be quick or easy; nor is one single approach likely to provide a cure. Instead, a balanced blend of technological fixes, business and consumer education, legislation, and enforcement will be required. Technology that empowers consumers in an easy-to-use manner is essential to getting immediate results for a number of frustrated end-users. Any solution to the problems caused by spam should contain the following elements:

1. Enhanced enforcement tools to combat fraud and deception;

2. Support for the development and deployment of technological tools to fight spam;

3. Enhanced business and consumer education; and

4. The study of business methods to reduce the volume of spam.

The Commission's legislative recommendations, discussed below, would enhance the agency's enforcement tools for fighting spam. In addition, the FTC will continue vigorous law enforcement and reach out to key law enforcement partners through the creation of a Federal/State Spam Task Force to strengthen cooperation with criminal authorities. The Task Force can help to overcome some of the obstacles that spam prosecutions present to law enforcement authorities.

The Commission's experience shows that the primary law enforcement challenges are to identify and locate the targeted spammer. Of course, finding the wrongdoers is an important aspect of all law enforcement actions, but in spam cases it is a particularly daunting task. Spammers can easily hide their identity, forge the electronic path of their email messages, or send their messages from anywhere in the world to anyone in the world. Tracking down a targeted spammer typically requires an unusually large commitment of staff time and resources, and rarely can it be known in advance whether the target's operation is large enough or injurious enough to consumers to justify the resource commitment. For example, in some instances, state agencies spent considerable front-end investigative resources to find a spammer, only to discover at the back end that the spammer was located outside the state's jurisdiction. State and federal agencies recognize the need to share the information obtained in investigations, so that the agency best placed to pursue the spammer can do so more efficiently and quickly. The Task Force should facilitate this process. Further, it can serve as a forum to apprise participating agencies of the latest spamming technology, spammer ploys, and investigational techniques.

Through the Task Force, the FTC will reach out not only to its civil law enforcement counterparts on the state level, but also to federal and state criminal authorities. Although few criminal prosecutions involving spam have occurred to date,[(15)] criminal prosecution may well be appropriate for the most egregious conduct. The FTC and its partners in criminal law enforcement agencies continue to work to assess existing barriers to successful criminal prosecutions. The FTC will explore whether increased coordination and cooperation with criminal authorities would be helpful in stopping the worst actors.

Improved technological tools will be an essential part of any solution as well. A great deal of spam is virtually untraceable, and an increasing amount crosses international boundaries. Panelists estimated that from 50 percent to 90 percent of email is untraceable, either because it contains falsified routing information or because it comes through open relays or open proxies.[(16)] Because so much spam is untraceable, technological development will be an important element in solving spam problems. To this end, the FTC will continue to encourage industry to meet this challenge.

Action by consumers and businesses who may receive spam will be a crucial part of any solution to the problems caused by spam. A key component of the FTC's efforts against spam is educating consumers and businesses about the steps they can take to decrease the amount of spam they receive. The FTC's educational materials provide guidance on how to decrease the chances of having an email address harvested and used for spam, and suggest several other steps to decrease the amount of spam an address may receive. The FTC's educational materials on spam are available on the FTC website.[(17)]

Finally, several initiatives for reducing the overwhelming volume of spam were discussed at the FTC's Spam Forum. At this point, questions remain about the feasibility and likely effectiveness of these initiatives. The FTC intends to continue its active role as catalyst and monitor of technological innovation and business approaches to addressing spam.

Legislation to Enhance the FTC's Effectiveness To Fight Fraudulent Spam

Effective spam legislation must address the following three issues: First, legislation must address how to find the person sending the spam messages. Although we believe that technological changes will most effectively resolve this issue, we have proposed several procedural legislative changes that can provide some assistance in our law enforcement investigations. Second, legislation must deal with how to deter the person sending the spam messages. As discussed below, the Commission believes that civil penalties, and possibly criminal sanctions, would help address this issue. Finally, legislation must determine what standards will govern non-deceptive, unsolicited commercial email. The Commission believes that the appropriate standards would include clear identification of the sender of a message and by empowering consumers to end the flow of messages that they do not wish to receive.

It would be useful to have additional legislative authority, addressing both procedural and substantive issues, that would enhance the agency's effectiveness in fighting fraud and deception. The procedural legislative proposals would improve the FTC's ability to investigate possible spam targets, and the substantive legislative proposals would improve the agency's ability to sue these targets successfully, including increased penalties for violations.

Procedural Proposals

The FTC's law enforcement experience shows that the path from a fraudulent spammer to a consumer's in-box frequently crosses at least one international border and often several. Thus, fraudulent spam exemplifies the growing

problem of cross-border fraud. Two of the provisions in the Commission's proposed cross-border fraud legislation, discussed at the recent reauthorization testimony, would be particularly helpful to enable the FTC to investigate deceptive spammers more effectively and work better with international law enforcement partners.

First, the Commission has asked Congress to amend the FTC Act to allow FTC attorneys to seek a court order requiring a recipient of a Civil Investigative Demand ("CID") to maintain the confidentiality of the CID for a limited period of time. Several third parties have told us that they will provide notice to the target before they will share information with us, sometimes because they believe notice may be required and sometimes even if such notice clearly is not required by law.

Second, the Commission asked Congress to amend the FTC Act so that FTC attorneys may seek a court order temporarily delaying notice to an investigative target of a CID issued to a third party in specified circumstances. Currently, the Right to Financial Privacy Act ("RFPA") and the Electronic Communications Privacy Act ("ECPA") require such notice.

The FTC's experience is that fraud targets often destroy documents or hide assets when they receive notice of FTC investigations. Although the RFPA and ECPA provide a mechanism for delaying notice, the FTC's ability to investigate would be improved by tailoring the bases for a court-ordered delay more specifically to the types of difficulties the FTC encounters, such as transfers of assets offshore. In addition, it is unclear whether FTC attorneys can file such applications, or whether the Commission must seek the assistance of the Department of Justice. Explicit authority for the FTC, by its own attorneys, to file such applications would streamline the agency's investigations of purveyors of fraud on the Internet, ensuring that the agency can rapidly pursue investigative leads.

Other legislative proposals would enhance the FTC's ability to track deceptive spammers. First, we request that the ECPA be clarified to allow the FTC to obtain complaints received by an ISP regarding a subscriber. Frequently, spam recipients complain first to their ISPs, and access to the information in those complaints would help the agency to determine the nature and scope of the spammer's potential law violations, as well as lead the agency to potential witnesses.

Second, we request that the scope of the ECPA be clarified so that a hacker or a spammer who has hijacked a bona fide customer's email account is deemed a mere unauthorized user of the account, not a "customer" entitled to the protections afforded by the statute. Because of the lack of a statutory definition for the term "customer," the current statutory language may cover hackers or spammers. Such a reading of the ECPA would permit the FTC to obtain only limited information about a hacker or spammer targeted in an investigation. Clarification to eliminate such a reading would be very helpful.

Third, we request that the ECPA be amended to include the term "discovery subpoena" in the language of 18 U.S.C. § 2703. This change is particularly important because a district court has ruled that the FTC staff cannot obtain information under the ECPA from ISPs during the discovery phase of a case, which limits the agency's ability to investigate spammers.[(18)]

Substantive Proposals

Substantive legislative changes also could aid in the FTC's law enforcement efforts against spam. Although Section 5 of the FTC Act provides a firm footing for spam prosecutions, additional law enforcement tools could make more explicit the boundaries of legal and illegal conduct, and they could enhance the sanctions that the agency can impose on violators. As the Commission recently testified at its Reauthorization hearing before this Committee, the Telemarketing and Consumer Fraud and Abuse Prevention Act ("TCFAPA"), 15 U.S.C. §§ 6101-6108, provides a model for addressing unsolicited commercial e-mail. Amendments to the TCFAPA would authorize the FTC to adopt rules addressing deceptive and abusive[(19)] practices with respect to the sending of unsolicited commercial e-mail. Approaching spam through this statutory model would provide the market with direction, but would do so within a framework that could change as the problems evolve. Regardless of the statutory approach taken, however, the Commission believes that the following elements are important.

First, any legislation should give the FTC some authority via rulemaking to address deceptive practices relating to spam. Agency rules could be adapted to new changes in technology without hindering technological innovation, thus providing the market with direction, but doing so within a framework that could change as the problems evolve. Whether addressed through the legislation itself or through rulemaking, unlawful practices that should be prohibited include: using false header or routing information; using false representations in the "subject" line; using false claims

that an unsolicited commercial email message was solicited; using false representations that an opt-out request will be honored; sending any recipient a commercial email message after such recipient has requested not to receive such commercial email messages; failing to provide a reasonable means to "opt out" of receiving future email messages; and sending commercial email to an address obtained through harvesting or a dictionary attack. Morever, any statute also should prohibit assisting and facilitating any of the above, *i.e.*, providing substantial assistance to another party engaged in any violation knowing or consciously avoiding knowing that such party is engaged in such violation.

Second, any legislation should embody the same standard of liability that is embodied in Section 5 of the FTC Act, without a general requirement to show intent or knowledge. Imposition of intent or knowledge requirements as a precondition of liability would actually make the FTC's ability to enforce the specific anti-spam statute more restrictive than the agency's existing authority under Section 5 to attack spam and would unnecessarily complicate enforcement.

Third, any statute or rule issued under the statute should be enforceable by the FTC like other FTC rules. This entails actions in federal district court, authority to seek preliminary and permanent injunctions and other equitable relief, and liability for civil penalties of up to $11,000 per violation. (The amount of civil penalties is governed by statutory factors, such as ability to pay, previous history of such conduct, egregiousness of the conduct, etc.).

Fourth, any legislation should authorize states to enforce the statute or FTC rule in federal court. A state enforcement mechanism has proven successful in other areas of consumer protection, such as telemarketing, and would make the states more capable law enforcement partners with the Commission.

Finally, any statute should seek to assure consistency between state and federal laws. The scope of the Internet and of email communication is global, transcending national boundaries. Congress should seek to minimize artificial barriers that would break up this market.

Additionally, the criminalization of false header and routing information should be explored. The FTC staff has been discussing with criminal authorities the likely effect of a specific statute that criminalized this conduct. At this time, the FTC has no recommendations on whether changes in the criminal code are necessary or appropriate.[(20)]

Admittedly, we recognize that these legal steps alone will not solve the growing spam problem. Nor is it clear what impact these steps will have on some of the other problems associated with spam (*e.g.*, volume and security). These issues may need to be addressed separately. Nevertheless, the FTC believes that legislation, such as that described above, would provide more effective investigative and enforcement tools and would enhance the FTC's continuing law enforcement efforts.

Conclusion

Email provides enormous benefits to consumers and businesses as a communication tool. The increasing volume of spam to ISPs, to businesses, and to consumers, coupled with the widespread use of spam as a means to perpetrate fraud and deception, put these benefits at serious risk. The Commission looks forward to continuing its research, education, and law enforcement efforts to protect consumers and businesses from the current onslaught of unwanted messages.

The Commission appreciates this opportunity to describe its efforts to address the problem of spam.

Endnotes:

1. The views expressed in this statement represent the views of the Commission. My oral statements and responses to any questions you may have represent my own views, and not necessarily the views of the Commission or any other Commissioner.

2. The FTC has limited or no jurisdiction over specified types of entities and activities. These include banks, savings associations, and federal credit unions; regulated common carriers; air carriers; non-retail sales of livestock and meat products under the Packers and Stockyards Act; certain activities of nonprofit corporations; and the business of insurance. *See, e.g.*, 15 U.S.C. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. §§ 1011 *et seq.* (McCarran-Ferguson Act).

3. *E.g., FTC v. 30 Minute Mortgage, Inc*., No. 03-60021 (S.D. Fla. filed Jan. 9, 2003)

4. No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002)

5. No. 032-3030 (N.D. Ill. filed Apr. 15, 2003).

6. "Spoofing" involves forging the "from" or "reply to" lines in an email to make it appear that the email was sent from an innocent third-party. The third party then receives bounced-back undeliverable messages and angry "do not spam me" complaints.

7. *FTC v. NetSource One*, No. 022-3077 (W.D. Ky. filed Nov. 2, 2002).

8. *FTC v. Cyber Data,* No. CV 02-2120 LKK (E.D. Cal. filed Oct. 2002); *FTC v. Internet Specialists*, No. 302 CV 01722 RNC (D.Conn. filed Oct. 2002)

9. FTC Press Release, *Law Enforcement Posse Tackles Internet Scammers, Deceptive Spammers* (May 15, 2003), *available at* <http://www.ftc.gov/opa/2003/05/swnetforce.htm >.

10. *FTC v. Patrick Cella et al.*, No. CV-03-3202 (C.D. Cal.) (complaint filed May 7, 2003), *available at* <http://www.ftc.gov/os/2003/05/patrickcellacmp.pdf >.

11. *FTC v. K4 Global Publishing, Inc. et al.*, No. 5:03-CV0140-3 (M.D. Ga.) (complaint filed May 7, 2003), *available at* <http://www.ftc.gov/os/2003/05/k4globalcmp.pdf >.

12. *FTC v. Clickformail.com, Inc.*, No. 03-C-3033 (N.D. Ill.) (complaint filed May 7, 2003), *available at* <http://www.ftc.gov/os/2003/05/clickformailcmp.pdf >.

13. In the other two cases, the FTC filed stipulated final orders prohibiting future participation in email chain letters. *FTC v. Evans*, No. 4:03CV178 (E.D. Tex.) (complaint and stipulated final judgment filed May 9, 2003); *FTC v. Benson*, No. 03CV0951 (N.D. Tex.) (complaint and stipulated final judgment filed May 6, 2003). Both are available at <http://www.ftc.gov/opa/2003/05/swnetforce.htm >.

14. An open relay is an email server that is configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties, which allows spammers to route their email through servers of other organizations, disguising the origin of the email. An open proxy is a mis-configured proxy server through which an unauthorized user can connect to the Internet. Spammers use open proxies to send spam from the computer network's ISP or to find an open relay. *See* FTC Facts for Business, *Open Relays - Close the Door on Spam* (May 2003), *available at* <http://www.ftc.gov/bcp/conline/pubs/buspubs/openrelay.htm>.

15. *See, e.g., United States v. Barrero*, Crim. No. 03-30102-01 DRH (S.D. Ill. 2003) (guilty plea entered May 12, 2003). Like the related case, *FTC v. Stuffingforcash.com Corp.,* Civ. Action No. 02 C 5022 (N.D. Ill. Jan. 30, 2003), the allegations in this criminal prosecution were based on fraud in the seller's underlying business transaction.

16. Brightmail recently estimated that 90% of the email that it analyzed was untraceable. Two panelists at the Commission's Spam Forum estimated that 40% to 50% of the email it analyzed came through open relays or open proxies, making it virtually impossible to trace. Even when spam cannot be traced technologically, however, enforcement is possible. In some cases, the FTC has followed the money trail to pursue sellers who use spam. The process is resource intensive, frequently requiring a series of ten or more CIDs to identify and locate the seller in the real world. Moreover, the seller and the spammer often are different entities. In numerous instances, FTC staff cannot initially identify or locate the spammer and can only identify and locate the seller. In many of those cases, in the course of prosecuting the seller, staff has, through discovery, sought information about the spammer who actually sent the messages. This, too, involves resource-intensive discovery efforts.

17. *See* http://www.ftc.gov/spam.

18. *See FTC v. Netscape Comm. Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000).

19. The FTC has determined, in the Statement of Basis and Purpose for the Amended TSR, that the undefined term "abusive" used in the legislation authorizing that Rule will be interpreted to encompass "unfairness." 68 Fed. Reg. 4580, 4614 (2003).

20. Any legislation that criminalizes certain types of spam activities should not negatively impact the FTC's existing Section 5 authority or impose new standards of proof, scienter, or evidence for civil enforcement cases.