

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 messages, the sheer volume of spam being sent across the Internet, and the security issues raised when spam is used to disrupt service or to send spyware or viruses carrying malicious code.

The Commission has pursued a three-fold strategy to combat the plague of spam. First, it has pursued a vigorous program of law enforcement against spammers, both before the enactment of CAN-SPAM and since it became effective on January 1, 2004. Second, we have an extensive education program to alert consumers and businesses about self-help measures they can take against spam. Third, we have studied the problem of spam to inform our enforcement and consumer education efforts, and to remedy the paucity of reliable data about spam.

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.

Law Enforcement

The Commission has brought 62 law enforcement actions in recent years against alleged fraudulent operations using spam as an integral component of their scams. Most of these cases predate CAN-SPAM, and were brought under Section 5 of the FTC Act.² Two of our most-recent spam cases, filed in federal district court in April, target extremely prolific spammers and allege violations of both CAN-SPAM and the FTC Act.³

The Commission's complaint in the first of these cases, FTC v. Phoenix Avatar, LLC, et al.,⁴ alleges that the Defendants used materially false or misleading header information in their email messages, in violation of Section 5(a)(1) of the CAN-SPAM Act; specifically, the Defendants placed the email addresses or domain names of unsuspecting third parties in the "reply-to" and/or "from" fields of their spam (a practice known as "spoofing"). The complaint also alleges that the Defendants failed to provide the disclosures required by Sections 5(a)(5)(A)(ii) and (iii) of the Act, including the required notice of an opportunity to decline to receive further commercial email from the sender. Further, the complaint alleges that the Defendants made false and unsubstantiated claims about diet patches marketed in part through the email messages, in violation of Section 5 of the FTC Act. The Commission has obtained a

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>>.

⁴ Case No. 04C 2897 (N.D. Ill. filed Apr. 23, 2004)

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

In investigating and filing this matter, the Commission worked closely with the U.S. Attorney for the Eastern District of Michigan and the Detroit Office of the Postal Inspection Service, who are pursuing a concurrent criminal prosecution of the principals of this scheme. The U.S. Attorney filed a criminal complaint, executed a criminal search warrant, and arrested four principals.⁵ The principals have been charged with violations of the federal mail fraud laws as well as with criminal violations of the CAN-SPAM Act.

The second case, FTC v. Global Web Promotions Pty Ltd.,⁶ targets an Australian company that the FTC alleges is responsible for massive amounts of spam sent to consumers in the United States. According to the complaint, the Defendants used spam to advertise a diet patch similar to the one in Phoenix Avatar, as well as purported human growth hormone products "HGH" and "Natural HGH" that Defendants claimed could, among other things, "maintain [a user's] appearance and current biological age for the next 10 to 20 years." The Defendants sold the diet patch for \$80.90 and the HGH products for \$74.95. The FTC alleged that these claims are false and unsubstantiated, and therefore deceptive in violation of Section 5 of the FTC Act.

The complaint alleges that the Defendants also used materially false or misleading header information of unsuspecting third parties (spoofing), in violation of Section 5(a)(1) of the CAN-SPAM Act, and failed to include required disclosures in their email messages, including

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/online/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.

law enforcers from 17 agencies identified 1,000 potential open relays.¹² The agencies sent a letter, signed by 14 different U.S. and international agencies and translated into 11 languages, urging the organizations with these open relays to close them and explaining how to do so.

Studies and Workshops

Everybody receives spam, but there is little known about it. Reliable information about spam is extremely limited, although there is much “spam lore” that has little if any basis in fact. For example, some sources in Europe claim that the vast majority of spam originates in the United States.¹³ Similarly, some sources in the U.S. opine that most spam in Americans’ inboxes arrives from Asia, South America, or Eastern Europe.¹⁴ In fact, nearly all spam is virtually untraceable, either because it contains falsified routing information or because it comes through open proxies or open relays.¹⁵ Moreover, “spoofing” and “forging”¹⁶ of an email message’s

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/online/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 open relays and open proxies, and many of these machines are scattered throughout the world. See <http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,2122679,00.htm>; <http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/>.

¹⁵ In testimony presented to this Committee last year, Brightmail estimated that 90% of the email that it analyzed was untraceable. http://www.brightmail.com/pressreleases/102203_senate_bill_877.html. At the FTC’s May 2003 Spam Forum two panelists representing ISPs estimated that 40% to 50% of the email they analyzed coming to or through their networks made use of open relays or open proxies, making it virtually impossible to trace. FTC Spam Forum transcript, Day 1, *Open Relay, Open Proxies, and Formmail*

“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

fact, the low barriers to entry suggest that many individuals, and not just a handful, may engage in spamming and contribute significantly to the volume of spam traversing the Internet.¹⁹

The prevalence of “spam lore” of questionable validity and the corresponding paucity of reliable data on spam has prompted the FTC’s staff to perform research on the issue. In one of the first of these efforts, the Commission’s staff, working with a partnership of law enforcement officials in several states and Canada,²⁰ conducted a “Remove Me” surf in 2002 to test whether spammers were honoring “remove me” or “unsubscribe” options in spam. From email that the partnership 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. To test these “remove me” options, the partnership set up unique email accounts that had never been used before and submitted “remove me” requests from these accounts. The staff found that 63 percent of the removal links and addresses in the 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. In no instance did we find that any of our unique

<<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 3 months. FTC Spam Forum transcript, Day 2, *Economics of Spam Panel*, pp. 28-29, available at <http://www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf>.

²⁰ The “Remove Me” surf was conducted as part of the Northwest 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. See <<http://www.ftc.gov/opa/2002/04/spam.htm>>.

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.

message text,²³ and that in a smaller random sample of 114 pieces of spam taken from the same set of data, only one came from an established business in the *Fortune* 1000.²⁴ This study, the first extensive review ever conducted of the likely truth or falsity of representations in spam, underscores both the potential harm to consumers from spam and spammers' willingness to ignore the law.

One of the most important projects in our ongoing effort to study and understand the phenomenon of spam and its impact on the Internet and the economy at large was the Spam Forum, a three-day public forum from April 30 to May 2, 2003. This Forum provided a wide-ranging public examination of spam from all viewpoints.

The Spam Forum was organized into twelve panel discussions covering the mechanics of spam, the economics of spam, and potential ways to address the problem of spam.²⁵ Panelists at the Forum brought forward an enormous amount of information about spam and how it affects consumers and businesses. Several primary themes emerged from the various panels. First, there was much discussion about the increasing amount of spam. 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 increased dramatically in the two

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 company, and a 95% confidence that less than 3% of the email in our database was sent by or on behalf of a *Fortune* 500 company. The database now contains approximately 100 million messages.

²⁵ In addition to the 87 panelists who participated, 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 teleconference. Questions for the panelists were accepted from the audience and via a special email address from those attending through video link or teleconferencing.

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.*).

General of Washington, and is comprised of 136 members representing 36 states, several units within the Department of Justice, and the FTC.²⁹ The FTC staff so far has conducted two training sessions on investigative techniques for the Task Force, each of which was attended by approximately 100 individuals representing about 35 different states. The Task Force conducts monthly conference calls to share information on spam trends, technologies, investigative techniques, targets, and cases.

The Commission is also on target to complete the rulemakings and reports required by CAN-SPAM. On January 28, 2004, the Commission issued a Notice of Proposed Rulemaking for a mark or notice that will identify spam containing sexually oriented material.³⁰ The Commission received 89 comments in response.³¹ We issued a final rule in advance of the statutory deadline of April 14.³² Effective May 19, the rule requires all messages containing sexually oriented material to include the warning “SEXUALLY-EXPLICIT: ” in the subject line. This rule also prohibits these messages from presenting any sexually explicit material in the

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 clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph.” (codified at 15 U.S.C. § 7704(d)(3)). Under CAN-SPAM, the term “sexually oriented material” is “any material that depicts sexually explicit conduct (as that term is defined in § 2256 of title 18, United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.” *See* 15 U.S.C. § 7704(d)(4). 18 U.S.C. § 2256, in turn, provides that “sexually explicit conduct means actual or simulated (A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (B) bestiality; (C) masturbation; (D) sadistic or masochistic abuse; or (E) lascivious exhibition of the genitals or pubic area of any person.”

³¹ Available at <<http://www.ftc.gov/os/comments/adultemai labeling/index.html>>.

³² See <<http://www.ftc.gov/opa/2004/04/adultlabel.htm>>.

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 from this public comment process, the staff has used additional tools to enhance its understanding of all relevant issues. First, the staff has held meetings on the record with more than 80 interested parties representing more than 60 organizations to explore all aspects of the concept of a “Do-Not-Email Registry” from as many viewpoints as possible. Second, the Commission also issued compulsory process to a number of ISPs and other entities under Section 6(b) of the FTC Act to obtain information relevant to this report and other reports required by CAN-SPAM. Third, the Commission issued a Request for Information from vendors for creation of such a registry, and obtained assistance of expert consultants to assess vendors’ submissions. Through these efforts, the Commission has received invaluable information that will allow us to prepare a comprehensive report.

In addition, the staff is actively gathering information for and preparing:

- a report due September 16, 2004, setting forth a system of monetary rewards to encourage informants to report the identities of violators of CAN-SPAM;³⁹
- a report due June 16, 2005, recommending whether or not commercial electronic mail should be identified as such in its subject line by the use of a label like “ADV”;⁴⁰ and
- a report due December 16, 2005, on the efficacy of the Act .⁴¹

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.