My name is Marsha Ferziger Nagorsky, and I am the Director of Internal Communications and Lecturer in Law at the University of Chicago Law School. Among other papers, I am the co-author of "Snitching for Dollars: The Economics and Public Policy of Federal Civil Bounty Programs."[1] I have also taught a course entitled "Electronic Commerce Law" at the University of Chicago Law School for the past five years. I have been asked to consult with the Federal Trade Commission ("FTC") staff on the potential design of a system to pay rewards to private citizens for information leading to successful litigation against spammers. I have talked extensively with the FTC staff, read the FTC's draft report, and given the FTC staff ideas**,** some of which have been incorporated into its report. I have written this assessment at the request of the FTC staff. I support the analysis and conclusions in the FTC's report and believe that they are focusing on the proper set of issues in order to determine whether and how to structure a bounty program for informants on violations of the CAN-SPAM Act ("CAN-SPAM").[2]

I. INTRODUCTION

The FTC staff has informed me that it is interested in using a bounty system to gain information about violations of CAN-SPAM, particularly violations that involve masking the source of the spam and identity of the spammer, which shows the spammer's level of involvement in the spamming activity. The FTC staff say that they ideally seek information about large-scale violators, information key to a successful litigation against the spammer. I will refer to this information as "high value" information. Bounty systems only succeed when they are designed to incentivize informants with high value

[1] Marsha J. Ferziger and Daniel G. Currell, "Snitching for Dollars: The Economics and Public Policy of Federal Civil Bounty Programs", 1999 University of Illinois Law Review 1141 (hereinafter "Ferziger and Currell")**.** This article was published under my maiden name, Marsha J. Ferziger. I now use the name Marsha Ferziger Nagorsky.

[2] 15 USCS § 7701 et seq. (2004).

information to provide it, even where there is likely high risk to them. Should a reward system be deemed a useful part of CAN-SPAM enforcement, this report outlines considerations to be taken into account in its design.

II. TYPES OF INFORMANTS

There are, essentially, three kinds of informants that could possess information about spam. First, there are people who receive the spam and report it, doing no additional work themselves and having no additional information. Second, there are people who track down information about the spammers on their own. Third, there are people who have actual insider information about the spammers, unknown to anyone outside the spam business.

The FTC staff tell me that they already receive information from the first kind of informant – these are the people who send over three hundred thousand pieces of spam daily to spam@uce.gov.[3] The value of this information lies mainly in the aggregation of the data. It is information that the FTC could easily collect on its own. Put simply, this kind of information will flow to the FTC simply because average people are incensed enough to use a simple method provided by the FTC without any other incentive being necessary.

The second kind of informant is the kind Professor Larry Lessig discusses: technically adept citizens who are not simply interested in passing on what they receive, but investigating it themselves.[4] These techies, often known as cybersleuths,[5] can be

[3] Previously, the address uce@ftc.gov was used for this purpose.
[4] Lessig believes that these are the people who need to be incentivized. See, for example, Michael Bazeley, "new Weapon for Spam: Bounty," www.siliconvalley.com, (April 26, 2003).
[5] Cybersleuths is a name that has been given to internet users who believe it is their civic (and netizen) duty to track down lawbreakers in cyberspace and provide that information to the authorities. See Ferziger and Currell at 1193.

skilled at tracing fraudulent headers on spam, often through several relays, and often provide such information to the FTC. It is my opinion that cybersleuths are not the appropriate subject of a bounty program. First, and most importantly, the information that cybersleuths provide is not likely to yield evidence that either identifies the spammer directly, or that is admissible in an enforcement proceeding. Although the cybersleuths might be able to get the information at lower cost than the FTC could (by providing their labor for free), they can rarely identify the spammer due to their absence of subpoena power. It is of only marginal use to the FTC to hear from a cybersleuth that the fourth server in a spammer's relay system is in Indonesia, if they cannot connect that information to a particular spammer. Cybersleuths may have good intuitions, and be able to, on hunch, draw links between information that turn out to be accurate, but such hunches and intuitions often do not constitute admissible evidence. Without subpoena power, the cybersleuth can rarely identify the spammer because much of the evidence as to the spammer's identity is in the hands of third parties who cannot be forced to provide it without compulsory process. Without subpoena power, a cybersleuth cannot take information and turn it into admissible evidence.[6]

Furthermore, the cybersleuth has a considerably lower downside risk to herself than other informants might need to have overcome by a bounty.[7] More importantly, many cybersleuths already inform without financial incentives - they wish to keep the

[6] See FTC Report, Section III.D.2.a., including Footnote 82 and accompanying text.
[7] This kind of informant can be termed a "low risk, high reward" informant. As will be explained later, these types of informants do not generally need bounties to come forward. See Ferziger and Currell at 1193. It is true that spammers are unsavory characters and there might be some risk to any informant, but the risk to an individual cybersleuth would be much, much lower than it would be to an informant with actual connections to a spammer.

internet a clean and legal space and to show off their own skills.[8] The combination of these two facts creates a dramatic risk of over-informing.[9] If there is no risk to the informant and a monetary reward involved, many more people will be incentivized to inform than the FTC would actually want.[10] In addition, there would be a perverse incentive to fabricate tips. Given that the information is not of high value, that the cybersleuth encounters no risk to herself, and that there is a substantial risk of overinforming and fabrication, a bounty system targeting cybersleuths likely would create huge administrative costs to the FTC for very little benefit.[11]

The third kind of informant, the insider, has high value information, and this is the kind of informant that should be the focus of a CAN-SPAM bounty system, if one is established. The insider[12] can have information about actual violations of the Act, actual knowledge by the spammer, and connections between the person and the acts. This is exactly the kind of information that is difficult for the FTC to get by itself. All the

---

[8] John Reed Stark has chronicled such behavior by cybersleuths in both the SEC context and the spam context more than five years ago. Stark notes that cybersleuths provide "painstaking details of potential violations, usually offering identifying information about themselves in case the SEC needs to contact them. Cybersleuths even list the potential securities violations of fraudsters by statute, rule, and regulation, sometimes by precise citation. Cybersleuths receive no reward or bounty for their benevolence, just the satisfaction of helping to keep the Internet clean and safe for all investors, and their numbers continue to swell." John Reed Stark, "Tombstones: The Internet's Impact Upon SEC Rules of Engagement," in *Securities Regulation and the Internet* 793, 837 (PLI Patents, Copyrights, Trademarks & Literary Prop. Course Handbook Series, No. G0-0001, 1998), available in WESTLAW, 520 PLI/PAT 793.

[9] "Over-informing" refers to the situation where an agency is receiving a large number of low-value tips, making it difficult to sort out the tips it can actually use and raising administrative costs substantially. More detail on this is discussed in Ferziger and Currell at 1197-98.

[10] Microsoft, in its report, has raised similar concerns, and raised an additional one. Microsoft is concerned that incentivizing this group of informants could lead to individuals demanding information from ISPs that they are not authorized to provide without a subpoena. ISPs could then be seen as uncooperative, causing consumer backlash. Microsoft Report, n. 27.

[11] While there is always a risk in bounty programs of overinforming and tip fabrication, it is possible to create a program that optimizes that risk. By going after high risk, high reward informants, and providing both high threshold requirements and high payouts, the program outlined in this document should have that optimizing effect. The risk will not go to zero, but it will, at best, minimize administrative costs.

[12] "Insider" in this context can be loosely defined as someone who is within a spammer's chain of independent contractors or who works directly with the main spammer. Other people who have inside knowledge of violations would not be excluded from the bounty system. It may be better to define an informant by the information they provide rather than by their relationships to the spammer on whom they are informing.

research in the world will only lead to servers where subpoena powers do not reach – this kind of informant can break past that problem and provide testimony or even documentary evidence connecting the spammer to the spam. This informant will provide this information only at some (or even great) risk to herself, as she will be informing on someone she as worked with and will be giving up part or all of her livelihood. In addition, there is some reason to believe that spammers, given their already unscrupulous behavior, might be of some threat to more than the livelihood of the informant. These are the informants that the FTC needs, and these are the informants that a bounty system might do the most good in bringing in. The rest of this report will focus on the creation of a system designed to entice this particular type of informer.

III. FEDERAL CIVIL BOUNTY PROGRAMS

Federal agencies have long used bounty schemes[13] to pay informants. Under these schemes, a private informant may receive a portion of any penalties the government receives from legal action taken based on the proffered information. The potential for payment is often large. The IRS, for example, can pay informants up to $2 million just for picking up the telephone.[14] In the first thirty years of the program, more than seventeen thousand informants snitched for the IRS, collectively earning over $35.1

[13] Throughout, I will refer to these systems as "bounty schemes." These schemes are variously known in the literature under such names as "reward programs," "incentive payment programs," and "moiety acts." "Moiety act" is the "name sometimes applied to penal and criminal statutes which provide that half the penalty or fine shall inure to the benefit of the informant." Black's Law Dictionary 1005 (6th ed. 1990). Some courts, however, use the same term for civil bounty statutes, including those that pay nowhere near half to the informant. See, e.g., Doe v. United States, 100 F.3d 1576, 1582 (Fed. Cir. 1996) (finding "moiety statute" money mandating).

[14] See IRS, Pub. No. 733, Rewards for Information Provided by Individuals to the Internal Revenue Service (1997) [hereinafter 1997 IRS Pub. 733]. The payment ceiling was raised from one hundred thousand dollars to two million dollars in 1997. See 1997 IRS Pub. No. 733.

million.[15] The IRS benefits as well; it recovered more than $ 2.1 billion in unpaid taxes during those 30 years because of the program.[16]

There are, essentially, three potential types of bounty schemes with regards to payment. First, there are schemes that pay modest, specified rewards for information, where the amount bears no relation to the recovery in the case. For example, the Environmental Protection Agency pays up to $10,000 for information on illegal dumping of hazardous materials.[17] Second, there are bounty schemes that provide payment on a percentage basis – the informant receives a percentage of any money the government actually recovers. These schemes target people with special information and include the potential for large rewards, but also the potential to receive nothing if the case fails or the defendant is judgment proof. Third, there are schemes that pay a percentage of the amount the government is intended to receive, whether or not the government ever recovers any money. These provide greater certainty (although not true certainty) to the informant, while still dangling large rewards in front of them.

There are three notable programs[18] that fall into the second and third categories. In 1988, Congress created legislation allowing the Securities and Exchange Commission

---

[15] 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 I1. The IRS program began in 1967.

[16] See id.; see also Lee Benson, Here's Truth: Lying Is Just Rampant, Deseret News (Salt Lake City), Aug. 19, 1998, at B1.

[17] 42 USC § 9609(d), 40 CFR 303.10 (1989). See also Matthew Lesko, Uncle Sam Pays Cash to Private Citizens Who Provide Information About Wrongdoings, Chi. Trib., Nov. 1, 1993, at C3.

[18] There are two other programs that are similarly modeled. The federal savings and loan industry bounty program, set out in the Financial Institutions Reform, Recovery, and Enforcement Act of 1989, at 12 U.S.C. 1831k (1994), has not gotten any real use but exhibits the same set of factors as the programs modeled here. Rewards are available under the federal False Claims Act ("FCA") for those providing information regarding frauds perpetrated upon the government. See 31 U.S.C. 3730 (1994). Under the FCA, private citizens - known as "relators" - must actually initiate litigation against a defrauder. See id. 3730(b). Because of the "relator" concept, the False Claims Act will not really be discussed here. It is an unusual situation for the government to allow citizens to sue on its behalf, and the FCA is special because it focuses on economic wrongs done to the government. It is hard to imagine that spam would be a similar type of injury, and even if it were, it is difficult to imagine high-risk informants, such as the ones sought here, suing on

(SEC) to award bounties to those who provide information leading to the successful prosecution of an inside trader.[19] However, the SEC appears to have awarded only three bounties in the decade since it promulgated regulations for administering the program.[20] The SEC bounty scheme was originally predicated upon the IRS's successful program of informant rewards. That program, which receives more than ten thousand bounty applications a year,[21] remains a benchmark of how informant rewards can enhance administrative enforcement of federal regulations. In addition to the IRS, the U.S. Customs Service has also long been authorized to award bounties for helpful information.[22]

A. SEC Insider Trading Bounties

In response to growing concerns over insider trading in the early 1980s, and spurred on by Wall Street scandals, the Insider Trading and Securities Fraud Enforcement Act of 1988 (ITSFEA)[23] moved quickly through Congress and was immediately signed by President Reagan. ITSFEA gave the SEC the right to award bounties to "the person or persons who provide information leading to the imposition" of a monetary penalty for insider trading.[24] Under the statute, a bounty cannot exceed ten percent of the money

---

behalf of the government. Furthermore, FCA cases have large sums of money at stake – more than enough to make it worth a relator's while to file suit and seek 15 to 30 percent of the recovery. Spam cases, on the other hand, have quite a low average payout, thus making it unlikely that any relator would ever bother to pursue a case. It should be noted, however, that CAN-SPAM gives ISPs a private right of action. This provision makes sense, as ISPs have many incentives to sue other than recovery of penalties. Other than the relator provision, all the other parts of the FCA bounty scheme are duplicated in the IRS, SEC or Customs schemes.

[19] See Insider Trading and Securities Fraud Enforcement Act of 1988, 15 U.S.C. 78u (2000).

[20] The SEC program has been used very little since its inception. See FTC Report p. 28, n. 76 and accompanying text. See also http://www.sec.gov/litigation/litreleases/lr17476.htm.

[21] See infra Table 2.

[22] See 19 U.S.C. 1619 (1986).

[23] Pub. L. No. 100-704, 102 Stat. 4677 (codified in scattered subsections of 15 U.S.C. 78).

[24] Id. 3(a), 102 Stat. at 4679 (codified at 15 U.S.C. 78u-l(e)) (2004).

penalties imposed in a case.[25] Since the maximum penalty a court may impose upon an inside trader is three times the trader's gain or avoided loss, the maximum bounty is thirty percent of the inside trader's take as calculated by the court.[26]

Congress intended the ITSFEA bounty scheme to increase the inflow of insider trading information to the SEC. The SEC implemented the program in 1989 with a series of regulations.[27] The SEC encourages informants to file applications stating the relevant information regarding the illegal trades and providing informants' names, addresses, and signatures.[28] This disclosure is not mandatory, however, and under the regulations, informants wishing to remain anonymous must simply apply for a bounty within 180 days after the entry of a court order in the case their information helped to initiate.[29] Although the application requests informants' names and addresses, this information may be omitted until after the case has been resolved - at which time it must be divulged.[30]

Awards are entirely within the discretion of the SEC and not subject to judicial review.[31] Perfectly good information from informants may lead to no reward if the Commission so decides. Informants will not receive money from the government until the government receives its penalty money from the inside traders. Thus, informants are not paid if the defendants are judgment-proof.[32] To protect the integrity of the regulatory process, certain federal employees and employees of self-regulatory organizations are not

---

[25] See id.
[26] See id.
[27] See Applications for Bounty Awards on Civil Penalties Imposed in Insider Trading Litigation, 17 C.F.R. 201.61 - .68 (1999).
[28] See SEC Form 2222, supra note 115.
[29] See 17 C.F.R. 201.63.
[30] See id. 201.65.
[31] See 15 U.S.C. 78u-l(e) (1994) ("Any determinations under this subsection, including whether, to whom, or in what amount to make payments, shall be in the sole discretion of the Commission... Any such determination shall be final and not subject to judicial review.").
[32] Bounties are available only from "amounts imposed as a penalty under this section and recovered by the Commission or the Attorney General." Id.

eligible for rewards, and other federal employees may not claim rewards based on information gained in the course of their employment.[33]

The statute authorizing SEC bounties does not require any procedures for the maintenance of informants' anonymity, so any assurances to that effect come from the SEC's own regulations. Under the regulations, bounty applicants may remain anonymous so long as they provide sufficient evidence to identify them later as the source of the information.[34] Thus, informants may anonymously provide information to the SEC and wait for a case's result before filing. Informants may, therefore, remain anonymous in the event that the case is unsuccessful. Before collecting a reward, however, informants must provide their names, addresses, and signatures for the Commission.[35] SEC regulations make no mention of anonymity, but in one of its publications, the SEC offers the following comfort to those who would snitch on the likes of Ivan Boesky.

> Absent compelling cause, the Commission ordinarily does not disclose the identity of a confidential source. In some instances, however, disclosure of that identity will be legally required or will be essential for the protection of the public interest. For example, a court may order disclosure during litigation, or the Commission may need to present the testimony of a bounty claimant to ensure the success of an enforcement action. Consequently, while the Commission and its staff will seriously consider requests to maintain the confidentiality of a source's identity, no guarantees of confidentiality are possible.[36]

The SEC's program does not currently get a great deal of use. As noted above, only three bounties have ever been paid out under this program. There are a number of potential reasons for the lack of use of this program. Some reasons may be part and

[33] This provision impairs the SEC's absolute power to award bounties by providing that awards may not be made to "any member, officer, or employee of any appropriate regulatory agency, the Department of Justice, or a self-regulatory organization." Id.
[34] See 17 C.F.R. 201.64 - .65.
[35] See id. 201.65.
[36] SEC Form 2222, supra note 115.

parcel of the SEC's statutory scheme, such as the lack of anonymity and fear of retaliation, or a potential reward amount that is insufficient. Other reasons that the SEC program is less used may come from the kinds of potential informants in insider trading cases. These informants are, by the nature of the crime, often likely to be high-level insiders themselves. They may be making too much money from illegal activity to make informing worth their while, or they themselves may likely be implicated and thus perceive the risk to be too high for them to come forward without promise of immunity. Finally, it is probably fairly common that the insider would only have such information if he or she were a trusted friend or family member of the people he or she would be turning in, thus making it unlikely that they'd inform no matter the amount of the bounty involved.

B. IRS Informant Reward Program

In 1867, Congress passed an internal revenue bill providing that "the commissioner of internal revenue... is hereby authorized to pay such sums... as may in his judgment be deemed necessary for detecting and bringing to trial and punishment persons guilty of violating the internal revenue laws."[37] Since 1867, the statute has remained essentially the same, though Congress clarified its administration in 1996.[38] Under current IRS regulations, any person not a present or former Treasury Department employee[39] who has provided information leading to the successful recovery of taxes is

[37] An Act to Amend Existing Laws Relating to Internal Revenue, and for Other Purposes, ch. 169, 7, 14 Stat. 471, 473 (1867).
[38] The IRS bounties provision is now codified at I.R.C. 7623 (1996).
[39] The informant cannot have been an employee of the Department of the Treasury when he came into possession of the information. Other federal employees are eligible so long as they did not gain the information in the course of their duties. See Treas. Reg. 301.7623-l(b)(2) (1999).

eligible to file a claim for an informant reward.[40] As with SEC bounties, the IRS does not guarantee rewards, and courts may not ordinarily review IRS determinations.[41] According to IRS regulations, rewards will "generally not... exceed fifteen percent"[42] of the taxes recovered, and the total reward is not to exceed two million dollars.[43] Until October 1997, the ceiling was ten percent or $100,000,[44] but in some cases individuals had bargained for more.[45] As with ITSFEA, the anonymity provisions in the IRS bounty scheme stem from agency regulations, not the statute. Unlike the SEC, however, the IRS promises to keep its informants anonymous throughout the process, and it appears that its promises are kept.[46]

IRS regulations state that "any person... [who] submits information relating to the violation of an internal revenue law is eligible to file a claim for reward under section 7623."[47] IRS Publication 733 makes clear that the size of an informant's reward will be determined based on "the value of information... furnished voluntarily and on [his] own initiative with respect to taxes, fines, and penalties (but not interest) collected" and that

---

[40] See id. 301.7623-1. This type of program is not unique to the United States. See, e.g., Tom Korski, International Taxes: China Will Pay Informants Who Turn in Corporate Tax Evaders, Daily Tax Rep. (BNA) No. 208, at G-1 (Oct. 28, 1997).

[41] See Saracena v. United States, 508 F.2d 1333, 1335 (Ct. Cl. 1975) (quoting United States v. Shimer, 367 U.S. 374, 381-82 (1961)).

[42] Treas. Reg. 301.7623-1(c) (1999). The change from 10% to 15% passed in October 1997 but was given retroactive effect to January 29, 1997. See Temp.Treas. Reg. 301.7623-1T(g).

[43] See 1997 IRS Pub. 733, supra note 6. The IRS will not pay rewards "if the recovery was so small as to call for payment of less than $ 100." Id.

[44] See 1987 IRS Pub. 733, supra note 6.

[45] In Stack v. United States, 25 Cl. Ct. 634 (1992), the court reported that Anthony Stack bargained with the IRS prior to providing the agency with information regarding tax fraud by K-Mart. According to the terms of the agreement, the reward would be calculated as "up to five percent of the net tax deficiencies, penalties, and fines subsequently collected as a direct result of information supplied, the total of all payments not to exceed $ 5,000,000." Id. at 635. Although Mr. Stack earned the IRS something in the nature of $ 100 million, the IRS determined that in awarding him "up to five percent" of the take, it would simply give him $ 182,743. See id. at 636, 638.

[46] IRS regulations allow claimants to provide tax fraud information under an alias and guarantee that "no unauthorized person shall be advised of the identity of an informant." Treas. Reg. 301.7623-l(e); see also 1997 IRS Pub. 733, supra note 6 (reiterating these points); 1987 IRS Pub. 733, supra note 6.

[47] Treas. Reg. 301.7623-l(b)(l).

the informant's tip must cause the investigation.[48] In the IRS's agreement with Anthony Stack, who provided the Service with information leading to a $ 100 million recovery from K-Mart, the Service agreed to pay a reward "upon receipt of valuable information... not previously known by the [IRS]... which results in the collection of taxes."[49] Understandably, the IRS will pay neither for information it already has nor for information that does not lead to an investigation.[50]

The IRS has other reward systems available that do not require payment of informants out of proceeds. For example, the Internal Revenue Manual allows for payments to confidential informants, cooperating witnesses or cooperating defendants from internal funds.[51] These payments have much in common with the above reward system, especially in that employees of the IRS are in no way authorized to provide an informant assurances of being paid a specific amount or being paid at all.[52]

C. U.S. Customs Service Rewards

Customs officials, like the IRS, have long been authorized to give rewards to informants providing information relating to the violation of Customs laws. Under the current system, persons who are not federal employees or officers[53] and provide information leading to the seizure of a vessel or baggage subject to seizure are eligible for rewards of up to twenty-five percent of the take.[54] Under the Customs rules, private citizens not only may provide information regarding Customs violations but also may

[48] 1997 IRS Pub. 733, supra note 6.
[49] Stack, 25 Cl. Ct. at 635.
[50] See 1997 IRS Pub. 733, supra note 6.
[51] Internal Revenue Manual section 9.4.2.5.5.4.
[52] Internal Revenue Manual section 9.4.2.5.5.4.(j).
[53] See 19 U.S.C. 1619(a)(1) (1994). Federal employees who circumvent this provision by contracting with another person for a share of the bounty (or in any other way) are subject to civil and criminal penalties. See id. 1620; 19 C.F.R. 161.12 (1999).
[54] See Tariff Act of 1930, 19 U.S.C. 1619 (1994).

actually seize the vessels or baggage in question as long as the seizure is reported immediately.[55] The total award cannot exceed $250,000 for any case,[56] but Customs pays otherwise eligible informants even when their information leads to the seizure of goods that cannot be liquidated.[57] Rather than paying informants directly from the proceeds of their cases, the Customs Service pays rewards from its appropriated funds.[58]

The Customs scheme's method of payment introduces at least one complication into the system. Because the contraband cannot be sold legally, it has no inherent value that can be used to determine the bounty payment. Congress has left open the question of what amount of bounty should be paid in drug cases. Informants subject to the drug bounty laws may still be paid; title 21 provides for payment of any amount the Attorney General deems appropriate.[59]

Unlike the SEC and IRS reward programs, courts may review Treasury Secretary decisions regarding Customs rewards. The Customs scheme leaves the Secretary with less discretion than either IRS district directors or SEC officials have in their own respective bounty programs. A line of cases has held that the statute gives informants a right to compensation if they fulfill the requirements of the section.[60] The Customs Service administers its bounty system under a rule similar to the IRS's. According to the Tariff Act of 1930, an informant must provide "original information" concerning a fraud

---

[55] See id. 1619(a)(1)(A).
[56] Customs will not pay awards of less than $ 100. See id. 1619.
[57] See id. 1619(b). The two instances listed are when the property is destroyed or when the property is turned over to the government for official use. In these cases, the amount of the bounty is calculated as “an amount that does not exceed 25 percent of the appraised value of such forfeited property.”
[58] See id. 1619(d).
[59] See 21 U.S.C. 886(a); see also Pomeroy v. United States, 39 Fed. Cl. 205 (1997), rev'd on other grounds, 173 F.3d 432 (Fed. Cir. 1998); Nicolas v United States, 35 Fed Cl 387, 389 (1996).
[60] See, e.g., Wilson v. United States, 135 F.2d 1005, 1009 (3d Cir. 1943) (holding that the Customs statute's use of the term "may" rather than "shall" with regard to the Secretary's award of bounties was not dispositive of the question of the Secretary's discretion); see also supra Part II.A.3.

upon the U.S. Customs Service.[61] By statute, the Customs Service must preserve an informant's anonymity,[62] and the protections are even stronger than the usual confidentiality provisions of the Customs law.[63]

The Customs Service also has an additional program at its disposal. The Department of the Treasury Forfeiture Fund, established by 31 USC § 9703, provides a Treasury Department fund available to the Secretary of the Treasury for the payment of expenses related to seizures and forfeitures.[64] This fund may be used for payment of "awards of compensation to informers under section 619 of the Tariff Act of 1930 (19 U.S.C. 1619)."[65] In addition, this Fund may be used to pay 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"[66] and "purchases of evidence or information" in a number of situations, including violations relating to money laundering, drug smuggling, coins and others, all at the discretion of the Secretary.[67] These payments are not in any way tied to recovery of penalties or any other funds by the government and are entirely discretionary.

[61] See 19 U.S.C. 1619(a)(l)(B) (1994).
[62] See 19 C.F.R. 161.15 (1999) ("The name and address of the informant shall be kept confidential. No files or information shall be revealed which might aid in the unauthorized identification of an informant.").
[63] See 19 C.F.R. 103.12(g)(4)-(i) (1998).
[64] 31 USC 9703(a) (2004).
[65] 31 USC 9703(a)(1)(C) (2004).
[66] 31 USC 9703(a)(2)(A).
[67] 31 USC 9703(a)(2).

D. Summary of Program Characteristics

The characteristics of these bounty programs are summarized in table 1.

	SEC	IRS	Customs
Eligibility and Threshold Conditions a. Gov't employees	No payment to members, officers, or employees of appropriate reg agencies, the DOJ, or an SRO.	Current / former Treasury employees ineligible. Other fed employees ineligible with work-gained info.	Employees and officers of the United States ineligible.
b. Co-conspirators	Co-conspirators eligible only before investigation begins.	Can pay regardless of guilt or innocence.	[Regulations do not provide any information about co-conspirators.]
c. Threshold conditions	Information leading to penalty for insider trading.	Info leading to successful tax recovery. Tip must cause investigation.	Original information leading to seizure of vessel or baggage.
Amount	Can not exceed 10% of money penalties.	Not normally > 15% of recovered taxes. Total not > $2M, nor < $100.	Up to 25% of the take, total not > $250,000 and not < $100.
Judicial review, guarantee and discretion	Not reviewable. No guarantee, by statute. Full agency discretion; good info need not get award.	Not normally reviewable. No guarantee, by statute.	Reviewable if under 19 USC 1619. Guarantee, by judge-made law. Entirely discretionary if under 31 USC 9703.
Payment	Paid out of penalties received.	Paid out of penalties received.	Paid out of Customs coffers, paid even if items do not lead to recovery.
Anonymity	Anonymous on filing, identity must be divulged after case is closed.	Anonymity guaranteed.	Anonymity guaranteed.

Table 1 – Characteristics of the Four Examined Bounty Programs

E. Analysis of Bounty Programs

There are five basic parameters that affect the success of bounty programs:

1. What threshold conditions must an informant meet to be eligible for a bounty?

2. How much is the bounty?

3. Is the amount guaranteed if certain requirements are met? If not, how much discretion does the agency have over the amount of the reward, and is that discretion subject to judicial review?
4. From what source are bounties paid?
5. Can the informant remain anonymous throughout the process?[68]

1. Eligibility and Threshold Conditions

The first step in designing a bounty system, should Congress decide to implement one, will be determining who will be eligible for a bounty. There are three main conditions generally discussed in eligibility requirements: federal employee eligibility, co-conspirator eligibility and threshold conditions.

In the case of a CAN-SPAM bounty scheme, the first two parts of eligibility would be quite clear, given that the intent is to find insider informants. Federal employee eligibility generally involves determining whether a federal employee may receive a bounty for providing information obtained in the course of her work. This will not apply here under a bounty system intended for insiders. By way of contrast, any CAN-SPAM bounty system must allow bounties to co-conspirators, as insiders will, at the very least, be potential co-conspirators. By stating explicitly that the bounty system is targeting insiders, and that co-conspirators will be eligible for bounty payments, the FTC would likely accomplish its goals on this front.

The more difficult component is defining what the informant must do and what the result of the information must be. Other bounty systems have been vague on the threshold conditions, and probably intentionally so, in order to preserve agency discretion to give bounties. The FTC report, on the other hand, has indicated that if Congress

[68] Ferziger and Currell, at 1145.

should decide to implement a reward system, such a system should encourage only insider informants with high-value information to come forward. Thus, being stricter about the threshold conditions, while still maintaining flexibility for purposes of increasing the chances of receiving high value information, will meet the goals of the CAN-SPAM Act.

If a bounty system for spam is created, I would propose that eligibility be limited to informants with high-value information, most notably insiders. One possible way to do this is to specify that only certain provisions of the Act – provisions the violation of which involve an inherent level of deception – be included within the scope of a reward system. Another possible way 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. To create a higher level of incentive for the informant, reward eligibility could be tied to the imposition of a final court order. It is important to note the definition of "successful imposition of a final court order." The FTC staff have told me that successful imposition of a final court order is the issuance of an injunction either as a result of a trial or a settlement filed in court.[69] It is important to insist that the information lead to successful imposition of a final court order – if not, the informant could back out too soon, the case could fail, and yet a bounty could still be demanded.

These threshold conditions have the advantage of including both bright line and discretionary rules. No solution will perfectly yield all the information the FTC wants with none that it does not, but if a bounty system is implemented at all, it is important to

[69] Many of the FTC cases are filed in federal district court under section 13(b) of the FTC Act. In these cases, the FTC often seeks consumer restitution under the equitable discretion of the court. Civil penalties are not available to the FTC in section 13(b) actions. See FTC Report p. 16, n. 37 and accompanying text.

give an opportunity for as much of the best information possible to come through, while still discouraging low value informants. The solution above, if utilized, would likely accomplish this. If the two possibilities above were used as ways to narrow eligibility, the scheme would provide a bright line rule – the information relates to violation of one of a specified set of provisions of CAN-SPAM, leading to successful imposition of a final court order. This would be easy to implement, but if this were to be the only rule, it would necessarily leave out an important group of informants that the FTC would want under such a system. Thus, the second category – the informant who provides information about knowledge – would be a necessary component. This rule would naturally require more analysis to determine whether the condition has been met, but without it, the bright line rule would be overly narrow and the FTC would miss out on important information. This is the age-old tradeoff between bright line and discretionary rules – bright-line rules are easy to implement but always overly narrow or overly broad, and discretionary rules are more difficult to implement but much more flexible in providing detailed results. If Congress wishes to implement a bounty system, it should seek to provide incentives to optimize the number of high-value informants, while still keeping out a majority of the low-value informants – thus making necessary a combination of bright-line and discretionary rules.

2. Amount and Payment

The next consideration for any potential FTC bounty system is the amount of the bounty to be paid. It is crucial to provide enough of an incentive to get high-value informants to overcome their potential risks, while not enough to have false informants

coming out of the woodwork. Current federal bounty schemes vary a great deal in the amount paid.

As noted above, there are three types of payment systems: paying a specific amount not tied to recovery, paying a percentage of the amount the agency recovers, and paying a percentage of the amount awarded in the case regardless of whether any amount is actually recovered. Each of these schemes has its benefits, much like the bright-line vs. discretion discussion above. The key to determining the appropriate payment scheme depends on the likely results of the agency's enforcement actions. The modest, specific reward entices informants with good information but low risk. It provides a certain reward, but a small one, and does not entice with potentially large payouts. This is an appropriate scheme for agencies looking for medium-level information from low-risk informants, at relatively low payout cost to the agency, where large financial recoveries are not expected by the agency. The percentage reward is very much the opposite, luring out high-risk, high-value informants with huge potential payouts. This has the added benefit of automatically being revenue-positive for the agency, since the agency will only pay rewards out of recoveries. This type of scheme works for agencies for which large recovery of penalties is expected and whose potential informants may experience significant risk to themselves. Perhaps most importantly, this scheme works best when informants might have an inflated sense of how much the recovery might be. The IRS is a perfect example of this kind of scheme at work – the IRS routinely collects large amounts from tax fraud cases, and the promise of a percentage of such recoveries is enough to bring out high-value informants. Finally, the percentage not paid from proceeds incentivizes a similar type of informant to the other percentage schemes, but

works better for agencies that do not often recover large penalties. The fact that rewards are paid even when no money is collected makes up, in the mind of the informant, for the fact that the agency is more likely to, for example, get an injunction but no penalty – the certainty of the agency's revenue stream is replaced by the certainty of a payout even if no money is recovered. The Customs scheme is an excellent example of this – much of what Customs seizes has no value unless sold illegally, and thus any percentage of a Customs recovery will often lead to no bounty. Thus, Customs pays regardless of whether it gets any revenue.

The appropriate payment scheme for a potential FTC bounty system is a combination of the first and third types. The FTC's goal for informants would optimally be to reach the potentially high-risk, high-value informant and to provide her with some certainty of reward. On the other hand, the FTC is not as capable of revenue collection as of getting injunctions. The reality is that the majority of spam cases are likely to result in penalty amounts well below what the statutory language might imply, due to the statutory factors that the court must consider in determining what penalty, if any, will be paid in even a successfully brought case.[70] Thus, the appropriate way to set up a CAN-SPAM bounty system is to use the specific, non-tied reward system, but to make the amount in question an "up to" amount that still allows for potentially large payouts. This would serve the goal of paying an amount that does not depend on the success of recovering penalties, but still would leave the potential carrot of a large payment that may make it worthwhile for the highest-risk informants to come forward.

It is very important to note here that the amount should not be anything that could be considered a "sum certain." Case law, particularly in the U.S. Customs area, has

[70] See FTC Report p.18, n. 44 and accompanying text.

sometimes found 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.[71] Thus, courts may find a binding contract, remove some discretion from the agency, and judicially review the payment of informants – exactly what the FTC would likely wish to avoid. If such contracts were to be found, it is easy to imagine the FTC spending all of its time defending eligibility disputes at high cost to the agency, instead of using the information to catch spammers. The best thing to do is to have the base amount (the amount paid regardless of what the government receives from the suit) be listed as "up to" a specific dollar amount.

The amount of the payment that would optimize informing is difficult to ascertain. The FTC staff likely have little reliable evidence about the business activities of the informants they currently seek – how much money these potential informants make from their activities, how much risk they may be at from their targets, how much incentive they may need to come forward. The only way to determine this amount may be trial and error, informed by the best guesses of the people and organizations with the most knowledge of the target informants. According to the FTC report, reward amounts could be in the range of $100,000, and in some cases as high as $250,000.[72] This is not unreasonable, given that many, if not all, of the informants will be giving up their lucrative (albeit illegal) livelihoods and risking potential legal action themselves. These amounts are speculative amounts, and may need to be adjusted based on the level of informing that actually materializes. However, these amounts are unlikely to be too

[71] See Wilson v. United States, 135 F.2d 1005, 1009 (3rd Cir. 1943), Lewis v. United States, 32 Fed. Cl. 59, 63 (1994) 9analyzing the effect of the 1986 amendments and upholding Wilson).
[72] See FTC Report p. 40 n. 111 and accompanying text.

large, given the quality of the information sought and the potentially enormous downside risk to the informant.

This reward amount cannot likely be achieved by way of specific legislation of it without creating the "sum certain" discussed above. Further, listing the amount as "up to," for example, $50,000 would not provide the incentive of a potentially very large payout that would be needed to bring in the most desirable informants. To avoid being a sum certain, an appropriate amount to offer initially might be "up to $250,000," with the intent that most payments would be in the $100,000 range, and the max payment would be awarded whenever warranted and publicized whenever awarded.

It is quite important that the bounty be paid regardless of whether the FTC collects penalties. Therefore, there will need to be a fund out of which to pay. Without such a fund, there will be little incentive to inform, because, as described in the FTC report, even where a judgment is granted the FTC often does not collect sufficient funds to be used for such payments. As the FTC report states, the likelihood of the FTC generating large revenues from spam cases – whether in the form of civil penalties or equitable monetary relief – is relatively low.[73] If a reward is tied to penalties, the public will quickly discover that such penalties are unlikely to yield big rewards for them, thus undermining the incentive to inform. If, however, the informant does not connect the likelihood of recovering penalties to the base amount of her award, she can be confident of some meaningful payout, while also likely to overestimate the likelihood of being one of the $250,000 cases. This combination would allow for the best combination of certainty and dreaming.

[73] See FTC Report section II.C and p. 36, n. 97 and 98 and accompanying text.

The informant reward fund need not be exceedingly large. This system would be designed to apply to only a small number of informants. These cases go on for a long time, and payments would only be made at the conclusion of successful imposition of a final court order. Even if six informants meet the requirements for the reward each year, with five averaging to $100,000 and one receiving the maximum,[74] the fund would only pay out less than $750,000 a year.[75] This might be a very small price to pay for stopping the high-value targets who these informants would be helping to bring to justice. Compared to the massive amount of financial cost created by spam[76] and the amount ISPs alone spend in fighting spam, three-quarters of a million dollars is nearly negligible. In fact, Congress might prefer for the fund to get even more use – it would not only be proof that the system was working, but might greatly reduce the spam problem.

By the same token, it is important, even though the recommended system would provide the discretion to pay out any amount up to $250,000, the FTC would likely want to pay an average amount close to the recommended $100,000, pay the maximum whenever it is warranted, and then publicize these payments a great deal. It is important

---

[74] Ten informants a year would seriously exceed my expectations. Due to the high threshold requirements and small number of informants targeted, I would expect that to be an upper limit that would never be reached in practice.

[75] Note that the fund set up for a similar program under the Customs service has been at least $50 million a year since 1994. See 31 USC 9703(g).

[76] Cost estimates for the "spam problem" vary widely. One research company put the cost of spam to US businesses in 2003 at $10 billion, which included "lost productivity and the additional equipment, software and manpower needed to combat the problem." See http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12. Another firm puts the cost at $874 a year for every office worker who has an e-mail account. That comes out to an approximate $87 billion United States spam burden. See http://www.lexisone.com/balancing/articles/n080003d.html One company trying to sell spam filtering software has a calculator on its website to determine the cost of spam to a single company. The site calculates that if a company has 100 employees earning $25 an hour, each receiving 25 spam messages a day (a serious underestimation for many people), the annual cost of spam will be just under $20,000. See http://www.cmsconnect.com/Marketing/spamcalc.htm. Calculating only for myself, at my hourly consulting rate, and averaging my current minimum of 200 spam messages a day, my annual spam cost alone is $6388.89. Other more sophisticated calculators, taking into account costs of computers, ISP accounts and the like, are available on line, including http://www.tmisnet.com/~strads/spam/costcalc.html

that the public see that payouts are often considerable. In order to entice the best informants, the publicity should lead them to realize that the amount they are likely to get is close to $100,000, with the potential for the believing that the more amorphous "up to" $250,000 could net them a huge payout.

3. Anonymity

Many federal bounty schemes incorporate a guarantee of anonymity for the informant. It is easy to see why this might entice more people to inform in the spam case – most of the informants will be implicated in the schemes themselves, and may have unsavory people quite unhappy with them for providing information to the government.

Should Congress choose to implement a bounty system, the FTC should provide anonymity to its informants, following the guideline of the IRS bounty program. The IRS program allows informants to be anonymous throughout the entire process, including after the bounty is paid, and makes their identities undiscoverable under FOIA at any time. Obviously, should the testimony of the informant be necessary, the FTC and the informant will have to make a decision. If the informant's testimony is crucial, they may be comfortable giving up their anonymity knowing that there will be no bounty at all if they do not assist in bringing the litigation to a successful close.

Anonymity is often important to informants because they may have relationships, business or otherwise, with the people on whom they inform. Some informants will be long-time associates of the violators, and without anonymity, they will fear retribution. In addition, there may be a friendship or other personal relationship. There must be a substantial financial incentive to get such an informant to come forward.

Anonymity may be a tricky issue given that many informants will themselves be guilty of crimes. The FTC staff indicate that the FTC does not have the authority to grant immunity from criminal prosecution to these informants, given that it is a civil law enforcement agency. Even if it were a criminal law enforcement agency, immunity is never a guarantee *ex ante* – the informant has to negotiate for it. This uncertainty about both anonymity and immunity may be enough to keep some informants from coming forward. At the very least, this is another reason why the initial payment to the informant must be quite high – it must be enough to overcome the fear not only of losing a stream of income and business relationships, but also overcome the uncertainty ex ante of being able to negotiate immunity.

4. Judicial Review, Guaranteed Recovery and Agency Discretion

The FTC staff have indicated a justified concern about potential liability for the FTC if an informant is displeased with a decision not to pay. If a reward system were to be created, any statute implementing this bounty program should be careful not to expose the FTC to such liability.

Existing bounty programs show how this can be accomplished. First, the statute must say explicitly that the payment of bounties is entirely within the agency's discretion and not subject to judicial review. The SEC bounty scheme has such a provision,[77] and the IRS bounty scheme has less concrete language[78] that has nevertheless been held by courts to leave awards entirely within the discretion of the Internal Revenue

[77] 15 U.S.C. s. 78u-1(e) (1994).
[78] 26 I.R.C. s. 7623 (West Supp. 1999).

Commissioner.[79] The original language in the Customs statute was not specific on discretion and was found by some courts to take some discretion away from the agency,[80] probably prompting the SEC's explicit language. The language of the SEC statute should be the model, to be as explicit as possible on this point.

The IRS and SEC programs also disclaim any obligations based on promises made to informants. The SEC states that no one is authorized to bind the that agency with regard to a payment or to the amount.[81] An informant, therefore, has no reason to believe that any deal he makes with the SEC staff regarding a bounty will be enforceable. Through this provision, the SEC has blatantly refused to yield its sovereign immunity. This should be built into any CAN-SPAM reward scheme as well.

Perhaps most importantly, if a reward system is implemented, Congress should explicitly provide that FTC decisions about which cases to pursue are not subject to judicial review, nor are its decisions about how it pursues the cases that do move forward. The FTC must never make or seem to make decisions about its cases based on the fact that a bounty may be paid or not, but even more crucial is that there be no judicial review of the FTCs decisions based on the fact that different tactics by the FTC might have yielded a bounty.

Pure agency discretion and lack of judicial review would dramatically decrease the cost of this program by reducing[82] lawsuits against the FTC for non-payment of

[79] See, for example, King v. United States, 168 F.3d 1307 (Fed. Cir. 1999).
[80] See Wilson v. United States, 135 F.2d 1005 (3d Cir. 1943). The Customs Service changed this language in its 1986 amendments, but later courts have still held the act to require payment, although the amount of the payment is now within the agency's discretion. See Lewis v. United States, 32 Fed. Cl. 59, 63-64 (1994).
[81] 17 C.F.R. s. 201.68 (1998).
[82] It is difficult to anticipate how many lawsuits will be filed, although building these provisions in will dramatically reduce or even the agency's liability in these suits. Obviously, there is a risk of frivolous

bounties. It is important, however, that the FTC make a practice – and a very public one – of paying out bounties whenever they are warranted. Agency discretion can introduce a great deal of uncertainty into the system, and such uncertainty can prevent informants from coming forth. If the agency shows itself willing to pay bounties when they are deserved, it will go a long way to curing that uncertainty and likely decrease both filed lawsuits and any potential liability.

5. Administrative costs

The most important concern to any agency in creating a bounty system is the administrative cost involved. As much as the FTC might like to gain information to successfully prosecute major CAN-SPAM violators, it is not worth it if it brings the agency to its knees in the process. A poorly developed bounty system could bury the FTC in low-quality and false leads as well as force it to spend precious time and resources fighting frivolous lawsuits about bounties. If implemented, the scheme developed in this report is designed to avoid both of those problems.

Administrative costs would likely be greatly lowered by making the eligibility requirements very strict – it would not be in the interest of most low-level informants to go through the bounty system, as it will be quite clear that they are not eligible. In addition, restricting the bounty system to only certain types of information on certain violations should provide a bright-line rule preventing most low-level informants from applying for bounties and from suing the FTC over this program. Finally, the combination of complete discretion by the FTC, no judicial review, and the generous

---

lawsuits. On the positive side, the IRS, which has the most-used bounty program currently in existence, has had to take very few cases to final judgment.

payment of bounties under the system might help reduce the number of costly lawsuits that other programs have faced.

Of course, all of these cost-saving devices themselves have a cost – every limitation put on the program will exclude some potential informants that the FTC could find valuable. For a program to prove workable, however, the key is not receiving every bit of information available – that would provide far too much bad information with the good. The key is *optimal* informing – getting the most high-value information for the least administrative cost.

6. Deterrence

The existence of a bounty system might be beneficial even if no one ever used the reward system. After all, it is distinctly possible for a well-considered bounty program to be put in place and for no one to step forward to use it.[83] I believe that the very existence of this bounty program, even on the off-chance that it was never used, could provide a very real benefit: deterrence.

If implemented, the FTC will clearly promote its bounty system widely as part of its own enforcement efforts. Those spammers that the FTC is targeting will certainly know quite quickly about the program. From the moment of implementation, any spammer will be aware that anyone he comes in contact with is a potential informant. Spammers will have to be more cautious and will likely be forced to curtail some of their activity. On the other hand, it is possible that these spammers may be driven to even more devious tactics, making it more difficult to prove individual liability. Given, however, that the entire purpose of a spammer's business is to stay one step ahead of

[83] See infra note 20.

detection methods in the first place, I believe that there is a relatively small downside risk to creating this form of deterrence, and a chance that the very existence of the program will decrease spam even if no one ever uses the program.

IV. CONCLUSION

Any system designed to incentivize private citizens will have its pros and cons. If a reward system is implemented, I believe the issues discussed in this report are important to maximizing the efficiency of such a program and should be given careful consideration.