PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

"UNSOLICITED COMMERCIAL EMAIL"

Before the

COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

U.S. SENATE

Washington, D.C.

May 21, 2003

Mr. Chairman, the Federal Trade Commission appreciates this opportunity to provide information to the Committee on the FTC's efforts to address the problems that result from bulk unsolicited commercial email. 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.[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] Commerce on the Internet, including unsolicited commercial email, falls within the scope of this statutory mandate.

---

[1] The views expressed in this statement represent the views of the Commission. Commissioners' oral statements and responses to any questions you may have represent their 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).

Unsolicited commercial email ("UCE" or "spam") is any commercial electronic mail message that is sent – typically in bulk – to consumers without the consumers' prior request or consent. The extreme speed, anonymity and negligible cost of sending spam differentiate it from other forms of unsolicited marketing, such as direct mail or telemarketing. Those marketing techniques, unlike spam, impose costs on marketers that limit their use.

There are two basic problems with spam. First, deception and fraud appear to characterize the vast majority of spam. Indeed, spam appears to be the vehicle of choice for many fraudulent and deceptive marketers. Second, a serious Internet infrastructure problem flows from the sheer volume of spam that is now being sent. Spam, even if not deceptive, may lead to significant disruptions and inefficiencies in Internet services, and may constitute a significant problem for consumers and businesses using the Internet. In addition, spam can spread viruses that wreck havoc for computer users. These problems together pose a threat to consumers' confidence in the Internet as a medium for electronic commerce.

Virtually all of the panelists at the Commission's recent Spam Forum, described in more detail below, 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 in email that could hinder, or even destroy, it as a tool for communication and online commerce. In other words, as some have expressed it, spam is "killing the killer ap." 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 helped to suggest paths to follow toward solutions to the spam problems. These solutions will depend on cooperative efforts between government and the private sector. In fact, 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.

The Commission has pursued a vigorous law enforcement program against deceptive spam, and to date has brought 53 cases in which spam was an integral element of the alleged overall deceptive or unfair practice.[3] 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.[4] 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*,[5] and *F.T.C.v. Brain Westby*[6] allege (1) that email "spoofing" is an unfair practice,[7] and (2) that failure to honor a "remove me" representation is a deceptive practice. In these cases, the

---

[3] A summary listing of these cases is attached as Appendix A.

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

[5] No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002)

[6] No. 032-3030 (N.D. Ill. filed Apr. 15, 2003).

[7] "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.

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[8] or that purchasers of a spamming business opportunity could make substantial profits.[9] Thus, through our law enforcement actions the Commission has attacked and will continue to attack deception and unfairness in every aspect of spam.

Experience in these cases 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.

---

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

[9] *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)

To complement its law enforcement efforts, the Commission endeavors to educate consumers and businesses on ways they can reduce the amount of unwanted spam they receive, and about particular types of scams commonly disseminated through spam, such as illegal chain letters and "Nigerian" scams.[10] These materials are available on the FTC's spam website, www.ftc.gov/spam.

Another aspect of the Commission's approach to spam is to investigate and research the problems it poses to understand them better. Through this research, the Commission can refine and better focus its law enforcement and consumer and business education efforts.

Studying the Spam Problem

The Commission has engaged in several research projects to explore how spam affects consumers and online commerce. These projects include a "Remove Me" surf, a "spam Harvest," and a study of False Claims in Spam.

The "Remove Me" Surf

[10] Claiming to be well-placed Nigerians, con artists offer to transfer millions of dollars into the prospective victim's bank account in exchange for a small fee. Those who respond to the initial offer may receive official-looking documents. Typically, the victim is then asked to provide blank letterhead and his or her bank account numbers, as well as some money to cover transaction and transfer costs and attorney's fees.

Last year the Commission announced the results of the "Remove Me" surf, in which the FTC and law enforcement partners tested whether spammers where honoring the "remove me"or "unsubscribe" options in spam.[11] From email that participating agencies had forwarded to the FTC's spam database, the Commission's staff selected more than 200 messages that purported to allow recipients to remove their names from a spam list. The agencies set up dummy email accounts to test the pledges. We found that 63 percent of the removal links and addresses in our sample did not function. If a return address does not work to receive return messages, it is unlikely that it could be used to collect valid email addresses for use in future spamming. This finding tends to disprove the common belief that responding to spam guarantees that you will receive more of it.

The "Spam Harvest"

In its "Spam Harvest," the Commission's staff conducted an examination of what online activities place consumers at risk for receiving spam. The examination discovered that one hundred percent of the email addresses posted in chat rooms received spam; one received spam only eight minutes after the address was posted. Eighty-six percent of the email addresses posted at newsgroups and Web pages received spam, as did 50 percent of addresses at free personal Web page services, 27

[11] The "Remove-Me" surf was conducted as part of International Netforce, an enforcement sweep in which the FTC was joined by the Alaska Attorney General, the Alaska State Troopers, Government Services of the Province of Alberta, the British Columbia Securities Commission, the British Columbia Solicitor General, the Canadian Competition Bureau, the Idaho Attorney General, the Montana Department of Administration, the Oregon Department of Justice, the Washington Attorney General, the Washington State Department of Financial Institutions, and the Wyoming Attorney General.

percent from message board postings, and 9 percent of email service directories. The "Spam Harvest" also found that the type of spam received was not related to the sites where the email addresses were posted. For example, email addresses posted to children's newsgroups received a large amount of adult-content and work-at-home spam.

As part of this project, the staff developed consumer education material, including a publication, "E-mail Address Harvesting: How Spammers Reap What You Sow," that provides tips, based on the lessons learned from the Spam Harvest, to consumers who want to minimize their risk of receiving spam. The tips advise, among other things, that consumers can minimize the chances of their addresses being harvested by using at least two email addresses--one for use on web sites, newsgroups and other public venues on the web, and another email address solely for personal communication. Another suggested strategy to reduce spam is "masking" (disguising) email addresses posted in public.[12]

The "False Claims in Spam" Study

An additional FTC staff study examined false claims in spam. The staff examined 1,000 spam messages selected randomly from three sources: our spam database of consumer-forwarded messages, the spam received at the addresses used in the Spam Harvest, and spam that reached FTC

---

[12] Masking involves putting a word or phrase in one's email address so that it will trick a harvesting computer program, but not a person. For example, if one's email address is "johndoe@myisp.com," one could mask it as "johndoe@spamaway.myisp.com." Some newsgroup services or message boards won't allow masking of email addresses and some harvesting programs may be able to pick out common masks.

employee computers. The staff analyzed the messages based upon the types of products or services offered, the indicia of deception in the content of the messages, and the indicia of deception in the "from" and "subject" lines of the messages.

The Types of Products or Services Offered - The staff found that 20 percent of the spam contained offers for investment or business opportunities, which include such things as work-at-home offers, franchise opportunities, or offers for securities. Another 18 percent of the spam offered adult-oriented products or services. Of those adult messages, about one-fifth included images of nudity that appeared automatically in the body of the message. Further, 17 percent of the spam messages involved finance, including credit cards, mortgages, refinancing, and insurance. All together, the investment/business opportunity, adult, and finance offers comprised 55 percent of our sample.

Indicia of Falsity in the Content of Spam Messages - The staff also determined how many spam messages appeared misleading. Using expertise gleaned from past law enforcement actions and recent research efforts, the staff identified specific representations likely to be false. The staff found that 40 percent of all the combined categories of spam messages contained indicia of falsity in the body of the message. An astonishing 90 percent of the investment/business opportunity category of spam contained indicia of false claims.

Evidence of Falsity in the "From" and "Subject" Lines - The staff also looked at evidence of deception in the "from" and "subject" lines of the spam. One third of the messages contained indicia

of falsity in the "from" line. Messages falling into this category included "from" lines connoting a business or personal relationship, such as using a first name only, or stating "Your Account@XYZ.COM." Another common instance of misleading "from" lines occurs when spammers make the sender's name the same as the recipient's address, so it appears that one has sent the message to oneself.

In addition, the staff found that 22 percent of the spam messages contained indicia of falsity in the subject line, such as using "Re:" to indicate familiarity or a subject line that was unrelated to the content of the message, such as "Hi" or "Order Confirmation." Over one third of adult-content spam contained false information in the subject line. Further, *only two percent* of the analyzed spam contained the label "ADV:" in the "subject" line, even though such a label is required by the laws of several states.

Conclusions of the False Claims in Spam Study - Adding up the various forms of deception, the staff found that 66 percent of the spam appeared to contain at least one form of deception.[13] This Spam Study confirms the Commission's earlier belief that fraud operators, who are often among the first to exploit any technological innovation, have seized on the Internet's capacity to reach millions of consumers quickly and at a low cost through spam. Not only are fraud operators able to reach millions of individuals with one message, but they also can misuse technology to conceal their identity. The

[13] The remaining spam messages were not necessarily truthful, but they did not contain any obvious indicia of falsity.

Commission believes the proliferation of fraudulent or deceptive spam on the Internet poses a threat to consumer confidence in online commerce and, therefore, views the problem of deception as a significant issue in the debate over spam.

The 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 more 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 possible solutions to the detrimental effects of spam.

The Commission believes that the Forum advanced both goals. As described below, the panelists contributed valuable information from a variety of differing viewpoints to the public record. In addition, the Forum spurred a number of participants into cooperation and action. Most notably, on the eve of the Forum, industry leaders Microsoft, America Online, and Yahoo! announced a collaborative

effort to stop spam. Moreover, several potential technological solutions to spam were announced either at or in anticipation of the Forum. The Commission intends to foster this dialogue, and, when possible, to encourage other similar positive steps on the part of industry.

The strong interest in addressing spam is shared by: consumers, Internet Service Providers ("ISPs"), law enforcement authorities, marketing services, bulk email marketers, anti-spammers, and retailers and manufacturers. These interest groups were represented at the Forum by 87 different panelists collectively possessing a tremendous range of expertise, and coming from all over the globe to participate in this discussion. Distinguished representatives from the European Commission, Canada, Australia, Korea, and Japan offered their views on how spam affects their countries and how they are trying to tackle the problem. On the domestic front, panelists included prominent representatives from all sectors affected by spam, such as the president of the consumer group, the SpamCon Foundation, the president of the Direct Marketing Association, vice presidents of America Online and Microsoft, and the Washington State Attorney General. Distinguished members of Congress - Senators Burns, Wyden, and Schumer, and Representative Lofgren – also addressed Forum attendees.

The Spam Forum was organized into twelve panel discussions that were conducted over the course of three days. In addition to the 87 panelists, approximately 400 people were present each day in the audience at the FTC Conference Center, with many more individuals participating via a video link or by teleconference. Questions for the panelists were accepted from the audience and via a special email address from those attending through video link or teleconferencing.

Day One of the Forum focused on the mechanics of spam. Panelists discussed in detail how spammers find email addresses and how deception in the sending of spam affects consumers and online commerce. Discussions then focused upon security weaknesses that enable or facilitate spam, such as open relays[14] and open proxies.[15] Day Two explored the economic costs of spam. Panelists participated in an in-depth discussion of economic incentives inherent in spam and the costs of spam to marketers, ISPs, and consumers, and its effects on emerging technologies. Specifically, panelists discussed spam blacklists, email marketers, and wireless spam (unsolicited text messages received via cell phone). Day Three focused on potential solutions to spam. Panelists discussed three potential avenues to a solution: legislation, litigation, and technology. Specific topics covered included: state, federal, and international legislation; civil and criminal law enforcement and private litigation against spammers; and various technological approaches.

Panelists at the Forum bought forward an enormous amount of information about spam and how it affects consumers and businesses. Several primary themes emerged from the various

---

[14] Open relays allow spammers to route their email through servers of other organizations, thereby disguising the origin of the email. Spammers identify and use other organizations' open relays to avoid detection by the filter systems that ISPs use to protect their customers from unwanted spam. Routing spam through open relays also makes it difficult for law enforcement agencies to track down senders of fraudulent or deceptive spam.

[15] A proxy server runs software that allows it to be the one machine in a network that directly interacts with the Internet. This provides the network with greater security. But if a proxy is not configured properly (*i.e.*, if it is an "open proxy"), it also may allow unauthorized users to pass through the site and connect to other hosts on the Internet. For example, a spammer can use an open proxy to connect to a mail server. If the server has an open mail relay, the spammer can send a large amount of spam and then disconnect - all anonymously.

discussions. First, the volume of spam is increasing sharply. Many panelists reported that the rate of increase is accelerating. For example, one ISP reported that in 2002 alone it experienced a 150 percent increase in spam traffic. Second, spam imposes real costs. The panelists offered concrete information about the costs of spam to businesses and to ISPs. Specifically, ISPs reported that costs to address spam have increased dramatically over the past two years. ISPs bear the cost of servers and bandwidth necessary to channel the flood of spam, even that part of the flood that is being filtered out before reaching recipients' mail boxes. America Online reported that it recently blocked an astonishing 2.37 billion pieces of spam in a single day. Third, spam is an international problem. According to our international panelists, most of the spam received in their countries is in English and advertises American products or companies. Most panelists agreed that any solution to stopping spam will have to involve an international effort.

Our law enforcement experience has taught that the path from a fraudulent spammer to a consumer's in-box typically crosses at least one international border and frequently several. Thus, fraudulent spam exemplifies the growing problem of cross-border fraud. To enhance our effectiveness in the fight against fraudulent spam and other kinds of fraudulent schemes that cross international borders, the Commission will be asking this Committee, as part of our forthcoming reauthorization testimony, for additional legislative authority in a number of areas, including measures that would: allow the agency to share such information on targeted schemes with our overseas counterparts; provide investigative assistance to them in appropriate cases; improve our ability to obtain information from U.S. criminal agencies and federal financial regulators, who are often investigating the same types of

fraudulent conduct that we are; and improve the agency's ability to obtain consumer redress in cross-border cases by clarifying the Commission's authority to take action in such cases, and by expanding the agency's ability to use foreign counsel to pursue assets offshore. Legislation expanding the Commission's authority in these ways is essential to improve the agency's ability to fight fraudulent spam in particular, as well as other manifestations of the more general problem of cross-border fraud.

Approaches to Solving the Spam Problem

The broad themes that emerged from the Forum panel discussions depict the spam problem as increasing volume, increasing costs, and increasing international effects. This confirms that finding solutions to the problems posed by spam will not be quick or easy; moreover, the consensus of panelists was that no single approach will likely cure the problem. Some panelists at the Forum stated that a large scale technological change in the email protocol system is not likely to occur. Nevertheless, others indicated that there are incremental technical changes that can be grafted onto the existing email protocol to ease the burden of unwanted email on ISPs and consumers. In addition, consumer representatives stressed that any solution should include consumer empowerment – to allow email recipients to decide what messages they want to receive in their inbox, and to give recipients the technical tools to effectuate those decisions. Some panelists, but by no means all, advocated additional federal legislation and law enforcement efforts as a means to provide needed accountability and deterrence.

All Spam Forum participants agreed that solving the problem of bulk unsolicited commercial email will likely necessitate an integrated effort involving a variety of technological, legal, and consumer action, rather than one single solution. Through the Forum and the follow-up efforts it suggested, the Commission hopes to act as a catalyst for technologists, industry, law enforcement, and policy officials to work together to find a solution.

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 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, and the outcome of its recent Spam Forum.