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 20, 2004

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 unsolicited commercial email ("spam"), its activities undertaken to date to fulfill the various mandates contained in the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM" or the "Act"), and its efforts to enforce the Act's substantive provisions.[1]

Spam creates problems well beyond the aggravation it causes to the public. These problems include the fraudulent and deceptive content of a large percentage of spam messages, the offensive content of many spam me0.000r6rom8.4(.4(m)8.4(bee As)8.1(acro probl0.0006 Tc-0.0008 Tw[(Sp

[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] 15 U.S.C. § 45. The Federal Trade Commission Act prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. *See* 15 U.S.C. § 41 *et seq.* The Commission 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; 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] *See* <http://www.ftc.gov/opa/2004/04/040429canspam.htm

temporary restraining order that, among other things, stops further deceptive product sales, freezes the Defendants' assets, and preserves their records.

temporaryT-p.ely n8.4(m)8.42004aScomlaitraintem5Thn investigati T asprincipals7haes,been charg04]T

[5] The caption and case number for the criminal complaint are: United States v. Daniel J. Lin, James J. Lin, Chris Chung, and Mark M. Sadek, Case No. 04-80383 (E.D. Mich.).

[6] Case No. 04C 3022 (N.D. Ill. filed Apr. 28, 2004)

disclosure of an opportunity not to receive further email, in violation of Sections 5(A)(5)(a)(ii) and (iii) of CAN-SPAM. Because the Defendants shipped their products using fulfillment houses in the United States, the Commission has obtained a preliminary injunction that, among other things, will enjoin the fulfillment houses from further delivery of the Defendants' deceptively-marketed products. In investigating this case, the Commission received invaluable assistance from the Australian Competition and Consumer Commission and the New Zealand Commerce Commission.

The CAN-SPAM cases the Commission is currently pursuing follow an extended Commission effort to target spam under Section 5 of the FTC Act. One aspect of this effort has been the Commission's two-year Netforce law enforcement partnership with other federal and state agencies, which has targeted deceptive spam. This partnership includes the Department of Justice, FBI, Postal Inspection Service, Securities and Exchange Commission, and Commodities Futures Trading Commission, as well as state Attorneys General, and local enforcement officials. In four regional law enforcement sweeps, the most recent announced in May 2003, the Netforce partners filed more than 150 criminal and civil cases against allegedly deceptive spam and other Internet fraud.[7] In one recent sweep case, for example, the Commission obtained a permanent spam ban against defendants who allegedly used deceptive "From" lines in their spam to claim

[7] More information about the Netforce law enforcement sweeps is available on the FTC's web site: <http://www.ftc.gov/opa/2002/04/spam.htm> (Northwest Netforce); <http://www.ftc.gov/opa/2002/07/mwnetforce.htm> (Midwest Netforce); <http://www.ftc.gov/opa/2002/11/netforce.htm> (Northeast Netforce); and <http://www.ftc.gov/opa/2003/05/swnetforce.htm> (Southwest Netforce).

affiliation with Hotmail and MSN in touting a fraudulent work-at-home envelope-stuffing scheme.[8]

The Commission remains committed to aggressive pursuit of spammers who violate Section 5 of the FTC Act and the CAN-SPAM Act, and we remain committed to working with our law enforcement partners to find and take action against spammers.

Consumer and Business Education

The Commission's educational efforts include a spam home page with links to 15 pamphlets for consumers and businesses, including one in Spanish, and summaries of our partnership enforcement efforts to halt deceptive spam.[9] One of the most important business education efforts was "Operation Secure Your Server," announced on January 29, 2004. Through this initiative, the Commission partnered with 36 agencies in 26 countries to highlight the problem of "open proxies"[10] on third-party servers that spammers use to hide the true source of their spam.[11] This project was an outgrowth of last year's "Open Relay Project," in which 50

---

[8] *FTC v. Patrick Cella, et al.*, No. CV-03-3202, (C.D. Cal. entered Nov. 21, 2003). *See* <http://www.ftc.gov/opa/2003/05/swnetforce.htm>; <http://www.ftc.gov/opa/2003/11/dojsweep.htm>.

[9] The home page is located at <http://www.ftc.gov/bcp/conline/edcams/spam/index.html>.

[10] Most organizations have multiple computers on their networks, but have a smaller number of "proxy" servers – the only machines on the network that directly interact with the Internet. This system provides more efficient web browsing for the users within that organization and secures the organization's network against unauthorized Internet users from outside the organization. If the proxy is not configured properly, it is considered to be "open," and may allow an unauthorized Internet user to connect through it to other hosts (computers that control communications in a network or administer databases) on the Internet. In this way, open proxies provide one of several methods that spammers use to hide their identities.

[11] The press release can be found at <http://www.ftc.gov/opa/2004/01/opsecure.htm>. Tens of thousands of owners or operators of potentially open relay or open proxy servers around the world received the Operation Secure Your Server business education letter.

[12] 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. By contrast, a "secure" server accepts and transfers mail only on behalf of authorized users. *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>.

[13] *See* <http://www.informationweek.com/story/showArticle.jhtml?articleID=18200812; http://www.spamhaus.org/news.lasso?article=150>.

[14] In fact, some sources estimate that anywhere from 30-80% of spam is routed through

"from" line and header information are common spammer stratagems.[17] Even with incredibly painstaking, expensive, and time-consuming investigation, it is often impossible to determine where spam originates. Spammers are extremely adroit at concealing the paths that their messages travel to get to recipients' in-boxes. Typically, the most that can be ascertained with certainty is the last computer through which the spam traversed immediately before arriving at its final destination. To frustrate law enforcers, clever spammers may arrange for this penultimate computer to be outside the country where the spam's ultimate recipient is located.

Another example of "spam lore" is the notion that a handful of "kingpin" spammers are responsible for the vast majority of spam. This may or may not be true, but nobody knows for sure. The Commission recently used its compulsory process authority under Section 6(b) of the FTC Act to require the production of information on an exhaustive list of spam topics from various ISPs and other entities. The Section 6(b) specifications included items focusing on the "kingpin" theory. These requests yielded wildly varying estimates, ranging from the familiar "200 spammers" figure to "thousands" of individuals responsible for the majority of spam.[18] In

---

Scripts Panel, pp. 257, 274, *available at* <http://www.ftc.gov/bcp/workshops/spam/>.

[16] "Spoofing" and "forging" involve manipulating an email's "from" line or header information to make it appear as if the message were coming from an email address from which it did not actually originate.

[17] At the FTC Spam Forum, Margot Koschier from AOL conducted a live demonstration of how to forge header information. In several minutes, she was able to send a message that appeared to come from FTC Chairman Tim Muris in the year 2024. Other Spam Forum panelists also discussed the prevalence of false "sender" information in spam. For example, an MCI representative stated that 60% of the spam complaints received at MCI have false headers, false email addresses, deceptive subject lines, or a combination of all three. *See* FTC Spam Forum transcript, Day 1, *Falsity in Spam Panel*, *available at* <http://www.ftc.gov/bcp/workshops/spam/>.

[18] This uncertainty is reflected, for example, in six lawsuits jointly announced by several ISPs on March 10, 2004. They sued nine individuals, and over 200 unknown "John Does." *See* Joint press release of AOL, Earthlink, Microsoft, and Yahoo!, *available at*

<http://www.microsoft.com/presspass/press/2004/mar04/03-10CANSPAMpr.asp>. Similarly, in 60 separate FTC cases targeting schemes that used spam as an integral part of the scam, no two cases had the same spammer.

[19] See remarks of Laura Betterly at the FTC Spam Forum. Betterly stated that she paid $15,000 for her email business and broke even within

email accounts received more spam after attempting to unsubscribe. This finding is inconsistent with the common belief that attempting to unsubscribe guarantees that consumers will receive more spam.

Another study in 2002, the "Spam Harvest," examined what online activities place consumers at risk for receiving spam.[21] We discovered that all of the email addresses that we posted in chat rooms received spam. In fact, one address received spam only eight minutes after the address was posted. Eighty-six percent of the email addresses posted in newsgroups and Web pages received spam, as did 50 percent of addresses in free personal Web page services, 27 percent in message board postings, and 9 percent in 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.

A third study focused on false claims in spam by analyzing a sample of 1,000 messages drawn from three sources.[22] The Commission staff issued a report on April 30, 2003, explaining that two-thirds of the sample contained indicia of falsity in the "from" lines, "subject" lines, or

---

[21] The"Spam Harvest" was conducted as part of the Northeast Netforce, an enforcement sweep in which the FTC was joined by the Connecticut Attorney General, the Maine Attorney General, the Massachusetts Attorney General, the New Hampshire Department of Justice, the New Jersey Division of Consumer Affairs, the New York City Department of Consumer Affairs, the New York State Attorney General, the New York State Consumer Protection Board, the Rhode Island Attorney General, the United States Attorney for the District of Massachusetts, the United States Postal Inspection Service, and the Vermont Attorney General. See <http://www.ftc.gov/opa/2002/11/netforce.htm>.

[22] The study's sources were the FTC's database of millions of spam forwarded to the Commission by consumers, messages received in the "Spam Harvest," and messages delivered to FTC employees' email accounts.

[23] *False Claims in Spam*: A Report by the FTC's Division of Marketing Practices (April 30, 2003), *available at* <http://www.ftc.gov/reports/spam/030429spamreport.pdf>.

[24] None of the spam in this sample was sent by a *Fortune* 500 company. The sample provides 95% confidence that less than 5% of the 11.6 million pieces of spam then in the FTC's database of spam forwarded by consumers came from a *Fortune 1000*

years immediately preceding the forum. ISPs bear the cost of maintaining servers and bandwidth necessary to channel the flood of spam, even that part of the flood that is filtered out before reaching recipients' mail boxes. At the Forum, America Online reported that it blocked an astonishing 2.37 billion pieces of spam in a single day.[26] Third, spam is an international problem. The panel discussing open proxies and open relays and the international panel described spam's cross-border evolution and impact. Most panelists agreed that any solution will have to involve an international effort.

The Commission convened this event for two principal reasons. First, as noted above, spam is frequently discussed, but facts about how it works, its origins, and what incentives drive it are elusive. The Commission anticipated that the Forum would generate an exchange of useful information about spam to help inform the public policy debate. Second, the Commission sought to act as a potential catalyst for solutions to the spam problem. Through the Forum, the Commission brought together 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. The panelists contributed valuable information from various viewpoints to the public record. In addition, the Forum spurred both cooperation and action among a number of participants. Most notably, on the eve of the Forum, industry leaders Microsoft, America Online, Earthlink, and Yahoo! announced a collaborative effort to stop spam. This promising effort continues today with participation from

---

[26] FTC Spam Forum transcript, Day 1, *Introduction to Spam Panel*, p. 39, *available at* <http://www.ftc.gov/bcp/workshops/spam/transcript_day1.pdf>.

additional industry leaders.[27] 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. We believe that the Forum contributed significantly to the ongoing effort on the part of industry, consumers, and government to learn how to control spam.

Efforts Since CAN-SPAM Went Into Effect

To provide additional tools to fight spam, Congress enacted the CAN-SPAM Act on December 16, 2003.[28] The Act took effect on January 1, 2004, and the Commission immediately sought to enforce the Act, to meet the aggressive deadlines it set for the completion of several rulemakings and reports, and to develop national and international partnerships to help combat deceptive spam. The Commission filed its first two CAN-SPAM cases within four months of the Act's effective date. As mentioned earlier, combating spam has been one of the Commission's top priorities for several years, and currently half of the staff members in the Bureau of Consumer Protection's largest enforcement division work on CAN-SPAM issues, as do staff in all of the Commission's regional offices and additional lawyers, investigators, and technologists throughout the FTC.

Moreover, to facilitate enforcement by other law enforcement agencies, we have consulted with our partners at the Department of Justice and have organized a task force with state officials to bring cases. The Task Force is co-sponsored by the FTC and the Attorney

---

[27] *See, e.g.*, "ISPs Sue Spammers," Article dated March 12, 2004, reporting on CAN-SPAM cases brought by four ISPs, *available at* <http://www.pcmag.com/print_article/0,1761,a=121533,00.asp>.

[28] Pub. L. 108-187 (codified at 15 U.S.C. § 7701 *et seq.)*.

[29] The Commission continues to try to recruit representatives from the remaining states.

[30] 69 Fed. Reg. 4263 (Jan. 29, 2004). Section 5(d)(3) of CAN-SPAM requires that "[n]ot later than 120 days after the date of the enactment of this Act, the [Federal Trade] Commission in consultation with the Attorney General shall prescribe

subject line or in the portion of the message initially viewable by recipients when the message is opened.

In addition, on March 11, 2004, the Commission issued an Advance Notice of Proposed Rulemaking ("ANPR") to define the relevant criteria to be used in determining "the primary purpose" of a commercial electronic mail message subject to CAN-SPAM's provisions.[33] The ANPR requested comment on this issue, as well as a number of other issues for which CAN-SPAM has provided the Commission discretionary rulemaking authority, such as modifying the definition of "transactional" email messages;[34] changing the 10-business-day statutory deadline for emailers to comply with consumers' opt-out requests;[35] and implementing other CAN-SPAM provisions.[36] The Commission received over 12,000 comments in response.[37] Commission staff is incorporating suggestions and recommendations from these comments into its Notice of Proposed Rulemaking.

The Commission is also actively preparing several reports required by the CAN-SPAM Act. The March 11 ANPR solicited comment from interested parties on a plan and timetable for establishing a national Do-Not-Email Registry, and an explanation of any practical, technical,

---

[33] Pub. L. 108-187, § 3(2)(A) (codified at 15 U.S.C. § 7702(2)(A)). The rulemaking is required by § 3(2)(C) (codified at 15 U.S.C. § 7702(2)(C)), and is on track for completion by the statutory deadline of December 16, 2004.

[34] Pub. L. 108-187 § 3(17) (codified at 15 U.S.C. § 7702(17)). Transactional messages must comply with the Act's prohibition against deceptive headers, *Id*., § 5(a)(1) (codified at 15 U.S.C. § 7704(a)(2), but are otherwise exempt from the Act. *Id*., § 3(2)(B) (codified at 15 U.S.C. § 7702(2)(B)). A rulemaking is permitted by § 3(17)(B) (codified at 15 U.S.C. § 7702(17)(B)).

[35] *Id*., § 5(a)(4)(A)-(B) (codified at 15 U.S.C. § 7704(a)(4)(A)-(B)). A rulemaking is permitted by § 5(c)(1) (codified at 15 U.S.C. § 7704(c)(1)).

[36] *Id*., § 13(a) (codified at 15 U.S.C. § 7711).

[37] *Available at*: <http://www.ftc.gov/os/comments/canspam/index.htm>.

security, privacy, enforceability, or other concerns commenters may have about the creation of such a registry, for a report to Congress due on June 16.[38] To supplement information collected

[38] *Id*., § 9 (codified at 15 U.S.C. § 7708).

[39] *Id*., § 11(1) (codified at 15 U.S.C. § 7710(1)).

[40] *Id*., § 11(2) (codified at 15 U.S.C. § 7710(2)).

[41] *Id*., § 10 (codified at 15 U.S.C. § 7709). The agency is gathering baseline data for this report through the § 6(b) requests for information and other activities.

Conclusion

Email provides enormous benefits to consumers and businesses as a communication tool. The increasing volume of spam, coupled with the use of spam as a means to perpetrate fraud and deception, has put these benefits at serious risk. The Commission intends to continue its law enforcement, education, and research efforts to protect consumers and businesses from the current onslaught of unwanted spam messages. The Commission appreciates this opportunity to describe its efforts to address the problem of spam and its activities to fulfill the mandates of CAN-SPAM.