A CAN-SPAM Informant Reward System

A Report To Congress

Federal Trade Commission
September 2004

A CAN-SPAM Informant Reward System: A Report to Congress

September 2004

Federal Trade Commission

Deborah Platt Majoras, Chairman
Orson Swindle, Commissioner
Thomas B. Leary, Commissioner
Pamela Jones Harbour, Commissioner
Jon Leibowitz, Commissioner

Table of Contents

Executive Summary

The Federal Trade Commission ("FTC" or "the Commission") submits this report pursuant to Section 11(1) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act" or "the Act"), 15 U.S.C. § 7701 et seq. (2003), which requires the Commission to prepare a report that sets forth a system for rewarding those who supply information about violations of the Act. In this report, the Commission examines the key issues that it believes should be considered in setting forth a reward system. The Commission then goes on to recommend the features or elements that a potentially effective reward system would need to incorporate, should Congress determine to implement one.

The Commission's views on a reward system are strongly influenced by its experience with the anti-spam enforcement program it has been conducting for several years under the FTC Act, before passage of the CAN-SPAM Act. Its views are also based on information gathered by several means:

- interviewing 47 individuals representing 37 organizations, including Internet Service Providers ("ISPs"), Email Service Providers ("ESPs"), spam-fighting organizations, law enforcement agencies, private attorneys with anti-spam litigation experience, federal government agencies that operate reward systems, technologists, and academics;
- requiring the seven ISPs that collectively control over 50 percent of the market for consumer email accounts to provide detailed information about their experiences with spam;
- soliciting public comments through an Advance Notice of Proposed Rulemaking concerning the CAN-SPAM Act rules and reports; and
- retaining the services of two experts, one an expert on electronic commerce law who is a published authority on federal reward schemes, and the other a computer scientist with special expertise in network security issues and applied cryptology.

In considering the possibility of a reward system under the CAN-SPAM Act, the Commission has focused chiefly on how such a system could be designed to facilitate clearing the hurdles in the cases it pursues as part of its anti-spam law enforcement efforts. Because the CAN-SPAM Act became effective on January 1, 2004, too little time has passed to amass a track record on enforcement of the Act. Nevertheless, the FTC's anti-spam law enforcement prior to the CAN-SPAM

Act, undertaken under Sections 5 and 13(b) of the FTC Act, suggests that three significant hurdles facing the Commission in spam cases are: (1) to identify the source of the spam; (2) to develop the evidence needed to prove the individual defendant's participation in, or knowledge and control of, corporate spamming activity, sufficient to prove such person liable; and (3) to obtain a monetary award.[1]

Against this backdrop, the Commission's analysis of reward system issues first addresses the question of how a reward system might improve enforcement of the CAN-SPAM Act. In other words, how could it assist the Commission in clearing the hurdles, mentioned above, that are common to enforcement actions targeting spam? If a reward system could facilitate the Commission's task of obtaining the evidence necessary to support cases, it is likely that such a system could improve the effectiveness of CAN-SPAM enforcement. Such evidence would likely focus on the violations of only certain provisions of the CAN-SPAM Act that are directed at a spammer's attempt to conceal his or her identity, such as the prohibitions on using false or misleading transmission information, deceptive subject lines, and open relays. The violation of such provisions involves an inherent element of falsity and deception, and the violators of such provisions often are the most egregious spammers. Such evidence would also facilitate the Commission's task of identifying and locating individuals responsible for specific spam campaigns, and would demonstrate their direct participation in, or their control and knowledge of, corporate activity violating the CAN-SPAM Act.

The second issue in the Commission's analysis is who are the individuals most likely to be in a position to supply this information to the Commission? The Commission believes persons most likely to possess such "high-value" information are insiders or potential "whistleblowers" – personal or business associates of spammers. The Commission does not believe that the vast majority of consumers who are now forwarding 300,000 pieces of spam daily to the FTC spam database are likely to be a good source for such information. Nor does it believe that persons with above-average skills and knowledge relating to Internet technology – the legions of so-called "cybersleuths" that advocates of a bounty system envisioned – are likely to be a good source of such information.

1. In cases under Sections 5 and 13(b) of the FTC Act, the Commission seeks monetary awards for consumer restitution (when injured consumers can be identified and located, and distribution of the funds to them is otherwise practicable) or disgorgement of revenues the defendants have earned by violating the law. Under the CAN-SPAM Act, the Commission would also be empowered to seek monetary civil penalties of up to $11,000 per violation.

Cybersleuths may be able to employ their sometimes considerable talents and expertise to construct educated guesses linking seemingly unrelated spam to a common source. For example, even absent subpoena power, it is sometimes possible to identify similarities in factual patterns found in spam messages, websites, and header information. However, much of this sleuthing is based on intuition or other inadmissible perceptions, does not definitively identify the spammer, and would not constitute admissible evidence in an enforcement action. The Commission believes that, lacking subpoena power, cybersleuths cannot obtain and supply to the Commission admissible evidence of a spammer's identity, whereabouts, or level of illegal activity. Insiders are the only parties privy to this information, and would not need compulsory process to obtain it.

The third factor in the Commission's analysis is an assessment of the likely incentives and counter-incentives that would influence potential insider informants' decisions to provide high-value information to the FTC. A major factor relevant to this calculus is whether available rewards could be offered at a sufficiently high dollar amount to make it worthwhile for an insider informant to come forward. Put another way, how much cash would be enough to overcome potentially powerful disincentives that weigh against coming forward? These disincentives include such considerations as: uncertainty over whether information submitted actually will be used by the government, and if so, whether that use will result in a successful legal proceeding; fear of losing a lucrative stream of income; fear of incurring personal legal liability for his or her part in the targeted scheme; and fear of loss of anonymity, perhaps resulting in personal retaliation. The Commission is unable to establish with any degree of certainty the dollar amount that might be high enough to overcome these countervailing considerations, but believes that reward amounts in the range of $100,000, and in some cases as much as $250,000, are reasonable estimates.

The fourth aspect of the Commission's analysis is whether the benefits of improved enforcement likely outweigh the costs of establishing and maintaining a reward system. To the extent a reward system is successfully designed to encourage insiders to come forward with high-value information, the enforcement value of such information could be quite significant. The information could lead to faster, more effective, and more numerous law enforcement actions, creating an enhanced deterrent effect. However, to the extent an insider has "unclean hands" and faces potential legal liability, it is questionable whether such a person would

be willing to assume the significant personal risk of coming forward. Thus, the benefits of a reward system remain unclear.

The potential costs of a reward system include those associated with processing incoming information, determining and resolving eligibility issues, defending against lawsuits based on unsatisfied eligibility claims, maintaining internal agency procedures to track and monitor the sources of information utilized by attorneys in bringing cases, obtaining technology necessary to create a reward system database in conjunction with or separate from the FTC's existing Consumer Sentinel database, and conducting public education campaigns to publicize the reward system. Taken together, these costs could be significant.

Based on this analysis, the Commission recommends that if Congress determines to require a reward system, the system should incorporate the following elements:

- to make recovery of a reward more certain, and thus, enhance the incentives of insiders to come forward with high-value information, eligibility should be tied to imposition of a final court order, rather than to collection of civil penalties;
- to insure rewards of a sufficiently high dollar amount, reward payments should be funded through appropriations, rather than based on collected civil penalties;
- to minimize administrative costs and to discourage reward claimants possessing only low-value information, eligibility for rewards should be targeted at persons with high-value information – e.g., proof of a spammer's violation of the CAN-SPAM provisions that involve an inherent level of deception, such as falsifying header information;
- to minimize claimant eligibility disputes and attendant costs, reward determinations should be wholly within the FTC's discretion and not subject to administrative or judicial review; and
- the reward amounts should be high enough to encourage insiders to provide high-value information.

While including these elements may not guarantee that a reward system will achieve its purpose, the FTC believes that absent these elements, any reward system would likely fail.

In addition to the above essential elements, Congress may wish to consider additional specifications, if it determines to go forward with a reward system:

- to discourage "disinformation," it should be specified that it is unlawful to provide false information in connection with the reward system;
- to dispel fear of exposure leading to loss of income or retribution, informants' identities should be protected, allowing them to remain anonymous whenever testimony is not necessary for case prosecution; and
- to preclude misunderstandings and pointless haggling with potential informants, it should be explicitly stated that the FTC cannot grant immunity.

The Commission believes that a poorly designed reward system without the elements described above would not only fail to achieve its purpose – that is, improved CAN-SPAM enforcement – but also result in significant costs to the Commission. The Commission thus proposes that careful consideration be given to the issues discussed in this Report, should Congress determine to implement a reward system.

Section I: Introduction and Overview

The Federal Trade Commission (the "FTC" or "Commission") submits this Report pursuant to Section 11(1) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act" or "the Act"), 15 U.S.C. § 7701 et seq. (2003), which requires the Commission to prepare a report that sets forth a system for rewarding those who supply information about violations of the Act.[2]

In preparing this Report, the Commission obtained input from a number of individuals and organizations and used a number of information-gathering techniques. First, between January and June 2004, the Commission interviewed over 45 individuals representing 37 organizations, including Internet Service Providers ("ISPs"), Email Service Providers ("ESPs"), spam-fighting organizations, law enforcement agencies, private attorneys with anti-spam litigation experience, federal government agencies that operate reward systems, technologists, and academics.[3]

Second, using its compulsory process powers under Section 6(b) of the FTC Act, 15 U.S.C. § 46(b), the Commission required the seven ISPs that collectively account for over 50 percent of the market share for consumer email accounts to

---

2. Section 11(1) of the CAN-SPAM Act, 15 U.S.C. § 7710(1), provides that:

The Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce--

(1) a report, within 9 months after the date of enactment of this Act [enacted Dec. 16, 2003], that sets forth a system for rewarding those who supply information about violations of this Act, including–

(A) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of this Act to the first person that--

(i) identifies the person in violation of this Act; and

(ii) supplies information that leads to the successful collection of a civil penalty by the Commission; and

(B) procedures to minimize the burden of submitting a complaint to the Commission concerning violations of this Act, including procedures to allow the electronic submission of complaints to the Commission . . . .

3. A complete list of interviewees has been attached to this Report as Appendix 1. Many of these interviews were transcribed by a court reporter, some were untranscribed, and others, at the request of particular interviewees, were conducted in confidence.

Citations to the interview transcripts identify the organization, representative from the organization, and page number of the transcript. For instance, the citation "Google: McLaughlin, 14" would refer to a statement made by Google employee Andrew McLaughlin on page 14 of the transcript.

provide detailed information concerning their experiences with spam.[4] The 6(b) Orders were issued to gather information for various purposes, including the Commission's Report on a National Do Not Email Registry ("Registry Report"), which was submitted to Congress on June 15, 2004.[5] The 6(b) Orders requested, among other things, data concerning the volume and types of spam hitting these companies' mail servers and being delivered to their subscribers' inboxes, and detailed information regarding their enforcement efforts.

Third, the Commission solicited comments from the general public in a March 11, 2004 Advance Notice of Proposed Rulemaking concerning CAN-SPAM Act rules (the "ANPR"). The Commission received 132 comments specifically addressing the reward system.[6]

Some of the parties interviewed submitted written comments. Some supplemented their comments after being interviewed.[7] Finally, to ensure that the Commission's assessment regarding a reward system was well-grounded, the Commission retained the services of two experts. The first, Marsha Ferziger Nagorsky of the University of Chicago Law School, is a published authority on federal reward schemes[8] and an expert on electronic commerce law.[9] Ms.

---

4. The Commission issued 6(b) Orders to America Online, Comcast, EarthLink, Microsoft, MCI, United Online, and Yahoo!. To ensure that their anti-spam techniques do not become known to spammers, the ISPs have requested confidential treatment of their 6(b) Order responses. When possible, the Commission has aggregated data from these responses. When the Commission relies on a 6(b) Order response from a particular ISP, this Report does not identify the particular ISP.

5. Part III of the Commission's Registry Report, submitted to Congress pursuant to Section 9 of the CAN-SPAM Act, 15 U.S.C. § 7708, is attached to this Report as Appendix 2. It sets forth a detailed and concise explanation of how the email system works, and how it enables spam by permitting the sending of unauthenticated messages. The Report can also be found online at http://www.ftc.gov/reports/dneregistry/report.pdf. Citations to the Registry Report include the report section and page numbers; for example, the citation "Registry Report: III.A. 2, 6-8" refers to Part III, Section A.2 of the Registry Report at pages 6-8.

6. Citations to the ANPR comments identify the organization or person submitting the comment and the page number of the comment. For instance, the citation "DMA-Comment, 3" refers to page 3 of the comment submitted by the Direct Marketing Association. The Commission has posted the comments online at http://www.ftc.gov/os/comments/canspam/index.htm. The ANPR can be found at 69 Fed. Reg. 11776 (Mar. 11, 2004).

7. Citations to these written submissions identify the organization, representative from the organization, and page number of the comment. For instance, the citation "AOL: Curran, 2" would refer to a statement made on page 2 of America Online's written submission, provided by AOL employee Charles Curran. The written submissions are available online at http://www.ftc.gov/reports/rewardsys/comments.pdf.

8. Ms. Nagorsky is co-author of a leading law review article and comparative analysis of federal reward schemes: Marsha J. Ferziger and Daniel G. Currell, *Snitching for Dollars: The Economics and Public Policy of Federal Civil Bounty Programs*, U. Ill. L. Rev. 1141 (1999). In that article, Nagorsky and Currell create a useful framework through which federal reward schemes can be analyzed, elucidating incentives and motives underlying agency-informant interactions throughout the reward process.

9. Ms. Nagorsky is Lecturer in Law and Director of Internal Communications at the University of Chicago Law School.

Nagorsky conducted an independent appraisal of the issues surrounding a possible FTC reward system, and her assessments and recommendations provide an unbiased view of the challenges involved in creating an effective reward system.[10]

The second expert the Commission consulted is Dr. Dan Boneh of Stanford University. Dr. Boneh is a computer scientist with special expertise in network security issues and applied cryptology.[11] He has prepared a report explaining in detail the present technological difficulties of tracing spam to its source, particularly in cases where spammers deliberately employ techniques to conceal the electronic origins of their spam.[12]

Section II of this Report begins by briefly describing the difficulties of tracing spam[13] and the key challenges to law enforcement. This background information is useful in identifying the kinds of information that the FTC believes would be most valuable to enforcement efforts, and that a reward system should therefore aim to elicit. A more detailed discussion of the email system, its vulnerabilities to spammers, and spammers' exploitation of these vulnerabilities is set forth in the Registry Report excerpt attached here as Appendix 2. Section III discusses the key issues considered by the FTC in setting forth a reward system as described in this Report, and in assessing its likely effectiveness. These issues include: how a reward system could be designed to improve enforcement of the CAN-SPAM Act; who the potential reward informants are and the kinds of incentives and counter-incentives that might influence such individuals; and whether and how the benefits of improved enforcement could outweigh the costs of creating and maintaining such a reward system. Drawing upon this analysis, Section IV identifies certain elements that the FTC believes would be essential or important to the potential effectiveness and success of a reward system, should Congress decide that one

---

10. Ms. Nagorsky's expert report ("Nagorsky Report") is available online at http://www.ftc.gov/reports/rewardsys/expertrpt_nagorsky.pdf. Citations to the report reference the report and the page number, e.g., "Nagorsky Report, 2."

11. Dr. Boneh is an Associate Professor of Computer Science and Electrical Engineering at Stanford University. His research primarily concerns applied cryptology and network security, and he directs Stanford University's Applied Cryptology Laboratory. Dr. Boneh has written over 60 articles in the field of computer security.

12. Dr. Boneh's expert report ("Boneh Report") is available online at http://www.ftc.gov/reports/rewardsys/expertrpt_boneh.pdf. Citations to the report reference the report and the page number, e.g., "Boneh Report, 4."

13. Because Section 11(1) of the CAN-SPAM Act provides that the Commission report set forth a system for rewarding those who supply information about *violations* of the Act, for purposes of this Report, "spam" refers to unsolicited commercial electronic mail messages that do not comply with the CAN-SPAM Act.

should be implemented. Finally, Section V describes procedures to minimize the burden of submitting a complaint concerning violations of the CAN-SPAM Act to the FTC.

Section II: Investigating Spam: The Major Challenges For Law Enforcement

The FTC is pursuing a vigorous law enforcement program against spam. To date, the Commission has brought 63 cases in which spam was an integral element of the alleged deceptive or unfair practice.[14] The Commission's experience shows that there are several major challenges to successfully investigating and prosecuting spammers. Based on its own enforcement experience and that of other law enforcement agencies, as well as the anti-spam litigation experience of ISPs, the Commission has identified three hurdles that any law enforcement investigation and action against spam must overcome. Understanding these hurdles is critical to assessing the capacity of a reward system to contribute meaningfully to the nation's efforts to combat spam.

A. Tracing and Identifying the Spammer

The single greatest challenge for anti-spam law enforcement is to identify and locate the source of a particular spam campaign.[15] Finding the wrongdoer is an important aspect of all law enforcement efforts, but in spam cases it is a particularly daunting task. Because the present email system lacks any mechanism requiring that a sender's identity be authenticated, spammers can and do conceal their identities with ease. Part III of the Commission's Registry Report describes in detail how the open structure of the email system facilitates the proliferation of spam. This characteristic of the email system makes it possible, indeed cost efficient, for spammers to send email messages to millions of email accounts worldwide, while allowing them to hide their identities and

---

14. Most of these cases were filed before the CAN-SPAM Act became law, and therefore were brought under Section 5 of the FTC Act, 15 U.S.C. § 45.

15. *See, e.g.*, EarthLink: Baker, 25-26; Federal Bureau of Investigation, Internet Crime Complaint Center ("FBI-IC3"): Larkin; Microsoft: Cranton, 4; Microsoft-Comment, 16; New York Office of Attorney General ("NYOAG"): Kline; United Online: Squire, 5-8; Virginia Office of Attorney General ("VAOAG"): McGuire, 5-11, 37, 63-68; Washington Office of Attorney General ("WAOAG"): Selis, 15-16; Wellborn Firm: Wellborn, 14, 16-17, 44. *See also* America Online ("AOL"): Curran, 1; Internet Commerce Coalition ("ICC"): Halpert, 2-3; Washington Association of Internet Service Providers ("WAISP"): Kendall, 1-2.

the origins of their email messages. As long as there is no standard method for authenticating the sender's identity, law enforcers will continue to face formidable difficulties in tracing spam.

Currently, there are two main paths that a spam investigation may follow to seek the origin of the spam and the spammer's identity and location. The first is to follow the electronic trail, attempting to trace the spam through the information in the email header back to the spam's point of origin.[16] As explained below, this approach is rarely successful because spammers routinely employ elaborate obfuscatory techniques to avoid being identified. The second path is to follow the money trail. It typically starts by focusing on the spam's "call to action," which is the part of the body of the email message that urges the recipient to do something. Typically, the call to action is a hyperlink that, if clicked, will take the spam recipient to a website where he or she purportedly may purchase a good or service.[17] As explained below, with tenacious effort, this investigatory approach may eventually lead to the person(s) responsible for the spam.

1. The Difficulties of Following the Electronic Trail

Following the electronic trail of the spammer to try to trace the email message back to its original computer source is difficult and often impossible. Spammers routinely employ a variety of obfuscation techniques to conceal the source of their email.[18] Through combining these techniques and developing new ones in a "cat and mouse" pattern, spammers can usually circumvent even the most sophisticated technological tracking techniques. Although there is no definitive study identifying the percentage of email that is currently untraceable, many industry experts have estimated – based on a variety of different sources and methodologies – that as much as 90 percent of spam is untraceable.[19]

16. For a detailed description of headers and how they record certain information about the path an email message has taken from the sender's computer to the recipient's computer, *see* Registry Report: III.A.2, 6-8 (entitled "Email Headers"). *See also* Boneh Report, 2-4, 7-9 for background on headers, and 10-16 for electronic analysis techniques.

17. Obviously this approach is appropriate only for unsolicited email messages that are commercial in nature. Spam that does not seek to promote a good or service – *e.g.*, certain pranks or virus-spreading spam – generally does not include a "call to action" that can be used to trace the origin of the spam.

18. Boneh Report, 2-10. *See also* AOL: Curran, 1 ("Spam outlaws typically use multiple levels of falsification in both their email operations and the financial aspects of their business operations."); FBI-IC3: Larkin; United Online: Squire, 15; VAOAG: McGuire, 11; WAISP: Kendall, 1-2.

19. *See* Dr. Boneh's discussion of various industry estimates, and his opinion as to why these estimates appear to be sound. Boneh Report, 11, Attachment B. For example, Paul Wood, Chief Information Analyst at MessageLabs, estimates that 60 to 70 percent of all spam is sent through zombie drones serving as open

continued...

As the Boneh Report explains in detail, spammers use numerous techniques to conceal their identities. Below is a brief description of some of these techniques.[20]

Spoofing: "Spoofing" refers to the falsification of email header information. This technique disguises an email to make it appear to come from an address other than the one from which it actually came. Not only can a spammer send out millions of spoofed messages, but any bounced messages – messages returned as undeliverable – will flow to the person whose address was spoofed rather than to the spammer. As a result, an innocent email user's inbox may become flooded with angry, reactive email, and the innocent user's Internet service may be shut off due to the volume of complaints.

Open Relays: An open relay is an unprotected, or "unsecured," email server that is configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties. By routing their email through open relays of other organizations, spammers disguise the origins of their email. For example, if a spammer located in the United States sends email through an open relay in China, the email may appear to have come from China.[21]

Open Proxies: Most organizations have multiple computers on their networks, but have a smaller number of proxy servers that are the only machines on the network that directly interact with the Internet. If a proxy is configured improperly in a way that permits unauthorized Internet users to connect through it to other hosts (computers that control communications in a network or administer databases) on the Internet, it is considered to be "open." Such misconfigurations can arise through setup errors by administrators, unforeseen effects of seemingly unrelated systems changes, or outside forces such as trojans or worms. This kind of proxy misconfiguration is common and results in general purpose forwarding that is utilized by hackers and spammers. For example, a spammer can send

---

proxies. Paul Wood, *Anyone for Spam?* British Computer Society Review 2004, *available at* http://www.bcs.org/review04/articles/itsecurity/spam.htm. *See infra*, this Section, for a definition of "zombie drones." Likewise, Brightmail estimated in testimony before the U.S. Senate Committee on Commerce, Science and Transportation that 90 percent of the email that it analyzed was untraceable. http://commerce.senate.gov/pdf/salem052103.pdf. Ted Leonsis of AOL testified that 80 percent of spam was being sent via zombie drones. "Unsolicited Commercial Email" testimony before U.S. Senate Committee on Commerce, Science and Transportation (May 20, 2004) (Statement of Ted Leonsis, Vice Chairman, America Online, Inc.).

20. *See* Boneh Report, 4-9; Edelman, 42-46.

21. *See* Boneh Report, 7-9; *see also* FTC Facts for Business, *Securing Your Server: Shut the Door on Spam* (Jan. 2004), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/secureyourserver.pdf.

email through an open proxy as an intermediate step before routing the message to the recipient's email server. The headers for messages that pass through an open proxy indicate the proxy's Internet Protocol ("IP") address in the "Received: from" line, and not the true originating IP address. In this way, open proxies provide another means for spammers to hide their tracks. Spammers sometimes route their messages through a series of open proxies, referred to as a "proxy chain."[22]

Zombie Drones and Bot Networks: A "zombie drone" is a computer on which email server or proxy software has been downloaded which, without the knowledge of the computer owner, causes the computer to spew out spam or to serve as a relay or proxy for spam. A "bot network" consists of a large number of zombie drones controlled by the same entity. Some observers report bot networks with as many as 400,000 drones.[23] When each drone in the network is instructed to generate or relay spam, the aggregate spam generation rate can be very large.[24]

Untraceable Internet Connections: There are several ways for people to access the Internet through a network address that cannot be linked to an individual or a physical location. Users who connect to the Internet through public Internet cafes, through free (or stolen) Wireless Fidelity ("WiFi") connections, or through certain universities' on-campus networks need not identify themselves and can therefore send messages anonymously on the Internet. Spammers may also purchase ISP roaming access using false names and untraceable payment methods.[25]

Pursuing those who use these techniques to hide their identities and locations is a formidable task. Doing so requires extensive use of the Commission's compulsory process to compel various third parties, such as ISPs, ESPs, services that register IP addresses and domain names, or web hosting companies, to

---

22. *See* Boneh Report, 6-7, Attachment A; *see also* FTC Facts for Business, *Securing Your Server: Shut the Door on Spam* (Jan. 2004), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/secureyourserver.pdf.

23. Boneh Report, 5, citing Laurianne McLaughlin, *Bot Software Spreads, Causes New Worries*, IEEE Distributed Systems Online 1541-4922, 5(6) (June, 2004), *available at* http://csdl.computer.org/comp/mags/ds/2004/06/o6001.pdf (quoting Alfred Huger, senior director of Symantec's Security Response team).

24. *See* Boneh Report, 5-6. For more on bot networks and zombie drones that promulgate spam, *see* Jeff Gelles, *Consumer Watch: Next Big Step in Thwarting Spammers*, Philadelphia Inquirer, June 16, 2004, at C01; Saul Hansell, *Spammers Can Run But They Can't Hide*, N.Y. Times, Nov. 9, 2003, at C1; Frank Hayes, *ISPs' Spam Fight*, Computerworld (Mar. 15, 2004), *available at* http://www.computerworld.com/printthis/2004/0,4814,91182,00.html.

25. Boneh Report, 9.

disclose information about their customers. Indeed, it is not uncommon for the FTC to issue successively in a single case dozens of administrative subpoenas, known as civil investigative demands ("CIDs"), to trace the electronic origins of the spam, or to even simply link seemingly unrelated spam campaigns to a common source.[26] Even so, attempting to track spammers through the electronic trail is most often unsuccessful, unless the spammer is an amateur or incompetent in the use of the obfuscatory techniques described above.[27]

Other law enforcement agencies,[28] as well as all the major ISPs with whom we consulted[29] – many of whom have significant anti-spam litigation programs of their own – agree that identifying the spammer may be the single greatest challenge in spam litigation. Even after employing their substantial technological expertise in analyzing large volumes of spam data, ISPs' collective experience shows that following the electronic trail alone is typically insufficient to identify the spammer.

2. The Difficulties of Following the Money Trail

The more effective investigative technique to identify spammers has been the approach of "following the money." This approach is more successful because behind many fraudulent spam schemes there is a person who ultimately benefits financially from the transmission of spam.[30] This technique follows the

---

26. By contrast, in a typical FTC telemarketing fraud case, the Commission can frequently identify culpable parties and gather sufficient evidence to warrant filing a complaint and seek a temporary restraining order without issuing a single CID, or by issuing only a single CID to a telephone or shipping company.

27. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2702-03, further complicates Commission spam investigations by limiting the types of information that the Commission can obtain from providers of electronic communication services or remote computing services, such as ISPs. Under ECPA, the Commission can issue a CID seeking six types of information to a domain hosting an email account that was used to send spam: (1) name of the email account holder; (2) address of the account holder; (3) records of session times and durations; (4) length of service and types of service utilized; (5) subscriber number or identity, including any temporarily assigned network (IP) address; and (6) means and source of payment for services. 18 U.S.C. § 2703(c)(2). While the name and address of an account holder may often be false, the account holder's IP address and payment records frequently provide useful investigative leads. However, the Commission cannot compel information about the volume of email sent from an email account nor can it compel copies of complaints the ISP received about the email account holder. Further, compelling copies of email in the spammer's email account is difficult because of various court decisions interpreting ECPA. *See Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003) (as amended Feb. 17, 2004).

28. FBI-IC3: Larkin; NYOAG: Kline; VAOAG: McGuire, 9-10, 63-68; WAOAG: Selis, 15-16.

29. EarthLink: Baker, 25-26; Microsoft: Cranton, 4; Microsoft-Comment, 16; United Online: Squire, 5-8; Wellborn Firm: Wellborn, 14, 16-17, 44. *See also* AOL: Curran, 1; ICC: Halpert, 2-3; WAISP: Kendall, 1-2.

30. *See*, *e.g.*, Wellborn Firm: Wellborn, 37-38; Saul Hansell, *Detectives Get Into War On Spam*, N.Y. Times, May 31, 2004; Confidential 6(b) response; Sorkin, 45.

trail of money to that person, and then to the spammer with whom that person is associated. In many cases, a kernel of information can be found in the email message linking the sender to the product being offered. An illuminating account of how this was done in one FTC case is found in the Court's Opinion and order granting a preliminary injunction in *FTC v. Phoenix Avatar, LLC*.[31]

Nevertheless, there are limits to what can be accomplished by following the money. Spammers often use novel payment methods, cash transactions, multiple layers of payment processors, stolen credit card accounts, and other techniques that make tracing the flow of money a painstaking, and sometimes futile, endeavor.[32] In any case, just as in attempting to follow the electronic trail, following the money relies very heavily on the use of compulsory process.[33] For example, without compulsory process, the Commission is often unable to obtain essential information about an investigative target's financial transactions from third parties, such as banks, credit card processors, and other payment processors.[34]

B. Proving the Individual Liability of the Spammer

Even when the FTC successfully identifies an entity sending deceptive spam, determining the individual liable for the law violations, and developing admissible evidence that proves such liability, present additional obstacles to enforcement. In the FTC's experience, fraud targets in general, including spammers, typically distance themselves from the illegal activity at the heart of the scam to make it difficult to prove the individual defendant's involvement. A critical issue in virtually every fraud case is to prove the individual defendant's level of involvement in the scheme – be it in the form of direct or indirect participation in, or knowledge and control of – the illegal activity conducted through one or more corporations.

---

31. *FTC v. Phoenix Avatar, LLC*, No. 04-C-2897 (N.D. Ill. July 30, 2004).

32. *See*, *e.g.*, NYOAG: Kline; VAOAG: McGuire, 6-10, 61-62; Wellborn Firm: Wellborn, 38.

33. *See* NYOAG: Kline; SpamCop: Haight, 37; Spamhaus: Brower, 61; Spamhaus: Reid, 63; VAOAG: McGuire, 10-11; WAOAG: Selis, 15-16; Wellborn Firm: Wellborn, 16-17, 38.

34. It is not uncommon for spammers to use offshore payment processors and banks, beyond easy reach of the FTC's compulsory process, which makes the Commission's task even harder. Legislation currently pending in the Senate and House of Representatives would help the FTC reach offshore payment processors and banks in several ways, including by broadening reciprocal information sharing, expanding cross-border investigative cooperation (including use of compulsory process), and providing for international agreements to accomplish these goals when necessary. S. 1234, 108th Cong., (2003); H.R. 4996, 108th Cong., (2004).

The Commission has two basic avenues available for enforcement of the CAN-SPAM Act, and each involves proof of some level of knowledge on the part of an individual defendant. Following one approach, the Commission may, by referral to the Department of Justice, initiate an action for civil penalties of up to $11,000 per violation.[35] Under this approach, the Commission must prove, among other things, that the defendant possessed "actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by [the Act]."[36]

Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), provides the Commission with an alternative avenue of enforcement, authorizing it to seek equitable remedies for violations of any law it enforces, including the CAN-SPAM Act. These remedies include disgorgement of unjust enrichment or restitution to injured consumers (but not civil penalties, which is a legal, as distinguished from equitable, remedy).[37] In a Section 13(b) action, the Commission also generally must prove, among other things, that an individual defendant either directly or indirectly participated in the law violations that caused the consumer injury, or controlled one or more corporations that caused the injury and possessed some level of knowledge of the corporate wrongdoing.[38]

Typically, targets in Section 13(b) enforcement actions are sophisticated and adept at distancing themselves from their schemes in such a way that proving knowledge is not easy. Spammers appear to fit the profile of the typical FTC fraud defendant. For example, some spammers employ a decentralized network of persons to perpetrate their unlawful activities.[39] The network encompasses

---

35. 15 U.S.C. § 45(m)(1)(A); Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461; 16 C.F.R. § 1.98. Violations of the CAN-SPAM Act are treated as though they were violations of an FTC Trade Regulation Rule promulgated under Section 18(a)(1)(B) of the FTC Act, 15 U.S.C. § 57a(a)(1)(B). 15 U.S.C. § 7706(a).

36. In an action seeking civil penalties for violations of an FTC Trade Regulation Rule promulgated under 15 U.S.C. § 57a(a)(1)(B), the government must prove knowledge, as quoted in the text. Because the CAN-SPAM Act treats violations of that Act as though they were violations of an FTC Trade Regulation Rule, the same knowledge requirement applies. 15 U.S.C. § 45(m)(1)(A).

37. Civil penalties are a legal remedy. 15 U.S.C. § 45(m). Equitable powers are those flowing from the inherent powers of the federal district court.

38. The Commission must show "actual knowledge, reckless indifference, or an awareness of high probability of fraud along with intentional avoidance of truth." *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 573-75 (7th Cir. 1989).

39. *See*, *e.g.*, AOL: Curran, 1; Internet Research Task Force, Anti-Spam Research Group ("ASRG"): Levine, 51-53; ASRG: Shafranovich, 53; Microsoft: Cranton, 2, 3; NYOAG: Kline; SpamCop: Haight, 38-39; Spamhaus: Murphy, 61-62; Spamhaus: Reid, 25-26, 56-60; United Online: Squire, 13-14, 20-21; WAISP: Kendall, 1-2; Wellborn Firm: Wellborn, 16-23, 44.

not only the seller of the product or service promoted through the spam, but in some cases scores of "affiliates" and "sub-affiliates" participating in an elaborate "incentive" program to drive traffic to the seller's website through spam. There may be compilers and sellers of email address lists and high-volume professional spammers. In either case, there may be web technicians involved in the creation and removal of deceptive websites in real-time, and payment processors of various types. Any of these parties could be liable under CAN-SPAM and/or Section 5 of the FTC Act, depending on the role he or she played and his or her level of involvement. But proving the requisite level of knowledge is an important issue in virtually every instance. Most, if not all, of these parties are sophisticated enough to leave little or no trail of their knowledge.[40]

C. Obtaining and Collecting Civil Penalties or Monetary Judgments

The third important hurdle in anti-spam law enforcement actions lies in obtaining, and successfully collecting, civil penalties or monetary judgments in cases, whether resolved through litigation or stipulation. As discussed in further detail in Sections III and IV below, this point is especially relevant to the issue of whether a reward system that ties the reward to the successful collection of civil penalties will provide a sufficient incentive – in terms of monetary reward amount and certainty of remuneration – to attract informants with valuable information.

1. Civil Penalties in FTC Enforcement Actions

As noted above, violations of the CAN-SPAM Act are treated as though they are violations of an FTC Trade Regulation Rule promulgated under Section 18(a)(1)(B) of the FTC Act, 15 U.S.C. § 57a(a)(1)(B). Thus, the Commission may, by referral to the Department of Justice, initiate an action involving violations of the CAN-SPAM Act for civil penalties of up to $11,000 per violation.[41]

---

40. *See* FBI-IC3; Microsoft: Cranton, 3; NYOAG: Kline; Spamhaus: Murphy, 61-62; Spamhaus: Reid, 56-60; United Online: Squire, 13-14, 20-21; Wellborn Firm: Wellborn, 16-23, 44. For example, frequently one party will have little or no contact with other parties involved in the spammer's scheme. Hence, developing the evidence needed to hold individually liable the "mastermind," or person(s) who financially benefit the most from the scheme, can be extremely difficult.

41. *See supra* fn. 35.

In CAN-SPAM cases involving literally millions of violations, the maximum civil penalties theoretically could be astronomical. In reality, however, the FTC Act directs courts to consider several statutory factors, with respect to the defendant's conduct, that often serve as mitigating considerations in determining the amount of a civil penalty: (1) degree of culpability; (2) history of prior conduct; (3) ability to pay; (4) ability to continue to do business; and (5) other matters as justice may require (*e.g.,* consumer injury, level of ill-gotten gain realized through non-compliance, and deterrence).[42] These factors permit courts a great amount of discretion in assessing civil penalties. In applying these factors to the particular facts of a case, courts generally assess civil penalties that are substantially below the amounts originally sought by the government,[43] and that do not approach the maximum of $11,000 per violation alleged. When cases are actually litigated, the government collects much less, and consent orders settling cases without trial generally reflect the litigation result anticipated by the FTC and the Department of Justice.

In practice, the statutory factors courts look to in assessing civil penalties may work in favor of defendants. Two statutory factors in particular – the defendant's "ability to pay" and "ability to continue to do business," often come into play in favor of defendants. Many spammers have limited assets, or have effectively dissipated or concealed their assets.[44] In assessing civil penalties, courts exercise enormous discretion in weighing the importance of the various statutory factors to the facts of a particular case. Ability to pay can be given decisive weight in the assessment of civil penalties.

2. Disgorgement Awards in FTC Enforcement Actions Targeting Spam Under Sections 5 and 13(b) of the FTC Act

Most of the 63 spam-related cases brought by the FTC predate the CAN-SPAM Act. They were filed in federal district court under Sections 5 and 13(b) of the FTC Act, which permit the FTC to seek and obtain preliminary and permanent injunctive relief to stop violations of any law enforced by the Commission, as well as equitable monetary remedies. Civil penalties are not available to the Commission in Section 13(b) actions.

---

42. 15 U.S.C. § 45(m)(1)(C).

43. Commission internal data.

44. Industry participants share this experience. *See, e.g.*, AOL: Curran, 2: "Based on AOL's experience, only a limited number of outlaw spammers have the sort of wealth or resources that would yield meaningful financial recoveries for whistleblowers . . . ."

In pursuing equitable monetary remedies under Section 13(b), the Commission places priority on obtaining restitution for injured consumers. Where this is not possible, the Commission seeks equitable disgorgement of ill-gotten gains. Final judgments have been entered in 57 of the 63 spam-related cases brought thus far. Most of these 57 cases resulted in monetary judgments where the money was specifically earmarked for consumer restitution. In some cases, when individual injured consumers were difficult to identify, when the amount of injury attributable to the law violation could not be calculated, or when the administration of redress funds to consumers was impracticable, the court judgments permitted such funds originally earmarked for consumer restitution to be paid to the U.S. Treasury under the theory of equitable disgorgement of ill-gotten gains. Should Congress decide to go forward with a reward system under the CAN-SPAM Act, one way to supplement the pool of funds available to pay rewards might be to provide the Commission with authority to use funds collected in CAN-SPAM cases brought under Section 13(b) for this purpose, when it is impracticable to restore the money to injured consumers.[45] However, even in the cases where the Commission pays funds to the U.S. Treasury under the theory of equitable disgorgement of ill-gotten gains, the funds available are often quite modest.

Section III: Key Issues Considered in Setting Forth a Reward System and in Assessing Its Likely Effectiveness

In approaching the task of setting forth a reward system and in assessing the potential effectiveness of such a system, the Commission confronts four primary issues: (1) How would an FTC reward system improve enforcement of the CAN-SPAM Act? (2) Who are the potential informants who could identify CAN-SPAM violators and supply valuable information leading to successful law enforcement actions? (3) What incentives and counter-incentives would likely influence these individuals? And (4) Would the benefits of improved enforcement likely outweigh the costs of establishing and maintaining such a reward system?

---

45. It should be noted that under the Miscellaneous Receipts Act, 31 U.S.C. § 3302, the Commission presently has no authority to retain for its own use any funds it collects when an enforcement action is resolved, whether as civil penalties or as equitable disgorgement. Instead, civil penalties must be deposited with the U.S. Treasury. Any disgorgement funds which are not returned to consumers as redress or used for other equitable relief (such as consumer information remedies) also must be deposited with the U.S. Treasury.

A. How Could a Reward System Improve Enforcement of the CAN-SPAM Act?

Section 11 of the CAN-SPAM Act calls for a report on a reward system that focuses on information that "identifies the person in violation of this Act; and . . . leads to the successful collection of a civil penalty." At present, nearly all of the information the Commission receives, unprompted, from the public – forwarded spam and consumer complaints – shows that a law violation has, or may have, occurred. But if Congress were to establish a reward system that reflects the standard suggested by Section 11, the statutory specification, appropriately, would set the bar much higher: information meriting a reward at a minimum not only must tie the violation to the specific person committing the violation, but also must lead to a successful legal proceeding. The Commission believes it is correct to focus on the type of high-value information that currently is not available to the Commission without expenditure of considerable resources and effort. If a reward system could enable the Commission to obtain more information of this type, it is likely that it could improve the effectiveness of CAN-SPAM enforcement. A reward system makes sense, however, only if it can produce information about spammers more cheaply than the government can.[46]

1. The Nature of the Violation Is a Factor

Some of the numerous provisions of the CAN-SPAM Act address practices that neither involve fraud or deception nor an attempt by the spammer to conceal his or her identity. These provisions include the requirement to include in a commercial email message a valid physical postal address[47] and a clear and conspicuous identification that the message is an advertisement or solicitation.[48] Violations of these types of provisions often are plain on the face of the email. Legitimate companies that market through email and inadvertently stray into these types of violations would be easy for almost anyone to identify.[49] This is because

---

46. Put another way, for a reward system to be worthwhile, the enforcement value of the generated information should exceed its acquisition costs. *See* Ferziger and Currell, *supra* fn. 8, at 1172 ("Because all information imposes administrative costs, an optimal information flow is not a maximal information flow. An optimal information flow consists of a high rate of information that will lead to viable enforcement actions and a relatively low rate of 'static' or 'noise' – information that causes the agency to incur investigative costs but fails to bear out an actionable violation within the agency's jurisdiction.").

47. 15 U.S.C. § 7704(a)(5)(A)(iii).

48. 15 U.S.C. § 7704(a)(5)(A)(i).

49. *See*, *e.g.*, VAOAG: McGuire, 30-31; *cf.* Comerica-Comment, 2; Experian-Comment, 9-10; Reed Elsevier-Comment, 7.

legitimate companies typically do not attempt to hide their identities when sending commercial email. The FTC's existing spam database consists of spam messages consumers forward to the address "spam@uce.gov." The FTC's spam database currently captures data on these types of violations.[50] Because the FTC already has, or could easily obtain, this information, more of it would be of little or no value to the FTC.[51]

By contrast, certain other CAN-SPAM provisions take aim at the very heart of fraudulent spam, such as the prohibitions on using false or misleading transmission information,[52] deceptive subject lines,[53] and open relays.[54] Because these provisions specifically target a spammer's use of obfuscatory techniques to conceal his or her identity, the violation of these provisions involves an inherent level of falsity and deception.[55] Obtaining the evidence needed to prosecute such violators involves a much greater commitment of time, effort, and resources than obtaining evidence of the more easily detected violations of the CAN-SPAM Act. Information, usable in a legal proceeding, that identifies the perpetrators of these types of violations might be high-value, because it would significantly advance an FTC case while saving valuable investigatory resources.

The FTC is concerned that any reward system not encourage an inundation of information that provides evidence of facial violations that the FTC's spam database already receives in abundance, and where the identity of the sender of the email is clear on the face of the spam.[56] Thus, any reward system should be designed to elicit only high-value information.

---

50. Since January 1, 1998, the spam database has received over 140 million pieces of spam. Until July 2004, consumers forwarded spam email to uce@ftc.gov.

51. Of course, it is possible that hard-core spammers also engage in these types of violations. However, in such cases, the FTC does not need additional evidence of the violations. It needs information showing that such high-value targets, who conceal their identities, are responsible for such violations.

52. 15 U.S.C. § 7704(a)(1).

53. 15 U.S.C. § 7704(a)(2).

54. 15 U.S.C. § 7704(b)(3).

55. *See, e.g.,* Wellborn Firm: Wellborn, 19, 41-42, at 41 (on how certain violations, such as a deceptive subject heading or unauthorized use of open relays, involve "an inherent element of falsity and deception").

56. *See* Section III.D.2(a), *infra*, where we discuss the substantial risk that a reward system will generate a high volume of low-value and duplicative information, and that the administrative costs of processing such information could be high.

2. Evidence of an Identified Violator's Knowledge Is Valuable

As described in Section II, a major enforcement challenge for the FTC is developing the evidence necessary to establish the individual liability of the perpetrator of a fraudulent scheme conducted through a corporation. Because spammers often deliberately distance themselves from the underlying illegal act, proving their level of knowledge can be a difficult task. Hence, information that helps establish their level of knowledge is likely to be "high-value" information.

B. Who Are the Potential Informants Who Could Identify CAN-SPAM Violators and Supply Valuable Information Leading to a Successful Law Enforcement Action?

Some potential informants are more likely than others to possess "high-value" information – information identifying the violators and helping to establish their level of knowledge or culpability – that could lead to a successful law enforcement action. There are three possible categories of potential reward informants. First, there are people who receive the spam and report it, but who perform no additional investigatory work themselves and who possess no additional information about the origin of the spam or its senders. Second, there are people who actively try to collect information about spammers on their own. Third, there are people who have actual "insider" information about the spammers, as a result of a past or existing business or personal relationship.

The FTC already receives a vast quantity of information from the first kind of informant; these are the people who file complaints with the FTC Consumer Response Center, or who collectively forward over 300,000 pieces of spam daily to the FTC's spam database. These people take no additional steps to identify the spammer beyond merely forwarding complaints and spam to the FTC. Thus, they generally can neither identify the spammers who deliberately conceal themselves, nor supply information showing the spammers' level of knowledge or culpability. Clearly, an FTC reward system should *not* encourage this category of informant.[57] Were a reward system to encourage this type of informant to seek a reward, the costs of processing leads submitted by these persons would outstrip the meager enforcement value of such leads.

---

57. Although the spam forwarded to this database is extremely valuable to the FTC, its value lies mainly in providing data in the aggregate. For example, it assists the FTC in tracking and analyzing the volume and patterns of certain spam campaigns, and in identifying new trends. However, consumers who forward spam to this database are generally unable to identify the spammers who deliberately conceal themselves. *See* fn. 79, *infra*.

The second type of potential informant is the private individual who expends personal time and effort to track down information about spammers (hereafter referred to as a "cybersleuth"). Proponents of a reward system envisioned "an army of computer geeks who seek out spammers for their and the public's benefit."[58] Indeed, it is this category of persons that Professor Larry Lessig, in first advocating a reward program, was envisioning as private spam investigators.[59] This type of person may possess a high level of technical expertise or personal interest in pursuing spammers.[60] The cybersleuth is often motivated by a desire to fight spam and help make the Internet a clean and legal environment.[61] Many of these cybersleuths already provide useful information to the public for free,[62] and may not be further motivated by the prospect of a monetary reward.[63]

The critical issue is the extent to which cybersleuths can provide the kind of high-value information deemed most useful by the FTC. In fact, cybersleuths can do little to identify spammers who deliberately conceal their identities, or to supply evidence showing a spammer's level of knowledge or culpability in a particular spam campaign, that is likely to be admissible in any enforcement proceeding. Cybersleuths lack subpoena power – a *critical* enforcement tool that is typically required to obtain the kind of evidence that would be admissible

---

58. *See* Senator Corzine's statement on creating incentives for such individuals to track down spammers. 149 Cong. Rec. S. 13012, 13041 (2003).

59. Professor Lessig has referred to this class of persons as "spam-vigilantes." Lawrence Lessig, *A Bounty on Spammers*, CIOInsight (Sept. 16, 2002), *available at* http://www.cioinsight.com/print_article/0,3663,a=31039,00.asp. In an interview with the FTC, Lessig stated that he recommended a reward system only if the CAN-SPAM Act had contained certain features, including an advertising label requirement so that vigilantes could easily identify non-compliant spam.

60. *See*, *e.g.*, Edelman, 42-45; VAOAG: McGuire, 54-56; WAOAG: Selis, 59; Wilson, Sonsini, Goodrich, and Rosati ("WSGR"): Kramer, 34-35.

61. *See*, *e.g.*, ASRG: Levine, 44, 46; Internet Law Group: Praed, 41; SpamCop: Haight, 50; Spamhaus: Brower, 6, 27; Spamhaus: Murphy, 6-7, 10-11; VAOAG: McGuire, 54; WSGR: Kramer, 34-35.

62. *See* sources cited *supra* in fn. 61; *see also* AOL: Curran, 3; United Online: Squire, 10-11, 23-24; WAOAG: Selis, 58. Competition for rewards among individual cybersleuths could possibly have the perverse effect of chilling this activity. *See*, *e.g.*, Spamhaus: Murphy, 83 (anticipating that some people who currently share anti-spam information freely might experience "a potential chilling effect of not wanting to share that information if the information [had] a monetary value that would be lost by sharing it" under a reward system).

63. Another class of potential informants are major ISPs, who have access to a large volume of aggregate spam data, and possess the resources and expertise to process and analyze such data. To the extent the larger ISPs bring private actions against spammers, they also acquire subpoena power. However, these ISPs can and already do provide substantial assistance to law enforcement. *See, e.g.*, VAOAG: McGuire, 21-22; EarthLink: Baker, 51. Moreover, as several large ISPs have indicated in interviews or written comments, they already have strong incentives to assist the FTC in strengthening enforcement efforts, and the prospect of a monetary reward provides them no additional incentive. EarthLink: Cashion, 7; ICC: Halpert, 2; United Online: Squire, 16-18; *see also* ASRG: Levine, 48.

in an enforcement proceeding. As discussed in Section II, identifying hard-core spammers typically requires extensive use of compulsory process. Unless cybersleuths bring private actions on their own, they lack the subpoena power required to elicit information that would identify a spammer. In addition, as the Boneh Report describes in detail, cybersleuths are unlikely to successfully identify the spammer when the various obfuscatory techniques are used to conceal his or her identity.[64] Cybersleuths are also unlikely to possess information regarding a target's knowledge or culpability. Information that helps to establish the spammer's participation in or knowledge of the violative act typically comes from extensive investigation and discovery involving the use of compulsory process. It follows that potential informants who lack subpoena power, and who are not "insiders" possessing personal knowledge of the spammer, are highly unlikely to possess or produce the kind of information deemed most useful to the Commission. Hence, the FTC is dubious that cybersleuths could provide high-value information under a reward system. Many sources with whom the FTC consulted emphasized the importance of subpoena power in effectively investigating and developing legally admissible evidence in prosecuting spammers.[65] As one major ISP stated:

> In our experience, purported links between a spam campaign and a particular spammer – while frequently accurate – are often based on speculation, intuition or other inadmissible perceptions. While such suggestions are helpful in focusing the nature of an investigation, they are not usually definitive and, more importantly, are not based on evidence likely to be admissible in any enforcement proceeding. Indeed, we find that critical admissible evidence is frequently not available without subpoena. That is, the strong and admissible evidence by which a spammer can be identified and prosecuted is often in possession of a third-party (for example, a domain registrar, ISP, hosting company, on-line payment company or affiliate program operator) that is unwilling or unable to provide such information without compulsory process. Thus, such information is equally unavailable to industry experts and "spam watchers," and reports from such entities are unlikely to provide the definitive evidence necessary for prosecution.[66]

---

64. Boneh Report, 10-16.

65. *See* Section II.A, *supra*, on the critical importance of compulsory process. *See also* EarthLink: Baker, 25; Edelman, 43; EarthLink: Cashion, 16, 28; SpamCop: Haight, 32-34; The SpamCon Foundation ("SpamCon"): Atkins, 54; Wellborn Firm: Wellborn, 16-17; United Online: Squire, 8-10.

66. Microsoft-Comment, 16.

Of course, it is possible that a reward system could occasionally generate information that may be useful in helping to focus an FTC investigation. The FTC is not ruling out the possibility that cybersleuths could employ their considerable talents and expertise to construct educated guesses linking seemingly unrelated spam to a common source.[67] For example, even absent subpoena power, it is sometimes possible to identify similarities in factual patterns found in spam messages, websites, and header information. However, as stated by the above-referenced ISP, much of this information is based on intuition or other inadmissible perceptions, does not definitively identify the spammer, and would not constitute admissible evidence in an enforcement action.[68]

Moreover, the FTC is concerned that a reward system that openly invites submissions from the above two classes of informants – ordinary consumers and cybersleuths – would do little to assist the FTC in identifying the largest-scale, worst-offender, hard-core spammers. As one major ISP stated:

> Presently, both ISPs and the FTC must make significant efforts to discern the patterns of spam-related activity by large-scale actors, in order to ensure that their enforcement resources are targeted at the worst actors. The creation of financial incentives for such reporting would create "lottery"-like incentives for reporting of every quantum of evidence relevant to CAN-SPAM enforcement, regardless of the quality of that complaint data, or its materiality to the prosecution of significant CAN-SPAM violations. Moreover, a bounty-driven reporting system might result in an overweighting of investigation of small-scale, "technical" violations of the CAN-SPAM Act by legitimate companies, rather than pursuit of professional spammers using techniques of obfuscation specifically designed to thwart their identification. As a result, investigative resources might be diverted away from enforcement efforts against the largest-scale "outlaw" spammers impacting the greatest numbers of consumers.[69]

---

67. The rationale behind Professor Larry Lessig's proposal of a reward system was to improve enforcement against spammers by tapping into the vast pool of talent and labor offered by cybersleuths or "spam-vigilantes." In fact, it can be thought of as substituting the work of private individuals for that of government employees. Thus, one way of assessing the effectiveness of a reward system is to evaluate to what extent it produces high-value information more cheaply than the government can. As explained above, the Commission does not believe that cybersleuths can provide admissible evidence identifying spammers more cheaply than the government can.

68. Microsoft: Cranton, 4. Some participants also raised the concern that a reward system that seeks to elicit information from the class of persons known as "cybersleuths" could lead to individuals demanding information from ISPs that ISPs are not authorized to provide without a subpoena. ISPs could then be seen as uncooperative, causing consumer backlash.

69. AOL: Curran, 2.

The third kind of informant – people who have inside information about wrongdoers – could be termed "insiders" or "whistleblowers." These persons can include current and former employees or associates with whom the spammer has a business relationship, or family and friends with whom the spammer has a personal relationship. As a result of their relationships with the spammer, these persons would know the spammer's identity, and would be best situated to possess information about the extent of the spammer's unlawful activities. The Commission believes that it is this type of "insider" that forms the most promising class of potential informants under a reward system. Section IV of this Report discusses a reward system designed to encourage this specific category of persons as informants.

C. What Incentives and Counter-Incentives Would Likely Influence Potential Informants' Decisions to Provide High-Value Information to the Commission?

In evaluating the likely success of a reward system, the FTC considered whether a reward system that is tied to the collection of civil penalties, as currently contemplated under the CAN-SPAM Act, would provide a sufficient incentive to induce informants to come forward with high-value information. To create effective incentives for potential informants, the system must promise a sufficiently high certainty of reward, a sufficiently high monetary reward amount, and a relatively low risk of detriment to the informant. As Ms. Nagorsky has written:

> The potential informant's expected bounty payment may be the single most important factor in ensuring optimal disclosures. If the amount is too low, few informants will risk their careers and even their own lives to "do the right thing." In instances where disclosure carries a high risk to the informant (presumably cases in which the alleged wrongdoing is particularly egregious or widespread), an informant is unlikely to come forward in return for only a small reward. If bounties are low, informants might only offer information about low-level crimes. If bounties are high, every potential informant with a crumb of information might crawl out of the woodwork hoping to hit the bounty jackpot. The administrative cost of wading through such a tide of applications might very well exceed the benefit gained from enticing a few risk-averse informants with excellent information on high-level crimes.[70]

70. Ferziger and Currell, *supra* fn. 8, at 1151-52.

Industry sources emphasize the importance of creating a sufficiently high incentive for a reward system to have any prospect of success.[71] It is doubtful that a reward system funded by the recovery of civil penalties could guarantee potential recipients either a sufficiently large award or a sufficiently high level of certainty of receiving it to make it worth their while to come forward with high-value information that could enable the FTC to improve CAN-SPAM enforcement.

Even if monetary incentives were sufficiently certain and large, potential informants, particularly insiders, may still face powerful disincentives for submitting information under a reward system. First, in deciding whether or not to come forward with information under a reward program, informants face, from the outset, substantial uncertainty over whether the information they provide will be acted upon by the FTC and result in a successful law enforcement action. Second, to the extent the most promising class of claimants – insiders – themselves have "unclean hands" and face potential legal liability, they may be unlikely to risk coming forward with useful information, for fear of being investigated and targeted themselves.[72] Given that the FTC has only civil law enforcement authority, it is not in a position to grant immunity from criminal liability. Nor could it promise immunity from liability under any federal or state statutes that the FTC has no authority to enforce. Consequently, it is questionable whether a potential informant would be willing to assume the significant personal risk of coming forward.[73]

Third, an insider informant may also be deterred from helping the government by the prospect of losing a lucrative stream of income. To the extent the informant belongs to the same "underground" cyberworld as the "hard-core" spammer, the lucrative possibilities for engaging in the same type of activity may alone deter such informants from "switching sides."[74] Another powerful disincentive lies in the fear of provoking personal retaliation by the wrongdoer.[75] As Ms. Nagorsky has documented, it appears that in some cases the degree to

---

71. *See* AOL: Curran, 2-3; WAOAG: Selis, 16, 53; NYOAG: Kline; Internet Law Group: Praed, 57-58; Coalition Against Unsolicited Commercial Email ("CAUCE"): Everett-Church, 46, 49.

72. *See*, *e.g.*, WSGR: Kramer, 55-56; Wellborn Firm: Wellborn, 49; Savicom: Bernard, 31; NYOAG: Kline.

73. *See*, *e.g.*, Wellborn Firm: Wellborn, 49 ("[W]ithout some kind of immunity I don't think you would see any of the insiders coming forward . . . ."); Savicom: Bernard, 30-31.

74. *See*, *e.g.*, United Online: Squire, 14; CAUCE: Everett-Church, 46; Word to the Wise: Atkins, 48.

75. *See, e.g.*, Electronic Frontier Foundation ("EFF"): Cohn, 64.

which the government agency can promise anonymity may be an important element in the success of a reward program. In Section IV, we recommend that if a reward system is implemented, it include a specification promising the informant anonymity, unless the informant is required to testify.

Fourth, it is possible that no incentive could be great enough to encourage insiders who have personal relationships with a target to disclose useful information. Frequently, such insiders are friends or family of the target, with whom the target has a longstanding relationship.

It is interesting to note that in the case of the bounty scheme operated by the Securities and Exchange Commission ("SEC"), the SEC has rewarded only three informants since the inception of its bounty scheme in 1988.[76] Insider informants are either already trusted associates, friends or family of the insider trader, with whom the insider trader has a relationship of trust, or they may be implicated in the illegal insider trading activity. These factors are possible reasons for the infrequent use of the SEC bounty scheme.[77]

D. Would Benefits of Improved Enforcement Likely Outweigh the Costs of Establishing and Maintaining a Reward System?

In general, in assessing the viability of a reward system, the overall benefits of a reward system should be weighed against its overall costs. As explained below, there is a significant risk that the costs of a reward program could outweigh the benefits of such a program.

1. The Benefits of a Reward System Are Unclear

To the extent a reward system is successfully designed to encourage insiders to come forward with high-value information, the enforcement value of such information could be quite significant. Indeed, legally admissible information that identifies hard-core spammers who go to great lengths to thwart identification, or that provides evidence of their level of involvement in the illegal activity, could greatly enhance the Commission's enforcement efforts in combatting spam. However, as noted above, to the extent an insider has "unclean hands" and faces potential legal liability, it is questionable whether such a person would be willing

76. Insider Trading and Securities Fraud Enforcement Act of 1988 ("ITSFEA"), 15 U.S.C. § 78; Interview with SEC staff.

77. Nagorsky Report, 10.

to assume the significant personal risk of coming forward. Thus, whether a reward system could lead to improved CAN-SPAM enforcement remains unclear.

A second possible benefit of a reward system is the potential deterrent effect it might have on spammers. Were Congress to implement a reward system that explicitly targeted information of "insiders," those spammers that the FTC is targeting would certainly learn quickly about the reward system. They would be aware that anyone with knowledge of their activities could become a potential informant. It is possible that a higher chance of detection could force some spammers to curtail some of their activity. In this sense, the very existence of a reward system could decrease spam even if no informant ever used it. However, it is also possible that a reward system would simply cause spammers to go further "underground," and become even more devious and sophisticated in their business practices.[78]

2. A Reward System Could Be Costly

A viable reward system would be one in which the value of the incoming information exceeds the total costs of the reward program. The total costs include: (1) costs of processing incoming information; (2) costs associated with determining and resolving eligibility issues, and potential legal costs incurred in defending against eligibility claims; (3) costs of maintaining internal agency procedures to track and monitor the sources of information utilized by attorneys in bringing cases; and (4) other miscellaneous costs, such as the information technology cost of creating a reward system database separate from the FTC's existing Consumer Sentinel database, and conducting consumer education about the reward system.

(a) Costs of Processing Incoming Information

As discussed in Paragraph A of this Section, the FTC has serious concerns that a reward system could generate an overwhelming volume of duplicative and low-value information. At present, the FTC's spam database receives on average over 300,000 copies of spam *daily*.[79] The same consumers who currently are self-motivated to forward complaints to this spam database may be *further* motivated

78. *See also* Nagorsky Report, 28.

79. The data contained in the FTC's spam database is particularly valuable in the aggregate, and assists the FTC in estimating the volume and patterns of spam, and in identifying new trends. It also helps the FTC identify consumer witnesses. However, unlike the case of reward submissions, the cost of processing information in the spam database is manageable because the FTC is under no obligation to analyze every single message it receives on an individual basis.

to submit the same types of complaints/spam by the prospect – however low – of a monetary reward.[80] Even assuming that only one percent of the persons who currently forward spam complaints attempt to do so under a reward system, that would amount to approximately 3,000 reward submissions per day. Industry participants consistently cautioned about the difficulties and costs of processing overwhelming volumes of leads of little or no value.[81]

As one ISP stated:

> [T]he difficulty is frequently not a lack of information, but rather an overwhelming and unmanageable volume of information to which limited investigative resources must be applied. Thus, there is no lack of candidates for enforcement efforts, and it is not particularly important to expand the pool of investigative targets through 'tips' from industry groups or participants.[82]

As another attorney who has represented EarthLink put it, "[I]t's much more of an information filtering exercise than it is an information finding exercise."[83] Currently, the FTC's task is to effectively process those leads it already has, to identify the source of untraceable spam, and to translate those leads into enforcement actions. Significant resources would be required to develop and operate an efficient system to sift through the high volume of "chaff," find the rare kernel that may be a valuable lead,[84] and translate that lead into an enforcement action. Processing costs related to low-value information could be high, and yet yield little high-value information. In such a scenario, establishing and operating a reward program would not enhance the FTC's enforcement efforts, but rather would divert scarce resources away from the investigation and prosecution of cases.[85]

Thus, any reward system should be designed in such a way as to discourage the inflow of low-value information, minimize administrative costs, and reduce

---

80. *See* ASRG: Levine, 45; CAUCE: Everett-Church, 43 (substantial educational hurdle); Piper Rudnick: Plesser, 75. *See also* EFF: Cohn, 70 ("[i]f it looks like a jackpot you're going to get a lot more false and bad information").

81. *See* AOL: Curran, 2; Wellborn Firm: Wellborn, 11-12; EarthLink: Baker, 24; Piper Rudnick: Plesser, 75; Word to the Wise: Atkins, 43; CAUCE: Everett-Church, 43; ICC: Halpert, 2; EFF: Cohn, 69.

82. Microsoft-Comment, 17.

83. Wellborn Firm: Wellborn, 12.

84. *See* AOL: Curran, 2; EFF: Cohn, 67-68; NYOAG: Kline; WAOAG: Selis, 52, 57-58.

85. *See*, *e.g.*, Wellborn Firm: Wellborn, 54-55.

the number of claimant eligibility disputes. One possible way to do this is to tailor the eligibility requirements narrowly.

(b) Costs Associated With Resolving Eligibility Disputes and Defending Against Legal Challenges to Eligibility Determinations

A reward system predictably may result in claimant eligibility disputes. The volume of such disputes is difficult to anticipate, but industry participants consistently warned about the likelihood of multiple claimant eligibility disputes.[86] The costs associated with determining and resolving eligibility claims could be significant. For example, administrative expenditures could include such costs as: (1) explaining to potential claimants why they are not eligible; (2) resolving multiple claimant eligibility disputes; and (3) defending against legal challenges to eligibility determinations.

The cost of simply responding to the claimants – in the form of sending out a Response or Acknowledgment Letter – would likely be considerable, given the large number of consumers who are likely to submit low-value information. In other cases, each of several claimants might have a reasonable belief that he or she is solely entitled to a reward. If Congress were to establish a reward system that follows the language of the CAN-SPAM Act, a claimant who would identify the violator of *any* provision of the Act could be potentially eligible for a reward. Absent a narrowing of the reward eligibility requirements, there is a significant likelihood that there could be multiple claimants providing overlapping and duplicative information regarding the same target.[87] The language of the CAN-SPAM Act appears to contemplate a system that would eliminate the possibility of multiple claimant disputes by limiting eligibility to "the first person" to submit the required information. However, the FTC is concerned that priority in time may not be easy to establish, and that the first informant in the door with information is not necessarily the informant with the information that is useful and leads to a successful case.[88]

As discussed below, in the FTC's view, if there is to be a reward system, it should explicitly target the type of high-value information that "insiders" most likely possess. This, in turn, should reduce the pool of potential claimants to a

---

86. *See* AOL: Curran, 3; EarthLink: Baker, 53 ("you're going to be the one charged with saying, '[s]orry, but somebody beat you to identifying that spammer by nine and a half seconds'"); ICC: Halpert, 2; Piper Rudnick: Plesser, 75; Promotion Marketing Association, Inc. ("PMA")-Comment, 9.

87. *See*, *e.g.*, Spamhaus: Murphy, 73-74; Spamhaus: Reid, 74.

88. *See* Ferziger and Currell, *supra* fn. 8, at 1151.

manageable level. A reward system that invites potential claimants with only low-value information would likely give rise to many disputes over who is entitled to a reward. Such disputes could be costly to resolve on an administrative level, and to the extent they result in litigation, the legal costs incurred in defending against such lawsuits could be quite significant.

(c) Costs of Internally Tracking/Monitoring the Sources of Information Utilized By Attorneys in Bringing Cases

Establishing and maintaining a reward program would necessarily entail setting up an internal system to track and monitor not only the sources of information received by the FTC staff, but also which of those pieces of information are utilized by investigators and attorneys in bringing cases. This would be necessary to enable the Commission to determine whether a claimant was eligible for a reward, and to ensure accountability to the public that the reward system was being fairly operated.

From a practical standpoint, a very likely scenario illustrates the absolute necessity of an effective tracking and monitoring system as part of any reward program. As previously described, many spammers hide their identity, and use multiple and constantly changing product names, websites, IP addresses, payment processors, and related third parties. A search in the FTC's Consumer Sentinel database or spam database conducted under one product name or IP address utilized by a targeted spammer might very well fail to uncover information about the same spammer that is actually entered in the database under a set of different product and company names, websites, or IP addresses associated with the spammer. The FTC could easily find itself in a situation where it investigates and brings an action, based on an informant's evidence about a particular target, only then to receive a claim from another informant for the reward, despite the fact that the FTC never relied on the second informant's evidence. Or the FTC could bring an action, without knowing about or relying upon information earlier provided by an informant about a particular target, only then to receive a claim from the informant for the reward. To prevent these kinds of eligibility disputes from arising, the FTC would need an effective internal tracking and monitoring system. The administrative costs of such a system likely would include the cost of creating a database designed to track the source of information and the time it is obtained, as well as whether and how such information is used by the FTC staff.

(d) Other Miscellaneous or Unforeseen Costs

There are several other potential miscellaneous costs that the FTC at present may not be able to foresee or quantify. Some of these costs could turn out to be relatively minor, others unexpectedly large. For example, costs would certainly be incurred to establish a database for receipt of reward submissions. Regardless of whether such a database is separate from or combined with the existing FTC consumer complaint submission mechanism, the database would need to be designed to capture efficiently not only high-value information most desired by the Commission, but also information necessary for an effective tracking and monitoring program for a reward system. Similarly, it would be necessary to publicize the reward system, both to encourage high-value submissions, and at the same time to minimize consumer confusion between the reward program and the general consumer complaint mechanism. As one industry participant warned, the FTC could face a substantial educational hurdle in trying to teach the average consumer that the reward system is not a general consumer complaint mechanism.[89] To the extent the FTC attempts to discourage the public from submitting low-value information to the reward system, such efforts might inadvertently result in a reduction of consumer complaints forwarded to the general consumer complaint mechanism.

Section IV: Elements of a Reward System

In light of the analysis in the preceding sections of this Report, and after careful consideration of the factors and tradeoffs involved in designing a reward system that could possibly achieve its purpose, the FTC has identified several elements that it believes a reward system, if Congress decides to mandate one, ought to incorporate. These elements are divided into two groups: (1) essential elements of a reward system, without which a reward system is unlikely to be effective or worthwhile ("essential" elements); and (2) elements that the Commission believes merit strong consideration.

89. CAUCE: Everett-Church, 43.

A. Essential Elements of a Reward System

If Congress legislates a reward system, the system should incorporate the following five elements:

- Eligibility should be tied to imposition of a final court order, rather than to the collection of civil penalties.
- Reward payments should be funded through appropriations, rather than based on collected civil penalties.
- Eligibility for rewards should be targeted at persons with high-value information.
- Reward determinations should be wholly within the FTC's discretion and not subject to administrative or judicial review.
- The reward amounts should be high enough to encourage insiders to provide high-value information.

While including these elements may not guarantee that a reward system will achieve its purpose, the FTC believes that absent at least these elements, any reward system would likely fail. Each of these essential elements is discussed in the sections immediately below.

1. Eligibility Should Be Tied to Imposition of a Final Court Order, Rather Than to the Collection of Civil Penalties

First, a reward system should provide sufficient economic incentives for an insider to submit high-value information. As discussed in Section III, a reward system that conditions reward eligibility on the collection of civil penalties is unlikely to create a sufficient incentive for informants with high-value information. To create a higher level of incentive for the informant, reward eligibility could be tied to the imposition of a final court order.[90] For example, reward eligibility could be specifically conditioned on, among other things,[91] the

90. As mentioned earlier, the Commission has two options for enforcing CAN-SPAM violations: (1) it can, by referral to the Department of Justice, initiate cases for civil penalties under Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A); or (2) it can file actions directly in federal district court pursuant to its authority under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), seeking equitable injunctive and monetary relief (and not civil penalties). Because the Commission chooses to bring a large number of cases directly in federal district court pursuant to the latter option, reward eligibility should be broadened to include final court orders obtained in these latter cases as well.

91. As discussed later in Section IV.A.3, reward eligibility should also be narrowed to only claimants who submit certain types of high-value information, not low-value information.

provision of "**information resulting in the imposition of a final court order**," in lieu of "information leading to the collection of civil penalties."[92]

A "final court order" should be interpreted to include court orders obtained as a result of not only litigation and trial, but also negotiated or stipulated settlements, or consent agreements, entered by the court. This is because the vast majority of the FTC's litigation efforts do not result in trial, but instead result in settlements that are filed with and approved by the court.[93] Assuming CAN-SPAM litigation conforms to the pattern established in the Commission's ongoing litigation program under Sections 5 and 13(b) of the FTC Act, a reward system excluding cases resulting in settlements would exclude well over 90 percent of all cases.[94]

2. Reward Payments Should Be Funded Through Appropriations, Rather Than Based on Collected Civil Penalties

It is unlikely that enough civil penalty cases could be brought or that enough funds could be obtained through the imposition of civil penalties in such cases to create a sufficient fund to support a meaningful reward program. While in some cases a reward program that pays rewards out of an agency's recoveries has the clear advantage of being revenue-positive, or "self-funding," the success of such self-funding reward programs depends largely on the generation of sufficiently high revenues from cases. For example, the Internal Revenue Service ("IRS") currently operates a reward system for information regarding the violation of the tax laws.[95] Because the IRS can rely on – and indeed has historically relied on – a high stream of revenues generated by the recovery of unpaid taxes, its reward

---

92. Some federal reward schemes, such as the SEC reward program, tie the reward to the collection of monetary penalties. *See* Nagorsky Report, 7-14. Other federal reward schemes pay informants regardless of whether the agency receives any proceeds. For example, the Department of the Treasury Forfeiture Fund, 31 U.S.C. § 9703, is available to the Secretary of the Treasury for the payment of expenses related to seizures and forfeitures. This fund may be used for payment of "awards for information or assistance leading to a civil or criminal forfeiture involving any Department of the Treasury law enforcement organization participating in the Fund" and "purchases of evidence or information" in a number of situations, including violations relating to money laundering and drug smuggling. The U.S. Customs Service, among other agencies, can pay informants out of the Fund, regardless of whether the agency receives any proceeds.

93. In many of its Section 13(b) actions filed in federal district court, the FTC successfully obtains broad preliminary injunctive relief and an asset freeze against the defendant, thereby making it easier for the FTC to reach a settlement with the defendant.

94. Commission internal data on number of settled cases.

95. *See* IRS Pub. No. 733, Rewards for Information Provided by Individuals to the Internal Revenue Service (1997), and IRS Form 211, Application for Reward for Original Information (2003). The IRS program began in 1967.

program can successfully operate out of these self-generated funds.[96] Similarly, under the federal False Claims Act ("FCA"), rewards are available for those providing information regarding frauds perpetrated upon the government. *See* 31 U.S.C. § 3730 (2004). In FCA cases, private citizens, known as "relators," must initiate litigation against a defrauder. *See* 31 U.S.C. § 3730(b). These rewards typically involve potentially enormous amounts of money, creating an incentive for relators suing on behalf of the government to obtain possibly windfall reward amounts. By contrast, in the case of FTC enforcement actions against spam, the likelihood of generating large enough revenues from such cases – be it in the form of civil penalties or equitable monetary relief – to effectively fund a bounty program is relatively low.[97] As discussed earlier in Section II.C.1, some spammers have limited assets, while others have effectively dissipated or concealed their assets even prior to the commencement of an enforcement action against them.[98] The FTC believes that a reward scheme that creates from the outset an insufficient level of incentive for informants makes little sense, and increases the likelihood that the administrative costs of such a program will exceed its enforcement benefits.

---

96. In the first thirty years of the program, more than seventeen thousand informants "snitched" for the IRS, collectively earning over $35.1 million. *See* Frank Green, *Telling on Cheats: How to Profit by Putting the IRS on the Tax Fraud's Trail*, San Diego Union-Trib., Mar. 29, 1998, at 11. The IRS recovered more than $1.2 billion in unpaid taxes during those 30 years because of the program. *See also* Nagorsky Report, 5-6, 10-12.

97. *See also* discussion in Nagorsky Report, 19. Nagorsky distinguishes between three types of payment systems. The key to determining the appropriate payment scheme depends on the likely results of the agency's enforcement actions. For the FTC, where the likelihood of revenue collection is significantly lower than that of obtaining injunctions, a reward scheme that does not tie payment of the reward to the collection of civil penalties makes sense.

98. Indeed, the most egregious spammers, like other fraud operators, are likely to transfer assets offshore to place them beyond the reach of U.S. courts. *See*, *e.g.*, EarthLink: Cashion, 30-31; Internet Law Group: Praed, 30-31, 47-49. In the FTC's experience, attempting to reach the defendants' offshore funds necessitates a foreign action to enforce a U.S. court judgment. This is time-consuming, expensive, and, in many cases, futile, as many countries do not enforce U.S. court judgments obtained by government agencies. *See, e.g.*, *Evans v. Citibank Ltd. & Others*, Equity Division Proceedings No. 4999 of 1999 (Sup. Ct. New South Wales), where a receiver appointed in an FTC matter, *FTC v. J.K. Publications, Inc*., CV 99-0044 ABC (AJWx) (C.D. Cal. filed Jan. 5, 1999), recently faced difficulties in obtaining relief from an Australian court. In that case, the receiver was not seeking direct enforcement of an FTC judgment, but instead was attempting to use the FTC's judgment as a basis for ordering a third-party bank to transfer certain assets to the control of the receiver under a constructive trust theory. The court held that the receiver's claims were "penal" in nature and denied the receiver's claim.

Similarly, *United States v. Asiatrust Ltd.*, Plaint No. 57/1999, was a case challenging the defendants' transfer of funds to a Cook Islands trust to defeat the FTC's judgment in *FTC v. Affordable Media, LLC*, Civ. No. CV-S-98-669-LDG (RLH) (D. Nev. *filed* Apr. 23, 1998). The High Court of the Cook Islands construed the case (which was pled as a new action) as one involving the enforcement of a penal law. The Cook Islands court dismissed the United States' action, holding that the FTC's action was one to enforce "regulatory rights and powers." "They are or have a flavour of punishment and I conclude that these are at least in part, penal

continued...

3. Eligibility for Rewards Should Be Targeted at Persons with High-Value Information

As discussed in Section III, the FTC believes that the most promising class of informants are "insiders," people who possess knowledge of a spammer's illegal activity. Many industry participants shared this view.[99] Indeed, a reward system would not improve CAN-SPAM enforcement if it were to result in a flood of low-value information, but little or no high-value information. Thus, in designing any reward system, one goal is to encourage disclosure of high-value information by insiders, but not the submission of low-value information.

Section 11 of the CAN-SPAM Act appears to contemplate a reward system under which a reward claimant would be eligible if he or she identifies the violator of any provision of the Act. This would include provisions, the violations of which are obvious on the face of the email, not necessarily rooted in deception or fraud, where the violator does not conceal his or her identity, and which the Commission's spam database already receives in abundance.[100] One possible way to minimize the inflow of such low-value information is to target the reward eligibility requirements more carefully. Only violations of those provisions of the Act which involve an inherent level of deception should be included within the scope of a reward system.[101] Another possible way to target higher value information under a reward system might be to specify that to be eligible for a reward, an informant must provide information relating to a spammer's level of participation in, or knowledge and control of, the fraudulent scheme. But even

---

provisions, and fall within the relevant principle. It is also a public law which is sought to be enforced by the state or the sovereign alone for regulatory purposes and is one which ought not be enforced here." (4 Dec. 2001 Judgment at 8). The matter ultimately was resolved by settlement and the defendants repatriated their assets to the FTC pursuant to a stipulated judgment.

Also, in *FTC v. Zuccarini,* C.A. No. 01-CV-4854 (E.D. Pa., filed Sept. 25, 2001), the FTC obtained a default judgment for disgorgement in the amount of $1.9 million, but the defendant had moved funds to offshore bank accounts in the Bahamas, Australia, and Europe. *See also Impediments to Digital Trade Before the House Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce*, 107th Cong. (2001) (statement of Jeff Kovar, Assistant Legal Advisor for Private International Law, Department of State) ("Most foreign judgments are already recognized and enforced in the U.S. under state law, but most of our trading partners do not usually grant the same treatment to U.S. judgments."). *See also* fn. 34, *supra*.

99. *See*, *e.g.*, AOL: Curran, 1; FBI-IC3: Larkin; Microsoft: Cranton, 3; Microsoft-Comment, 17; NYOAG: Kline; Sorkin: 46; *see also* Spamhaus: Brower, 15-16; Spamhaus: Reid, 13-15.

100. For example, CAN-SPAM requires commercial email to include a valid physical postal address and a clear and conspicuous identification that the message is an advertisement or solicitation. 15 U.S.C. §§ 7704(a)(5)(A)(iii) and 7704(a)(5)(A)(i).

101. *See also* Section III.A.1., *supra*.

with carefully targeted eligibility requirements, it is difficult to control or predict the quality or quantity of information likely to be generated by a reward system.

4. Reward Determinations Should Be Wholly within the FTC's Discretion and Not Subject to Administrative or Judicial Review

As discussed in Section III, one concern about a reward system is the potentially significant cost associated with resolving multiple claimant eligibility disputes, defending legal challenges to eligibility decisions, and potential agency liability arising from eligibility disputes. Given the nature of spam, and the likelihood of multiple claimants forwarding similar information that relates to the same target, the risk that an FTC reward system will generate a large number of multiple claimant eligibility disputes is potentially significant. To minimize this risk, as well as the attendant administrative and legal costs, the Commission strongly recommends that any reward system established by Congress should unambiguously provide the FTC sole discretion in deciding whether, to whom, or in what amount to make payments, and should specify that the Commission's decisions in this regard are final and not subject to judicial review. Absent such a feature, the agency could face an uncertain level of exposure to liability relating to eligibility disputes.[102]

Both the SEC and IRS reward statutes include a provision that the payment of rewards is solely within the agency's discretion and not subject to judicial review. The SEC statute provides that reward decisions – "including whether, to whom, or in what amount to make payments" – shall be "in the sole discretion of the Commission," and shall be "final and not subject to judicial review."[103] Similarly, the IRS reward statute states that "[t]he Secretary . . . is authorized to pay such sums as he deems necessary" for detecting tax fraud.[104] Although the language of the IRS statute is not as explicit, courts have held that that statutory language leaves awards entirely within the discretion of the Commissioner of the IRS.[105]

The IRS and SEC reward systems also disclaim any obligations potentially based on alleged promises made to informants. The SEC's final bounty provision in the Code of Federal Regulations is entitled "No Promises of Payment." Specifically, the SEC states that "[n]o person is authorized under this subpart to

---

102. For a more detailed discussion of potential agency liability, *see* fn. 111, *infra*.

103. 15 U.S.C. § 78u-1(e)(2004).

104. 26 I.R.C. § 7623 (2004).

105. *See, e.g.*, *King v. United States*, 168 F.3d 1307 (Fed. Cir. 1999).

make any offer or promise, or otherwise to bind the Commission with respect to the payment of any bounty or the amount thereof."[106] This language prevents an informant from bargaining with the SEC and later believing his deal will be enforceable. The provision also precludes claimant suits against the SEC. More specifically, under the doctrine of sovereign immunity, the government must specifically waive its right to immunity. Such waiver may occur when an agency signs a contract with an informant memorializing the arrangement between them. By specifically denying that its agents have the power to contract with the informants, the SEC avoids waiver of immunity.[107] Should Congress determine that a reward system should be established, consideration should be given to specifically disclaiming that any obligations based on promises made to informants are binding, thereby making it clear that sovereign immunity is not waived.[108]

5. The Reward Amounts Should Be High Enough to Encourage Insiders to Provide High-Value Information

It is difficult to determine the reward amount that would be high enough to encourage insiders to provide high-value information.[109] There currently is much "lore" about spammers, but little in the way of reliable data.[110] Consequently, little is known about who the illegal spammers are, how much money spammers make from their activities, how much risk an informant would assume in informing on a spammer, and how much monetary (or other) incentive informants need to come forward. Despite the absence of reliable data or knowledge about spammers, it is safe to assume that an "insider" who possesses valuable

106. 17 C.F.R. § 201.68 (2004).

107. For more details about the SEC and IRS statutes, *see* Nagorsky Report, 7-12.

108. Such specifications would hopefully minimize the number of unfounded eligibility claims, and the costs of responding to and defending itself against frivolous lawsuits. Nevertheless, it is possible that, despite the inclusion of such express statutory language, the FTC could still incur significant administrative costs in responding to meritless eligibility claims and disputes.

109. Current federal reward schemes vary a great deal in the amount paid. For example, under the current IRS regulations, the informant is eligible for a reward that will "generally not . . . exceed fifteen percent" of the taxes recovered, and the total reward is not to exceed two million dollars. *See* 26 CFR § 301.7623-1 (2004). Under the SEC reward scheme, a bounty cannot exceed ten percent of the money penalties imposed in a case. *See* 15 U.S.C. § 78u-1(e) (2004). The U.S. Customs Service rewards eligible informants up to twenty-five percent of the take, and the total award cannot exceed $250,000 for any case. *See* 19 U.S.C. § 1619 (2004). The Environmental Protection Agency ("EPA") pays up to $10,000 for information on illegal dumping of hazardous materials. *See* 42 U.S.C. § 9609(d) (2004), 40 C.F.R. § 303.10 (2004). Nagorsky Report, 7-14.

110. *See, e.g.*, *"Unsolicited Commercial Email:" Hearing on P.L. 108-187 before the Senate Comm. On Commerce, Science and Transp*., 108th Cong. (May 20, 2004) (statement of Timothy J. Muris, Chairman, FTC), describing, in part, "spam lore," *available at* http://www.ftc.gov/speeches/muris/040520spamemailtest.pdf.

information is likely to require a higher monetary amount to overcome any powerful disincentives – such as the loss of income, fear of retaliation, or fear of incurring personal legal liability – that such a person may have.

On the issue of a minimum monetary amount necessary to sufficiently incentivize potential informants, industry participants commented that coming up with the "optimal" amount at this stage would be largely speculative. The monetary amount needed to create an adequate incentive for informants depends largely on who the informants are, and the specific incentives and disincentives they face on a case-by-case basis. Despite these unknowns, the FTC believes that reward amounts in the range of $100,000, and in some high-value cases, as much as $250,000, are reasonable estimates and seem unlikely to be too large, given the quality of the information sought and the enormous downside risk to the informant.[111] Indeed, the FTC believes that insider informants who possess the highest value information likely would require a minimum of $100,000 in reward amount to bring them forward to disclose their information. Two private technology companies, in separate initiatives, offered rewards in the amount of $250,000 for information leading to the arrest and conviction of promulgators of particularly malicious computer viruses and worms.[112]

While it is impossible to know in advance whether a particular reward amount is the "right" amount, what is clear is that **positive results** in a reward program – and the publicizing of such results – are very persuasive to convince potential informants to come forward. To the extent the Commission shows itself

---

111. It is important to note here that if Congress were to amend the CAN-SPAM Act to include a reward scheme, care must be taken to avoid legislative language that could give rise to litigation over whether the reward statute is a "money-mandating" or a "money-authorizing" statute. Under relevant case law, statutory authority must be a "money-authorizing" statute, to preserve an agency's discretion over whether, to whom, and in what amount the reward should be paid. Care must be taken to avoid specifying a "sum certain," or fixed reward amount, to which an informant automatically has a right once he or she has met certain eligibility factors. In construing one of the reward programs operated by the U.S. Customs Service (19 U.S.C.§ 1619), some courts have ruled that where the statute provides a sum certain or a clear standard for payment, the statute is considered money-mandating, and thus creates an implied contract between the agency and the informant. *See*, *e.g.*, *Hoch v.United States*, 33 Fed. Cl. 39 (1995); *Lewis v. United States*, 32 Fed Cl. 59 (1994). In such cases, courts may find a binding contract between the agency and informant, remove discretion over payment of rewards from the agency, and judicially review the payment of informants. *See also* Nagorsky Report, 20-22.

112. For the "Sasser" worm, the lure of Microsoft's reward inspired an informant's tip resulting in an arrest. *See* Robert Lemos, *Microsoft's Bounty Hunter*, CNET News.com (June 10, 2004), *available at* http://news.com.com/2102-7355_3-5228216.html?tag=st.util.print. For Microsoft's reward program, *see* Brian Krebs, *Microsoft Offers Reward for Worm Authors*, washingtonpost.com (Jan. 29, 2004); *available at* http://www.microsoft.com/security/antivirus/default.asp; Microsoft: Cranton, 2. For SCO's reward program, *see* Jay Lyman, *SCO Sets $250K Bounty for MyDoom Worm Writer*, TechNewsWorld (Jan. 28, 2004), *available at* http://www.technewsworld.com/perl/story/32713.html; http://ir.sco.com/ReleaseDetail.cfm?ReleaseID=127545.

willing to pay sizeable rewards when they are deserved, such positive results would likely encourage future informants to utilize the program. This may also have a deterrent effect on spammers, who may see the potential risk from their associates. Conversely, to the extent the Commission were to pay paltry rewards when significant ones are deserved, such negative results over time would likely discourage potential informants from coming forward.

B. Important Elements that Should Be Strongly Considered

In addition to the above essential elements, Congress may wish to consider additional specifications, should it determine to go forward with a reward system:

- It should be specified that it is unlawful to provide false information in connection with the reward system.
- Protection of informants' identities should be provided for, allowing them to remain anonymous whenever testimony is not necessary for case prosecution.
- It should be explicitly stated that the FTC cannot grant immunity.

1. It Should Be Specified that It Is Unlawful to Provide False Information in Connection with the Reward System

Several industry participants expressed concern about the risk that informants could fabricate evidence or otherwise submit disinformation.[113] While all reward schemes carry a risk of receiving false or bad information, the particular difficulties of detecting fabricated evidence by technologically sophisticated persons in the case of spam is reason for heightened concern.[114] To minimize this danger, any reward system established by Congress should include a provision imposing civil penalties on anyone who provides information that he or she knows or should know to be false.[115]

---

113. *See, e.g.*, CAUCE: Everett-Church, 56; National Newspaper Association-Comment, 7-8; National Retail Federation-Comment, 16-17; Reed Elsevier-Comment, 7; Spamhaus: Murphy, 29; U.S. Small Business Administration-Comment, 6; Weston, Garrou and Dewitt-Comment, 10-13 (recommending that penalties be imposed on those who falsely report spam); Word to the Wise: Atkins, 55-56.

114. *See* Spamhaus: Murphy, 38-39; NYOAG: Kline; *see also* Boneh Report, 17, on the ease with which sophisticated spammers can generate false evidence, given the lack of authentication in the present email system.

115. Reporting false information to the government already constitutes a criminal violation of 18 U.S.C. § 1001. However, it would be beneficial to also specify that it is a civil violation, exposing a violator to civil penalties, to provide false information to the government in connection with a reward system. The burden of proof for a civil violation – "a preponderance of the evidence" – would be easier for the government to meet than the burden applicable in criminal cases ("beyond a reasonable doubt"). In addition,

continued...

2. Protection of Informants' Identities Should Be Provided, Allowing Them to Remain Anonymous Whenever Testimony Is Not Necessary for Case Prosecution

The promise of anonymity may be an important element in whether or not an informant decides to come forward.[116] Were a reward system established, consideration should be given to specifying, as do the guidelines of the IRS reward program, that informants can supply information anonymously throughout the entire process, including after the bounty is paid, and placing their identities beyond the reach of the Freedom of Information Act ("FOIA") at any time. Obviously, should the informant's testimony become crucial for successful litigation, the informant would at that point be required to give up his or her anonymity. However, the FTC and the informant would be able to make such a decision at that time.[117]

3. It Should Be Explicitly Stated that the FTC Cannot Grant Immunity

As previously discussed, even if the reward program explicitly makes clear that it is interested in "insider" information, the FTC is skeptical whether informants with this class of information will be willing to come forward. Since many insiders may themselves be involved in the schemes they betray, they face potential legal liability, including the risk of becoming the target of the investigation themselves. Given that the FTC has only civil law enforcement authority, it is not in a position to grant immunity from criminal liability. To preclude misunderstandings and pointless haggling with potential informants, it should be explicitly stated that the FTC cannot grant immunity.

---

unlike in the criminal context, the government would not necessarily need to establish proof of scienter to prove a civil violation. Thus, should Congress decide to establish a CAN-SPAM reward system, establishing a civil sanction for providing false information to the FTC could create a more flexible and effective deterrent to false reporting.

116. *See* Ferziger and Currell, supra fn. 8, at 1189-91.

117. *See* Nagorsky Report, 9-15, for a discussion of the anonymity provisions found in different federal reward schemes.

Section V: Procedures to Minimize the Burden of Complaining to the FTC About CAN-SPAM Act Violations

In connection with designing a reward system, Congress, in the CAN-SPAM Act, directed that this Report set forth "procedures to minimize the burden of submitting a complaint to the Commission concerning violations of [the CAN-SPAM Act], including procedures to allow the electronic submission of complaints to the Commission."[118] In this Section we review the Commission's current complaint procedures. As detailed below, the Commission has already implemented simple, non-burdensome, and user-friendly methods to register spam-related complaints. We also consider what additional procedures, if any, might be needed if the model reward system were implemented in the future.

A. Existing Spam Complaint Mechanisms Are Minimally Burdensome

The FTC has in place two main channels for collecting information and complaints about spam. The first is a general consumer complaint intake system, which collects and processes complaints about the wide variety of topics within the Commission's consumer protection jurisdiction. It can be accessed through an Internet-based Consumer Complaint Form or by telephoning a toll-free Consumer Response Center.[119] The second information-collection channel is the FTC's Spam Database, to which consumers forward approximately 300,000 items of spam email every day. Because each information channel employs complaint submission procedures that are quick, simple and cost-free, we conclude that both channels are minimally burdensome to use at present.

1. FTC Consumer Complaint Form and Call Center

The FTC processes consumer complaints about a wide variety of topics. Recognizing that some people may be more comfortable speaking with live representatives and others may prefer to submit complaints online, the agency has developed both Internet and telephone intake procedures. In both instances,

118. 15 U.S.C. § 7710(1)(B) (2004).

119. A relatively small number of consumer complaints are also submitted by mail, facsimile, and hand-delivery.

the complainants are posed identical questions.[120] Complainants are prompted to provide their personal contact information,[121] followed by a series of questions about their interactions with the persons or entities that are the targets of their complaints. A final, open-ended question invites the complainant to describe the problem that gave rise to the complaint.[122]

Consumers' responses are entered into a searchable, field-coded complaint database to facilitate case development and investigation. Complaints are reviewed by specially-trained coders and counselors to ensure the integrity of the data. Data fields captured in spam-related complaints include, for example, the particular provision of the CAN-SPAM Act allegedly violated, and the type of product or service promoted within the spam message. These complaints are available to FTC attorneys and investigators through the Consumer Information System ("CIS") database. Fraud-related complaints are shared with more than one thousand federal, state, and international law enforcement authorities, through the FTC's "Consumer Sentinel" network.

Consumers who wish to complain about CAN-SPAM Act violations can easily access the Commission's Consumer Complaint Form and Consumer Response Center. The FTC's telephone number and website address are featured prominently in media announcements and consumer education materials.[123] Internet complainants will find the Consumer Complaint Form only one click away from the FTC's homepage – and from many other web pages within the agency's website. Complaint submission instructions are clear and user-friendly, the questions asked of complainants are simple, and the complaint process averages only five minutes from start to finish.[124] Complainants are also informed of an additional, optional procedure to notify the FTC about unwanted spam – the FTC's spam database, discussed further below – so that those who do not wish to verbally describe their experiences can merely forward their spam to the FTC.

---

120. A copy of the FTC's online Consumer Complaint Form, which can be accessed through http://www.ftc.gov, has been attached to this Report as Appendix 3.

121. Note that anonymous complaints are permitted. "The information you provide is up to you. However, if you do not provide your name or other information, it may be impossible for [the FTC] to refer, respond to, or investigate your complaint or request." *Id.*

122. The FTC provides Spanish speaking phone counselors and Spanish language complaint forms for consumers who prefer to use such resources.

123. The FTC's toll-free number for consumer complaints is 1-877-FTC-HELP. The Consumer Complaint Form can be accessed through the FTC's website, http://www.ftc.gov.

124. The FTC's online Consumer Complaint Form contains a Paperwork Reduction Statement estimating that only five minutes are required to complete the form.

The Internet and telephone complaint submission procedures are rapid, simple, intuitive, and free. Thus, the Commission believes these streamlined complaint submission mechanisms are minimally burdensome and user-friendly.

2. Forwarding Spam Messages to the FTC's Spam Database

As discussed earlier in this Report, the Commission has developed a separate complaint database dedicated entirely to spam email. Recipients of illegal and unwanted spam messages are encouraged to forward copies of those messages electronically to the FTC's spam database.[125] Roughly 300,000 items are submitted daily to this spam database, permitting aggregated analyses and searches and allowing the FTC to track the volume, nature, and contents of spam email campaigns in circulation. This method of notifying the FTC about illegal spam additionally preserves certain hallmarks of a message's electronic trail, which can hold valuable clues to the identities of relatively unsophisticated spammers or persons who have accidentally violated the CAN-SPAM Act.

Submitting complaints by email epitomizes simplicity. To inform the Commission about illegal spam under this mechanism, a complainant merely employs her customary email interface. One may presume the complainant's prior familiarity with her email program renders this task extremely basic.[126] Under one widely-used email program, for example, a complainant must merely press the "forward" button and input the email address to which a copy should be sent. Because this method of electronic complaint submission is rapid, effortless, and cost-free, it too is minimally burdensome to the consumer.

B. Crafting Minimally Burdensome Reward Claim Submission Procedures

If a CAN-SPAM reward system were implemented, the FTC would need procedures to accept the information submitted for consideration under that system. (The remainder of this Section refers to such submissions as "claims" or

---

125. The FTC has designated a specific email address to which spam emails may be submitted: spam@uce.gov.

126. Not all email users know how to view or transmit copies of a received message's "full headers"– the clues within the message about its electronic trail. The transmittal of "full headers" differs widely from one email program and version to the next. Those people who know how to work with "full headers" forward message copies including the headers, and those who do not know how to display the "full headers" forward message copies without the headers. This has little effect on the quality of the database, as the large volume of spam messages transmitted daily ensures that there are generally multiple copies of spam messages from any given campaign.

"applications" under the reward system.) An eligible reward system claim must do more than generally allege that the CAN-SPAM Act has been violated. Were Congress to implement a reward system incorporating the essential elements discussed above in Section IV.A.3, an eligible reward claimant at a minimum must identify with particularity the person or persons who violated the Act, and provide information regarding violations of certain specified provisions of the CAN-SPAM Act.[127] In designing a reward system application procedure, the FTC would attempt to both (1) minimize the burden to persons who submit claims or applications, and (2) enhance the agency's efficiency in processing reward applications, identifying high-value information, and converting such information into successful enforcement actions.

There are two general approaches. The first might be to modify and expand the Commission's existing online Consumer Complaint Form to accept information and claims under the reward system. Alternatively, another approach might be to create an entirely new, free-standing mechanism to accept reward system applications. In either case, the mechanism should permit the FTC to identify and process high-value reward claims in a cost-efficient manner, and require minimal expenditure of time, effort, and financial resources on the part of consumers.

Section VI: Conclusion

The Commission is pleased to offer its analysis of the key considerations that it believes should come into play in evaluating a spam reward system. These considerations include: how a reward system might be designed to encourage insider informants to come forward with high-value information; the incentives and disincentives that influence such insider informants' decisions to provide information to the FTC; and whether the benefits of improved enforcement likely outweigh the costs of establishing and maintaining a reward system.

---

127. If a reward application does not "identify the person" who has allegedly violated the CAN-SPAM Act, that application is necessarily ineligible for a reward. 15 U.S.C. § 7710(1)(A)(i). *See also* discussion on narrowing eligibility requirements to violations of only certain specified provisions of the CAN-SPAM Act, *supra* Section IV.A.3.

Against this backdrop, the Commission has identified certain elements that it believes would be essential for an effective reward system. While including these elements may not guarantee that a reward system will achieve its purpose, the FTC believes that absent these elements, any reward system would likely fail. Therefore, should Congress mandate a reward system, the Commission urges consideration be given to the essential elements discussed in this Report.

Appendix 1: List of Interviews

Name (Last, First)	Organization	Date of Meeting	Transcript/ Submission Available?
Atkins, Laura	The SpamCon Foundation	2/10/2004	Yes
Atkins, Steve	Word to the Wise	2/10/2004	Yes
Baker, Dave	EarthLink	4/28/2004	Yes
Bernard, Ted	Savicom	3/8/2004	Yes
Brady, Betsy	Microsoft Corp.	2/17/2004	No
Brower, Adam	The Spamhaus Project	5/3/2004	Yes
Bruening, Paula	Center for Democracy and Technology (CDT)	2/11/2004	Yes
Carlon, Jeff	The SCO Group	2/4/2004	No
Cashion, Karen	EarthLink	4/28/2004	Yes
Catlett, Jason	JunkBusters Corp.	2/11/2004	Yes
Cerasale, Jerry	The Direct Marketing Association (DMA)	3/9/2004	Yes
Cohn, Cindy	Electronic Frontier Foundation (EFF)	2/11/2004	Yes
Cranton, Tim	Microsoft Corp.	2/17/2004	No
Cranton, Tim	Microsoft Corp.	7/16/2004	Yes†
Curran, Charles D.	America Online, Inc. (AOL)	5/7/2004	Yes†
Edelman, Ben	Harvard Law School	3/3/2004	Yes
Everett-Church, Ray	Coalition Against Unsolicited Commercial Email (CAUCE)	2/10/2004	Yes
Haight, Julian	SpamCop.net, Inc.	3/2/2004	Yes
Halpert, James J.	Internet Commerce Coalition (ICC)	6/14/2004	Yes†
Hoofnagle, Chris Jay	Electronic Privacy Information Center (EPIC)	2/11/2004	Yes
Judge, Paul Q.	CipherTrust	2/23/2004	Yes
Kendall, James H.	Washington Ass'n. of ISPs (WAISP) and Telebyte, Inc.	7/19/2004	Yes†

† Written submission is available, in lieu of an interview transcript.

Name (Last, First)	Organization	Date of Meeting	Transcript/ Submission Available?
Kline, Stephen	Office of the Attorney General, NY	5/14/2004	No
Kramer, David H.	Wilson, Sonsini, Goodrich, and Rosati	2/23/2004	Yes
Larkin, Daniel J.	Federal Bureau of Invest., Internet Crime Complaint Center (FBI-IC3)	7/26/2004	No
Laurant, Cédric	Electronic Privacy Information Center (EPIC)	2/11/2004	Yes
Lessig, Lawrence	Stanford Law School	2/9/2004	No
Levine, John R.	Internet Research Task Force, Anti-Spam Research Group (ASRG)	2/26/2004	Yes
Lewis, Chris	Nortel Networks Limited	2/23/2004	Yes
Mayor, Michael	NetCreations, Inc.	3/8/2004	Yes
McGuire, Russell E. (“Rusty”)	Office of the Attorney General, VA (VAOAG)	3/10/2004	Yes
McLaughlin, Andrew	Google	2/23/2004	Yes
Murphy, Alan	The Spamhaus Project	5/3/2004	Yes
Nigam, Hemanshu	Microsoft Corp.	2/17/2004	No
Plesser, Ron	Piper Rudnick for The Direct Marketing Association (DMA)	3/9/2004	Yes
Praed, Jon L.	Internet Law Group	2/23/2004	Yes
Reid, John	The Spamhaus Project	5/3/2004	Yes
Ressin, Charles	U.S. Customs and Border Patrol	6/2/2004	No
Rubin, Joe	U.S. Chamber of Commerce	3/9/2004	Yes
Schneider, Todd	U.S. Customs and Border Patrol	6/2/2004	No
Schneider, Todd	U.S. Customs and Border Patrol	6/7/2004	No
Selis, Paula	Office of the Attorney General, WA (WAOAG)	3/10/2004	Yes
Shafranovich, Yakov	Internet Research Task Force, Anti-Spam Research Group (ASRG)	2/26/2004	Yes
Shaw, Carla	EarthLink	4/28/2004	Yes

Name (Last, First)	Organization	Date of Meeting	Transcript/ Submission Available?
Sorkin, David E.	John Marshall Law School	3/3/2004	Yes
Squire, Brooke	United Online, Inc.	5/12/2004	Yes
Tuck, Russ	Google	2/23/2004	Yes
Uncapher, Mark	Information Technology Association of America (ITAA)	3/9/2004	Yes
Wellborn, Paul F., III (“Pete”)	The Wellborn Firm, LLC for EarthLink	4/28/2004	Yes

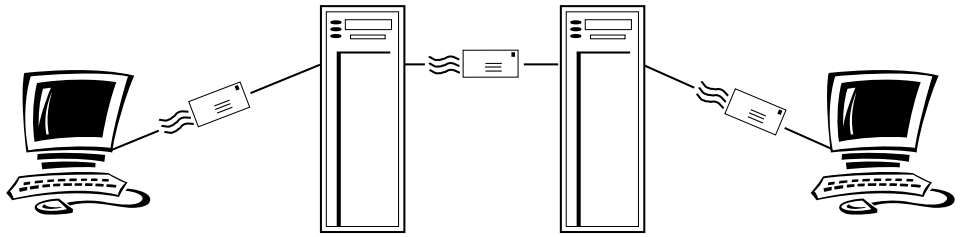
Appendix 2: Part III of the Commission's National Do Not Email Registry Report

III. The Email System and the Resulting Spam Problem

The email system is open, allowing information to travel freely with relative anonymity and ease. This structure facilitates the proliferation of spam by making it possible and cost-efficient for illegitimate marketers to send spam to billions of email accounts worldwide, while allowing them to hide

Federal Trade Commission

Graphic 1



their identities and the origins of their email messages. ISPs have responded to the spam problem by using blocking and filtering software. Currently, ISPs are attempting to combat this fundamental problem with spam – anonymity – by developing authentication technologies that would provide a method for identifying the true origin of an email.

A. How the Email System Works[14]

Email is a complex system that includes the sequential interactions of at least four computers[15] that engage in a five-part dialogue. (*See* Graphic 1). Each step in the email process is recorded within the email's "headers," so that an email's path through each computer can be tracked. Unfortunately, the system that makes email work, "Simple Mail Transfer Protocol" or "SMTP,"[16] does not require the transmission of accurate information. As explained below, the only piece of information that must be accurate is the recipient's address appearing in an SMTP command known as "RCPT TO."

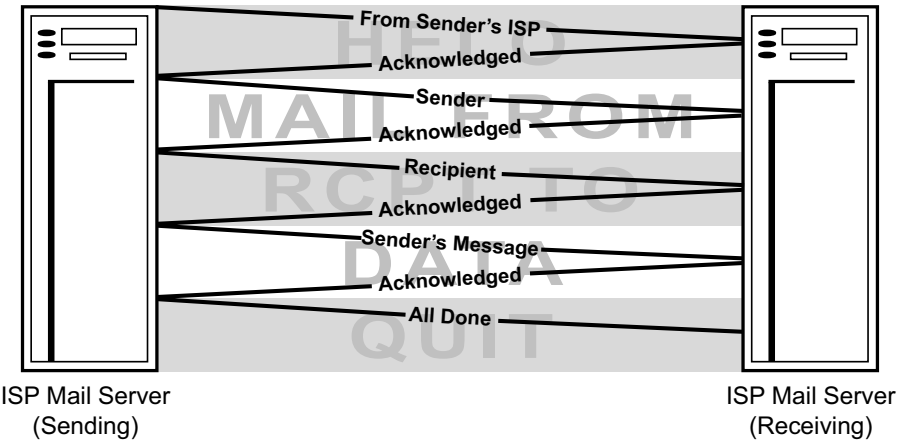
1. The five-part dialogue

Anyone who has ever used email knows what a "user-friendly" medium it is. To send a message, a person only needs to open an email program, type a recipient's address in the "To:" line, perhaps include a subject in the "Subject:" line, type the body of the message, maybe add an attachment, and select "send." A recipient has a similarly easy time. To read a message, a recipient only needs to open an email program, select the message listed in the inbox, and, if an attachment is included with the message, download or read the attachment.

The technical process of how email functions is, of course, much more complex. From the time that a person clicks "send" until the message arrives in a recipient's inbox, many processes occur involving – when reduced to the most basic form – at least four computers:

14. Don Blumenthal, the FTC's Internet Lab Coordinator, provided much of the material for this Section.
15. In reality, if a message is sent within an organization, only three computers may be involved because the sending mail server and the receiving mail server may be the same.
16. SMTP is defined in a "request for comments" posted by the Internet Engineering Task Force ("IETF") and known as RFC 2821. The IETF is an Internet-standards setting body.

Graphic 2



(1) the sender's computer; (2) a mail server owned by an ISP or other entity that provides the sender with an email account; (3) a mail server owned by an ISP or other entity that provides the recipient with an email account; and (4) the recipient's computer.

Clicking the "send" button transmits the email message from the sender's computer to the sender's outbound mail server. This sending server locates and begins a dialogue with the recipient's inbound mail server using SMTP. Under SMTP, the sending and receiving mail servers engage in a five-part dialogue. (*See* Graphic 2).

In the first part, the sending server initiates the exchange with the receiving server using a command known as "HELO," followed by the name of the sending mail server. If translated into English, the sending server would be saying "Hello, I'm <servername>." The receiving server responds with an acknowledgment back to the sending server. It is important to note that the receiving server uses this "HELO" command only to ensure that it is receiving a valid transmission.[17] The receiving server does not verify whether the servername listed after the "HELO" command is the sending server's actual, accurate name. This aspect of SMTP – the fact that the receiving server does not demand authentication that the sending server is what it purports to be – significantly impedes effective anti-spam solutions, including robust enforcement of the CAN-SPAM Act and the effective use of anti-spam filters by ISPs and other domain operators.[18]

After the receiving server has sent an acknowledgment, the sending server begins the second part of the dialogue, using a command called "MAIL FROM." The sending server, in effect, tells the receiving server, "I have mail to deliver from <sender>." The "MAIL FROM"

17. The receiving computer only validates whether the dialogue started properly. The "HELO" command is the first command allowed under the SMTP system. If there is no "HELO" command when using SMTP, then the transmission is invalid.

18. *See infra* Section III.B.1.

is followed by an email address, known as the "envelope from." The "envelope from" is analogous to the return address appearing on an envelope sent through the postal system. As with a return address on an envelope, nothing requires the "envelope from" to be accurate. Moreover, just as the return address on a letter need not match the return address on the envelope containing the letter, the "envelope from" does not have to match the "From:" line that a recipient sees when reading an email message.[19]

In the third part of the dialogue, the sending server, using the "RCPT TO" command, tells the receiving server the email address to which the message should be delivered, and the receiving server sends an acknowledgment back to the sending server. If the message is for more than one recipient, the sending server issues separate "RCPT TOs" for each one. As with the "MAIL FROM," nothing requires that the "RCPT TO" address match the address that appears in the "To:" line of the email. Spammers often exploit this feature to make it appear that their messages are personal. For example, a message's "To:" line may state "Bob," "Account Holder," or any other term designed to trick recipients into believing that they have a relationship with the spammer. In contrast, the email address in the "RCPT TO" command must be valid or the message cannot be delivered.[20]

In the fourth part of the dialogue, after the receiving server has acknowledged the "RCPT TO," the sending server, using the "DATA" command, transmits the actual message. While not required, the first line of the message usually begins with "Subject:," followed by the sender's desired subject. Other headers, such as "Reply-To:,"[21] "cc:," and "bcc:" also may be specified here.[22] The text of the message and any attachments then follow. A blank line with a period signals the end of the "DATA" section. This part of the dialogue concludes when the receiving mail server acknowledges receipt of the email.

In the fifth and final part of the dialogue, the sending server uses the "QUIT" command to terminate the process. The recipient then can view the message through a web interface or email program.

2. Email headers

In theory, the above-described email path is memorialized in "headers" that the recipient can view. Headers are added at three points in the basic four-computer model: (1) message creation; (2) transmission to the sender's server; and (3) transmission to the recipient's

19. Indeed, the Commission staff's April 2003 False Claims in Spam Study reported that 1/3 of the spam analyzed contained false information in the "From:" line. False Claims in Spam, 3.

20. *See infra* Section III.B.1.

21. "Reply-To:" may vary from the address in the "From:" line. This header has legitimate uses; for example, a sender with two addresses may want replies to go to only one address. Spammers, however, can use this header to deflect hostile responses. For instance, the "Reply-To:" address may identify a non-existent email address, in which case opt-out demands will disappear into the ether. Or, the spammer may identify a valid but innocent email address, thereby causing the maligned addressee to receive an avalanche of opt-out requests and complaints. *See infra* Section III.B.1.

22. The headers discussed in this section are only a subset of those available. They are, however the most commonly used and the most important for understanding email transmission and how spammers use the current system to hide their identities.

#	Header	Header's Source
1	Received: from server.sender.com (server.sender.com [123.45.67.90]) by server.recipient.com (8.8.5/8.7.2) with ESMTP id ABC12345 for <pan@recipient.com>; Tue, Mar 30 2004 20:06:22 EST -0500 (EST)	Receiving Mail Server
2	Received: from client.sender.com (client.sender.com [123.45.67.89]) by server.sender.com (8.8.5) id 003A23; Tue, Mar 30 2004 20:06:17 EST -0500 (EST)	Sending Mail Server
3	From: dmb@sender.com (D.M. Bloom)	Sender
4	To: pan@recipient.com	Sender
5	Date: Tue, Mar 30 2004 20:06:15 EST	Sending Mail Server
6	Message-Id: <dmb061346790416-00012487@sender.com>	Sending Mail Server
7	X-Mailer: Eudora v.6.0.3.0	Sender's Computer
8	Subject: How Email Works	Sender

server. Headers contain lines of information that provide details about the message and its transmission. Understanding headers is critical to understanding how email works and how spammers exploit the email system.

When an email is received, the recipient usually views only a few of the header lines, including the "To:" line, the "From:" line, the "Subject:" line, and the "Date:" line. Most email programs, though, enable recipients to view all of the headers for each message. A recipient who chooses to view all headers will see the information appearing in the second column of the table above, showing an illustrative email header, presented in the order in which it appears in the email.[23]

As a message travels from computer to computer, a new header is added to the top of the list of headers. Headers therefore should be read in reverse order. In the example above, the sender creates Line 8, the "Subject:" header. The sender's computer also creates Line 7, "X-Mailer," a header that denotes the sender's email program. The sender's mail server adds Line 6, the "Message-Id," a unique number that stays with the message from beginning to end. (Other "Ids" are created as the message passes through different servers). The "Message-Id" does not always have the email format shown here; it may be just a series of characters without the sender's domain information.[24] The sender's mail server adds Line 5, "Date:." This header shows the date and time the sender's mail server processes the message. Line 4, "To:," shows the intended recipient, and line 3, "From:," shows the sender's email address. The sender creates both Lines 4 and 3. "From:" also may show a name in brackets or parentheses.

Headers that begin with "Received:" are called "routing headers," and each mail server that a message passes through as it travels from sender to recipient adds such a routing header. These headers should be read from bottom to top. In the example above, the first "Received:" header (Line 2) indicates that the sending mail server (server.sender.com) received the message from the sender's computer (client.sender.com), which had the IP number, or Internet address, 123.45.67.89, on March 30, 2004, at 8:06 pm. The "8.8.5" shows

23. In reality, each line of an email header is not numbered, although for convenience of explanation, the table provides ordinal numbers in the first column.

24. The sender's domain information – where on the Internet the sender purports to come from – appears after the @ symbol in line 6.

the version of Sendmail, a mail server program, used on the sender's server. The second "Received:" header (Line 1) shows receipt of the message by the recipient's mail server from the sender's mail server. This header is similar to the previous one except for the format of the "ID" assigned at this step and the fact that it shows the intended recipient. The routing is now complete; the recipient's email program does not add a header when the message is retrieved.

The four-computer model is the simplest depiction of the core processes in sending an email message. Email routing is rarely that simple, however. There are almost always a number of additional intervening stops on the path from sender to recipient. This is because the sender's mail server must find the proper IP address for the recipient's mail server. If the sending server does not have a complete database of email servers and their corresponding IP addresses, it must route the message through intervening servers, or "relays," that narrow the destination down to the proper receiving server. Each server in the relay process adds a "Received from:" line to the headers.[25] When relays are secured properly, the system works well and a message can be traced to its origin.

B. How Spammers Exploit the Email System

Spammers are technologically adept at hiding their identities. Their concealment techniques make it extremely difficult to track them. In addition, spammers continually engage in a game of technological cat-and-mouse with the ISPs that try to block their messages.

1. Spammers exploit SMTP's anonymity

Spammers use many techniques to hide, including: spoofing, open relays, open proxies, and zombie drones. As explained below, each of these techniques makes it difficult, if not impossible, to identify spammers through email headers and significantly impedes law enforcement.[26]

First, spammers use "spoofing" to falsify header information and hide their identities. This technique disguises an email to make it appear to come from an address other than the one from which it actually comes.[27] A spammer can falsify portions of the header or the entire header. A spammer can even spoof the originating IP address.[28] The SMTP system facilitates this practice because it does not require accurate routing information except for the intended recipient of the email.[29] By failing to require accurate sender identification, SMTP allows spammers to send email without accountability, often disguised as personal email.[30] A spammer can send out millions of spoofed messages, but any bounced messages – messages returned

25. As part of the Data dialogue in part 4 of the SMTP dialogue described above, spammers also can add spurious "Received:" headers manually before sending a message.

26. *See infra* Section III.C.

27. Felten Report, 2. Spoofing requires virtually no technical sophistication and can be accomplished by simply changing the preferences in a computer user's email software. AOL: Koschier – Spam Forum (April 30, 2003), 175-82.

28. Bishop Report, 12 n.6.

29. *See supra* Section III.A.1.

30. An attorney representing AOL testified before the Pennsylvania State Senate Communications and Technology Committee that as much as 90 percent of spam messages contain falsified header or routing information (September 23, 2003).

as undeliverable – or complaints stemming from the spoofed emails will only go to the person whose address was spoofed. The spammer never has to deal with them. As a result, an innocent email user's inbox may become flooded with undeliverable messages and angry, reactive email, and the innocent user's Internet service may be shut off due to the volume of complaints.[31]

Second, spammers use open relays to disguise the origin of their email. The difference between an open relay and a "secure" one is critical. A computer must be connected to a mail server to send or receive mail. When someone sends an email message using an email server that is "secure," the mail server's particular software checks to make sure that the sender's computer and email account are authorized to use that server. If this authorization is in order, then the server sends the mail. If the computer and email account are *not* listed as authorized, the server refuses to accept the email message. On the other hand, if a mail server is *not* secure, i.e., some of its settings allow it to stay open, it will forward email even though the senders are not authorized users of that server. An open server is called an open relay because it will accept and transfer email on behalf of any user anywhere.[32]

Spammers who use open relays effectively bypass the email servers to which their computers are connected. Once the spam passes through an open relay, a routing header from that server is added to the email. Thus, the email will appear as if it originated from the relay mail server. This allows spammers to obscure their tracks, making it difficult to trace the path their message takes from sender to recipient.

Third, many spammers use "open proxies." They began doing this after ISPs and other mail server operators realized the negative impact of open relays and made efforts to identify and close them.[33] Again, a word of explanation is in order. Most organizations have multiple computers on their networks, but have a smaller number of proxy servers that are the only machines on the network that directly interact with the Internet.[34] 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. "[P]roxy misconfiguration is common and results in general purpose forwarding that is utilized by hackers and spammers."[35] For example, a spammer can use an open proxy to connect to another mail server and use that mail server to

31. The Commission has charged spoofing as a violation of Section 5 of the FTC Act, 15 U.S.C. § 45. *See e.g., FTC v. GM Funding*, No. SAVC 02-1026 (C.D. Cal. filed Nov. 6, 2002) (one victim of spoofing received 40,000 rejected messages in his inbox); *FTC v. Westby*, No. 032-3030 (N.D. Ill. filed Apr. 15, 2003). Moreover, spoofing violates Sections 4 and 5(a) of the CAN-SPAM Act, 18 U.S.C. § 1037 and 15 U.S.C. § 7704(a).
32. Rubin Report, 13.
33. Nonetheless, "open relays continue to exist in abundance." Rubin Report, 14.
34. A proxy server is so named because, when interacting with the Internet, it serves as a substitute or proxy for other computers on its network.
35. Rubin Report, 14.

send spam. The headers for messages that pass through an open proxy indicate the proxy's IP address in the "Received:from" line, and not the true originating IP address. In this way, open proxies provide another means for spammers to hide their tracks. MessageLabs, an email security company, believes that spammers sent more than two-thirds of all their email in 2003 through open proxies.[36]

Fourth, the most recent escalation in this cat-and-mouse game involves the exploitation of millions of home computers, using malicious viruses, worms, or "Trojans."[37] These infections, often sent via spam, turn any computer into an open or compromised proxy called a "zombie drone."[38] Once a computer is infected with one of these programs, a spammer can remotely hijack and send spam from it. Spammers target home computers with high speed Internet connections, such as DSL or cable modem lines, that are poorly secured. Spam sent via zombie drones will appear to originate (and actually will originate) from these infected computers.[39] This practice is all the more pernicious because users often do not know that their home computers are infected. The outgoing spam does not show up in their outbox. Once an ISP realizes spam is coming from one of its customer's machines, the ISP must shut off the customer's Internet service even though the customer had no knowledge that the spammer was using his or her machine.[40]

Although it is difficult to estimate the prevalence of zombie drones, Microsoft's Anti-Spam Manager has indicated that zombie drones presently account for somewhere between 15 and 60 percent of spam, and opined that the percentage is rising.[41] One major ISP reported a 41% increase in customer complaints regarding spam coming from other ISPs between October 2003 and February 2004.[42] This ISP believes that the shift is due to the increased use of zombie drones to transmit email messages from those other ISPs.[43] Another ISP reported that during 2003 it discovered over 600,000 open proxies or zombie drones.[44] Most recently, ISPs have observed compromised proxies shifting overseas, which means that the spam looks like it is coming from overseas, yet the virus author and spammer using the drones may be located in the United States.[45] If the past is an indication

36. MessageLabs states its conclusion, but does not explain how the company reached it. MessageLabs, "Spam and Viruses Hit All Time Highs in 2003," December 8, 2003 at http://www.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=613&region=. A background paper prepared by the Organization for Economic Cooperation and Development ("OECD") in January 2004, similarly states that 50 percent of spam flows through open relays and proxies, but does not explain the basis for this assertion. http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF. The OECD's paper does not indicate the time frame for this statistic.
37. Rubin Report, 14-15.
38. Felten Report, 2.
39. Rubin Report, 14.
40. CNN, "Your Computer Could be a 'Spam Zombie,'" February 18, 2004, at http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/.
41. March 10, 2004 briefing of FTC staff by Microsoft Anti-Spam Manager.
42. Confidential 6(b) Order Response.
43. *Id*.
44. Confidential 6(b) Order Response.
45. One ISP reports that in January and February of 2004, 56% of all spam that made it to its subscribers' inboxes was routed through a server or proxy located outside the United States. Confidential 6(b) Order Response.

of the future, within the next several months spammers will have found an as-yet unknown new technique for masking their identities.

2. ISPs' response to spammers' email exploitation

The ISP industry's standard practice is to prohibit unsolicited bulk email.[46] ISPs and email filtering companies attempt to enforce this rule mainly through the use of blocking and filtering software.[47] ISPs initially block email based on volume ("volume filtering") and not based on content because their filters cannot make a distinction between commercial and non-commercial email. Many ISPs first attempt to block email at the point of the attempted connection to the ISPs' networks (the first part of the five-part SMTP dialogue).[48] For example, an ISP may initially block a message based on an IP address it has determined is used by spammers as an open relay or open proxy, or because an IP address or domain is associated with sending high volumes of spam. Anti-spam organizations compile "blacklists" of reported open relays and proxies that ISPs and other operators of mail servers can use to support their filtering efforts.[49]

Although the first line of defense against spam is volume filtering, most ISPs add an additional layer by filtering based upon their own customers' complaints. ISPs use complaint data in a variety of ways, including Bayesian filtering – filtering based upon the concept that some words occur more frequently in known spam. By analyzing email that customers report as spam, ISPs generate a mathematical "spam-indicative probability" for each word.[50] Many email filtering companies combine this type of filtering with filtering based upon different components of the message headers.

ISPs and email filtering companies are concerned about potentially blocking legitimate messages. These "false positives" can be a serious side effect of combating spam. According to Assurance Systems, a spam solutions provider, ISPs block or filter 17% of permission-based email.[51] To reduce false

46. United Online ("UOL"): Popek, 30-31; Junkbusters: Catlett, 15; *See also* the acceptable use policies of MCI (http://global.mci.com/legal/usepolicy; http://privacy.msn.com/anti-spam), Earthlink (http://www.earthlink.net/about/policies/use; http://docs.yahoo.com/info/guidelines/spam.html), Comcast (http://www.comcast.net/terms/abuse.jsp), AOL (http://postmaster.aol.com/guidelines/bulk_email.html), Microsoft (http://privacy.msn.com/anti-spam), and UOL (http://www.netzero.net/legal/terms.html, http://www.juno.com/legal/accept-use.html, and http://www.mybluelight.com/legal/terms-bluelight.html).
47. Email blocking occurs at the point of attempted connection to the ISP's network. Email filtering occurs once an email enters the ISP's network, but before it reaches a recipient's inbox.
48. *See supra* Section III.A.1.
49. SpamCop: Haight – Spam Forum (May 1, 2003), 118.
50. Mertz, David. "Spam Filtering Techniques: Comparing a Half-Dozen Approaches to Eliminating Unwanted Email," Gnosis Software, Inc., August 2002 at http://www.gnosis.cx/publish/programming/filtering-spam.html.
51. http://www.returnpath.biz/pdf/Blocking_Filtering_Report.pdf. Assurance Systems determined the percentage of permission-based messages that were incorrectly filtered by ISPs by tracking the delivery, blocking, and filtering rates of over nine thousand email campaigns. High false positive rates undermine consumer confidence in the email system. In an October 2003 study of 483 randomly selected consumers with home Internet access, RoperASW found that 40 percent of consumers who subscribe to or receive email from their credit card issuer expressed concern about not receiving email from the issuer due to their ISPs' anti-spam filters. *Email and Spam: Attitudes and Behaviors Among Financial Services Consumers*, Study commissioned and submitted to the Commission by Bigfoot Interactive.

positive rates, ISPs compile "white lists" of marketers who agree to adhere to an ISP's policies and procedures regarding bulk email. Once a marketer is on an ISP's white list, the ISP does not filter that marketer's messages. A certain number of complaints regarding a particular marketer who is on the ISP's white list, however, will trigger removal of that marketer from the white list.[52] The threat of false positives is a significant barrier to more effective filtering by ISPs.

C. Email's Lack of Authentication Enables Spammers to Exploit the Email System

Obfuscatory techniques such as spoofing, open relays, open proxies, and zombie drones make it more difficult for ISPs to locate spammers. When ISPs and domain holders implement technologies designed to stop one exploitative technique, spammers quickly adapt, finding new methods to avoid detection. If the cloak of anonymity were removed, however, spammers could not operate with impunity.[53] ISPs and domain holders could filter spam more effectively, and the government and ISPs could more effectively identify and prosecute spammers who violate the CAN-SPAM Act or other statutes.

The marketplace is already moving toward creating systems for authenticating a message's originating second-level domain,[54] with major ISPs backing various approaches.[55] AOL champions the adoption of SPF ("sender policy framework"),[56] an authentication standard developed by Meng Weng Wong ("Wong") that verifies the "envelope from"[57] of an email message. Microsoft has proposed "Caller ID for Email,"[58] a protocol that would verify the "From:" line that appears in an email message.[59] Recently, Microsoft and Wong announced plans to merge SPF and Caller ID for Email into one technical specification.[60] Yahoo! has advocated the implementation of "Domain Keys," a standard that would involve the use of public/private key cryptography.[61] The IETF has also established a working group to develop an authentication standard.[62] The IETF working group intends to propose an authentication standard during the Summer of 2004.[63]

52. Briefing of FTC staff by an ISP concerning its Confidential 6(b) Order responses.
53. Comcast: Lutner, 42; Edelman, 28; Savicom: Bernard, 23; UOL: Skopp, 61.
54. A second-level domain is the name in an email address that appears between the "@" symbol and the dot. For instance, "ftc" is the second-level domain in the address "abc@ftc.gov."
55. U.S. Internet Service Provider Association ("USISPA")-Comment, 2 (stating that "several of its members and other technology vendors are in the process of developing solutions to spam based on identifying the origin or identity of email senders"). Digital Impact: Brondmo, 17-18; ESPC: Hughes, 11; Internet Commerce Coalition ("ICC"): Halpert, 25; NetCreations: Mayor, 24; Roving Software: Olson, 20-21.
56. http://www.ietf.org/internet-drafts/draft-mengwong-spf-01.txt.
57. *See supra* Section III.A.1.
58. http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf.
59. March 10, 2004 briefing of FTC staff by Microsoft Anti-Spam Manager.
60. http://www.microsoft.com/presspass/press/2004/may04/05-25SPFCallerIDPR.asp.
61. http://antispam.yahoo.com/domainkeys.
62. http://www.nwfusion.com/news/2004/0412marid.html.
63. *Id.*

None of these standards has been widely tested, and each is still in development. Estimates differ on how soon the market will test and widely deploy the competing authentication standards. Some believe that all email will be authenticated within a year.[64] Others are less sanguine. According to a technologist with Comcast, "[i]t might be even two years or more before any one solution is solid enough that it can be deployed even in smaller systems where it's not going to crush them."[65] Small ISPs are especially concerned that the multiple authentication standards will prove too costly to implement.[66]

It should be noted that these private market proposals do not authenticate the identity of the person sending an email. In other words, if a message claimed to be from abc@ftc.gov, the private market proposals would authenticate that the message came from the domain "ftc.gov," but would not authenticate that the message came from the particular email address "abc" at this domain. Nonetheless, domain-level authentication would confound spammers' ability to engage in spoofing and to send messages via open relays and open proxies, enable ISPs to deploy more effective filters, and provide law enforcement with an improved ability to track down and prosecute spammers.

64. Digital Impact: Brondmo, 24 (12 months); Roving Software: Olson, 23 (6 to 9 months).
65. Comcast: Lutner, 46.
66. Aritstotle: Bowles, 75.

Appendix 3:
FTC's Online Consumer Complaint Form

FTC Consumer Complaint Form

OMB #3084-004[illegible]

Use this form to submit a complaint to the Federal Trade Commission (FTC) Bureau of Consumer Protection about a particular company or organization. This form also may be used to submit a complaint to the FTC concerning media violence. The information you provide is up to you. However, if you do not provide your name or other information, it may be impossible for us to refer, respond to, or investigate your complaint or request. To learn how we use the information you provide, please read our Privacy Policy.

While the FTC does not resolve individual consumer problems, your complaint helps us investigate fraud, and can lead to law enforcement action. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel®, a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide.

We use secure socket layer (SSL) encryption to protect the transmission of the information you submit to us when you use our secure online forms. The information you provide to us is stored securely.

IMPORTANT:
* If you want to file a complaint about a violation of National Do Not Call Registry or register your telephone number on the Registry, Please go to www.donotcall.gov
* If you want to file a report about Identity Theft, please use our Identity Theft Complaint Form.
* If you want to file a complaint about an online transaction that involves a foreign company, please use our econsumer.gov complaint form.

If you have a specific complaint about **unsolicited commercial e-mail** (spam), use the form below. You can forward spam directly to the Commission at SPAM@UCE.GOV without using the complaint form.

How Do We Reach You?

First Name:
Last Name:
Age Range: **"Click" Arrow for Choices**
Street Address:
City:
State or Canadian Province: **"Click" Arrow for Choices**
Country: **"Click" Arrow for Choices**
Zip Code or Postal Code:
E-Mail Address:
Home Phone: ( ) *(Area Code)(Phone Number)*

(Numbers Only)

Work Phone: **(**) **Ext.** *(Area Code)(Phone Number)(Extension)*
(Numbers Only)

Social Security Number: - - ***Enter Only For Complaints Relating to the Accuracy of Your Credit Report***
(Numbers Only)

Tell Us Your Complaint...

Subject of Your Complaint: **"Click" Arrow for Choices**

Name of Company You Are Complaining About:

Check If Company Name Is Unknown:

Street Address:

City:

State or Canadian Province: **"Click" Arrow for Choices**

Country: **"Click" Arrow for Choices**

Zip Code or Postal Code:

Company Web Site:

Company E-Mail Address:

Phone Number: **(**) **Ext.** *(Area Code)(Phone Number)*
(Extension)
(Numbers Only)

How Did the Company Initially Contact You? **"Click" Arrow for Choices**

How Much Did the Company Ask You to Pay? *(Numbers Only)*

How Much Did You Actually Pay the Company? *(Numbers Only)*

How Did You Pay the Company? **"Click" Arrow for Choices**

Did You File a Dispute with the Credit Bureau? **"Click" Arrow for Choices**

Did You File a Dispute with the Credit Bureau More Than 45 Days Ago? **"Click" Arrow for Choices**

REPRESENTATIVE OR SALESPERSON
First Name:

Last Name:

Date Company Contacted You: **(MM/DD/YYYY)**

Explain Your Problem: (Please limit your complaint to 2000 characters.):

Submit Complaint | Clear Form

Paperwork Reduction Statement: This form is designed to improve public access to the FTC Bureau of Consumer Protection Consumer Response Center, and is voluntary. Through this form, consumers may electronically register a complaint with the FTC. We estimate that it will take, on average, 5 minutes to complete the form. Under the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. That number is 3084-0047, which also appears in the upper right-hand corner of the first page of this form


sp@m.filter
priv@cy.enforce@bility
dom@in.security
zombie.proxy
children.inbox
f@lse.positive
practical.filter
em@il.priv@cy.com
technic@l.authentic@tion
bayesi@n.filter
rel@y.server.com
anonymous.he@ders
security.em@il.com