The Federal Trade Commission

Opening Remarks of Deborah Platt Majoras
"Developing A Plan for Action in the Fight Against Malicious Spam"
Spam Summit: The Next Generation of Threats and Solutions
Wednesday, July 11, 2007
9:00 a.m.

Welcome and thank you for joining us. I especially want to thank our distinguished panelists for being here to share their insights and expertise.

In 1971, C.P. Snow, noted British author and commentator on science and technology issues, said of technology – "it brings you great gifts with one hand, and it stabs you in the back with the other." Although spam was known only as a lunch meat when Snow said this, his quote is spot on with respect to email and spam. Email technology has brought us great gifts in the form of quick, efficient, and ubiquitous communication. But it also has brought us spam, which has the potential to metaphorically "stab us in the back" by inundating consumers' inboxes with unwanted email, facilitating fraud and malware, and betraying consumers' trust and confidence in the Internet.

In 2003, the FTC convened a Spam Forum to discuss the technical, legal, and financial issues associated with spam. Today and tomorrow, in a continuing effort to stay apprised of developments, we will explore the next generation of spam threats and solutions. The volume of unsolicited emails being reported by email filtering companies is rising, creating costs for businesses and consumers alike. Botnets – networks of hijacked personal computers that spammers use to conceal their identities – have become the preferred method for sending spam. Even more troubling, spam reaching consumers' inboxes is more often being used to launch phishing attacks and to deliver malicious code or "malware" to consumers' computers.

This new generation of malicious spam goes beyond mere annoyance – it can result in significant harm to consumers and undermine the stability of the Internet and email in particular. If you click on a link in an email message, you may be lured to a website that will either trick you into divulging your personally identifying information, or infect your computer with spyware or other types of malware. Even merely opening a malicious email can subject you to harm from malware.[1] The surreptitious deployment of such malware can result in slowed computer performance; installation of key-logger software that can record and report your every keystroke; the spread of computer viruses; and the hijacking of your computer for use as a botnet.

In addition, new threats to communications media other than email are knocking on the door. Spam's cousins, SPIM (spam over instant messaging), SPIT (spam over internet telephony), and spam to mobile devices, threaten to undermine the benefits of mobile services and Internet telephony in the same way as spam. Social networking web sites have become yet another frontier for spam messages. The lessons we have learned and continue to learn from spam also will be valuable as we begin to address, or even better avoid, similar problems for other communications technologies.

[1] Cited originally in our Report to Congress concerning the effectiveness of the CAN-SPAM Act. http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf. "Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress" at 17 (December 2005).

We must work to combat malicious spam in several ways. The first way is through law enforcement. We cannot permit the electronic world to become a lawless frontier. The FTC has engaged in aggressive law enforcement to combat spam. Since 1997, the Commission has aggressively pursued deceptive and unfair practices perpetrated through spam in 89 law enforcement actions against 142 individuals and 99 companies, with 26 of the cases filed after Congress enacted the CAN-SPAM Act. For example, in one recent case, *FTC v. Dugger,* the FTC sought to stop the underlying use of botnets to send spam. The Commission alleged that the defendants relayed sexually-explicit commercial e-mails through other people's home computers without their knowledge or consent in violation of the CAN-SPAM Act.[2] Under the final order obtained in the case, the defendants are barred from violating the CAN-SPAM Act and required to turn over all of their ill-gotten gains. The defendants also are required to obtain the authorization of a computer's owner before using it to send commercial email and to inform the owner how the computer will be used.

Of course, malicious spam also can be a means to disseminate spyware, or other malware that causes some of the same problems as spyware. The FTC has actively pursued spyware companies using its authority under Section 5 of the FTC Act, bringing over 11 law enforcement actions in the past two years.[3]

[2] Section 5(b)(3) of CAN-SPAM, 15 U.S.C. § 7704(b)(3), states: It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under subsection (a) from a protected computer or computer network that such person has accessed without authorization.

[3] These actions have reaffirmed three key principles. First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures about software and its effects are not adequate, just as they have never been adequate in traditional areas of commerce. And third, if a distributor puts an unwanted program on a consumer's computer, he or she must be able to uninstall or disable it.

In most instances, the acts of malicious spammers are inherently criminal, and criminal law enforcement agencies are best suited to expertly shut down their criminal operations. For example, in June, the FBI and Department of Justice announced a crackdown on botnets and those who control them. As part of this operation, the FBI and DOJ identified more than one million personal computers infected with malware that allowed them to be hijacked and used as part of an army of bots to attack other computers, spread malware, or send spam.[4] To date, the crackdown has netted three arrests: Robert Soloway, who allegedly sold spam kits and access to botnets for spamming; James Brewer, who allegedly compromised more than 10,000 PCs around the world; and Jason Downey, who allegedly ran a botnet used to conduct distributed denial of service (DDoS) attacks. While there is no single solution to halt the use of botnets and malware completely, these large scale arrests and criminal law enforcement actions are significant.

A second way to defend ourselves from malicious spam is knowledge – knowing with whom we are interacting. Just as we can ask visitors to swipe identification badges and use biometric identifiers to verify who is entering our physical space, we can use authentication technology to verify who is entering our electronic space. At the Commission's November 2004 Email Authentication Summit, cosponsored with the Department of Commerce's National Institute of Standards and Technology, the Commission gathered a wide spectrum of interested parties to find a solution to the problem of email anonymity, with the goal of invigorating the search for - and agreement on - viable email authentication tools. Since that time, domain-level email authentication and email reputation services have been adopted at higher levels: over

[4] Over 1 Million Potential Victims of Botnet Cyber Crime, http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm, (June 13, 2007).

seventy percent of the Fortune 100 authenticate their outbound email,[5] while over twenty-five percent of the Fortune 500 authenticate their outbound email;[6] trade associations such as the Direct Marketing Association and the Email Sender and Provider Coalition even require their members to authenticate their email.[7] The Commission urges the continued improvement in anti-spam technology and, in particular, domain-level authentication. This technology, paired with reputation and accreditation systems, holds the greatest promise for preventing spammers from operating anonymously. The Commission intends to continue to work to spur industry efforts to create and deploy authentication technologies even more broadly.

Third, to protect ourselves, we must practice self-defense. As consumers, we all must learn how to spot, avoid, and defend ourselves against malicious spam. The FTC has taken steps to educate consumers about how to avoid problems with phishing, malware, and spambots in a consumer alert, "Botnets and Hackers and Spam (Oh, My!)" and on its comprehensive website, "OnguardOnline.gov." These education materials encourage consumers to use anti-virus and anti-spyware software and to keep the software up-to-date, among other tips. During this Summit, we will explore other measures that both consumers and businesses can take to further empower themselves in the fight against malicious spam.

[5] Over 70% of Fortune 100 Companies Authenticating Email Messages through Email Service Providers, Compliance with Email Service Provider Coalition Mandate Drives Wide Adoption by Major Brands, http://www.espcoalition.org/110905fortune.php (November 29, 2005).

[6] Fortune 500 Demonstrates Commitment to Online Safety, http://www.aotalliance.org/news/F500leaders3_6.html, (March 7, 2007).

[7] DMA Requires Members to Adopt E-Mail Authentication Systems, http://www.the-dma.org/cgi/dispannouncements?article=373, (October 17, 2005); Email Sender and Provider Coalition Issues Email Authentication Position Statement at INBOX West 2005, http://www.espcoalition.org/060105eaps.php, (June 1, 2005).

Fourth, just as we sometimes need help to protect ourselves in the physical world, collaboration among stakeholders in the electronic world is invaluable in the fight against malicious spam. Given the technical aspects of the spam problem, continued collaboration with experts from the technical community, including Internet Service Providers and email filtering companies, will strengthen efforts in the fight against malicious spam. In addition, because of the global nature of malicious spam, international cooperation is essential. Most of our enforcement actions involving spam have had an international component, and we have cooperated with foreign enforcement agencies on many of them. In addition to cooperating with foreign partners on individual cases, the FTC is active in the London Action Plan initiative, an informal network of spam enforcers and industry representative from over 20 countries that allows participants to discuss cases, investigation techniques, and educational initiatives. The recently-enacted US SAFE WEB Act, which gives us authority to cooperate more closely with our foreign counterparts, gives us tools we need to strengthen our enforcement program, and we are using those tools now to share information with our overseas counterparts.

My hope is that, at this two-day summit, you will work with us to further explore the problem and these and new approaches. By the end of the summit, we want to have a record that:

- defines the malicious spam problem;
- identifies methods used for sending malicious spam;
- uncovers the malware economy;
- identifies threats that malicious spam poses to emerging platforms such as mobile devices and social networking websites;
- examines methods that law enforcement can deploy to deter malicious spammers

and cybercriminals;

- develops educational tips for putting consumers back in control;
- explores technological tools for keeping malicious spam out of consumers' inboxes;
- identifies best practices for legitimate email marketers; and finally
- establishes a plan that stakeholders can quickly implement to reduce the deleterious effects of spambots and malicious spam.

The risk that malicious spam will erode confidence in the Internet's benefits to consumers and the global economy is too great to ignore, and we must continue to act quickly to address it. As Commissioner Orson Swindle said at our last Spam Forum in 2003, we must all work together to solve the spam problem. I look forward to the continued development of collaborative initiatives between criminal law enforcement, international bodies, and private industry to combat the proliferation of spambots and the spread of malware via spam.

Again, I welcome you, and I thank you, and now I will turn the workshop over to the first panel. Thank you very much.