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

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.

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.

(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]

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 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).

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**<br><br>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. | |

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 B provisions the violation of which involve an inherent level of deception B 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

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

large, given the quality of the information sought and the potentially enormous downside

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

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

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*

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.