MARQUETTE
UNIVERSITY
LAW SCHOOL

March 11, 2004

United States Sentencing Commission
One Columbus Circle, NE
Suite 2-500
Washington, DC 20002-8002
Attn: Public Affairs

**Re: Implementation of CAN-SPAM Act of 2003**

Dear Sir/Madam:

We are responding to the request for comments regarding implementation of the CAN-SPAM Act of 2003 (69 Fed. Reg. 2169). We are law professors at Marquette University Law School.[1] Professor O'Hear teaches and writes in the field of federal sentencing. Professor Goldman teaches and writes in the field of Internet law.

We are troubled by the possibility that criminal spam violations might be referenced to the existing fraud guideline. In particular, we believe that spam violations[2] should not be sentenced by reference to the loss table for economic crimes. In the interests of just punishment and administrability, we instead urge the Commission to develop a new, simple, spam-specific guideline.

## I. CAN-SPAM Violators Should Not Be Sentenced by Reference to the Fraud Guideline.

Fraud and other economic crimes are sentenced based principally on the amount of the loss intended or caused, according to the "loss table" set forth in U.S.S.G. § 2B1.1(b)(1). We have three principal concerns about tying CAN-SPAM violations to the loss table: (1) spam-caused losses are not appropriately analogized to losses from traditional economic crimes, (2) it would be difficult to accurately and fairly calculate spam-caused losses, and (3) loss table calculations would push most defendants towards the statutory maximum sentence, failing to adequately distinguish between defendants.

### (1) Spam Violations Are Not Zero-Sum Crimes Like Economic Crimes.

A traditional economic crime is zero-sum: the defendant benefits at the direct expense of the victim. For example, in an embezzlement case, the defendant takes money from the victim

[1] The views expressed herein are our own and should not be attributed to Marquette University or Marquette University Law School.
[2] By "spam violations," we refer to criminal violations of new 18 U.S.C. § 1037.

for the defendant's benefit. Every penny gained by the defendant comes directly at the victim's expense. In contrast, spam violations are not zero-sum. In fact, the defendant may not gain anything, and the victim may not suffer a loss (or may even derive a benefit).

Specifically, § 1037(a)(2)-(5) criminalizes sending multiple commercial electronic mail messages ("MCEMM") using techniques that make it harder to find the sender or the email's source ("obscuring techniques"). However, a sender does not inherently derive any value from using obscuring techniques, nor is benefit to the sender an element of the crime. Likewise, obscuring techniques do not inherently deprive a victim of value. To be sure, obscuring techniques might frustrate efforts by recipients or Internet service providers to block the emails, but circumvention of blocking attempts is not an element of the crime, either.

Indeed, in some cases, some "victims" could benefit from MCEMM, irrespective of whether they were sent using obscuring techniques. For example, some service providers charge customers based on the volume of data they receive, in which case the service providers financially benefit from the higher volume. Moreover, some individual recipients find MCEMM helpful and valuable. Indeed, there would be no such thing as MCEMM if some percentage of recipients did not respond favorably to some of the email offers they receive.

Section 1037(a)(1) differs from the subsections criminalizing the use of obscuring techniques; the offense is instead premised on unauthorized use of a service provider's computer resources. Nevertheless, even this subsection does not require any sender benefit or victim detriment as an element of the crime. Even unauthorized use of resources does not necessarily cause harm if the service provider's computer had unused capacity at the time of the sender's campaign.

Thus, unlike traditional economic crimes, spam violations do not require a sender's gain at a victim's expense. No unwitting victim sends a check to the sender. No cash drawer comes up short. The victims may never know that they have suffered a "loss." Some "victims" may derive a benefit from the email. Thus, economic crimes predicated on a zero-sum calculus do not provide a proper analogy.

(2) Difficulty Computing Spam-Attributable Losses Will Lead to Considerable Administrative Costs.

We agree with Judge Jon O. Newman's general critique[3] of the loss table: a table with sixteen different categories – and significant sentencing consequences in moving from one category to another – encourages considerable litigation over the meaning and measurement of "loss." This imposes needless burden on the court system. In theory, incremental loss should indeed produce incremental punishment, but the loss table carries this principle to an unwarranted extreme. In practice, the amount of loss shown at sentencing may depend on the diligence of the particular investigator working the case, random chance, and other variables having nothing to do with the defendant's actual culpability.

[3] *See* Jon O. Newman, *Towards Guidelines Simplification*, 13 FED. SENT. R. 56 (2000).

The loss table's general weaknesses are magnified in the context of spam violations. As discussed above, injury (or even intent to injure) is not an intrinsic element of the offense. Thus, in some cases, spam violations may be truly victimless crimes.

Even where a colorable theory of loss can be advanced, connecting that loss to a particular sender's email may be difficult. Prosecutors and judges may be tempted to count as losses a service provider's "fixed costs," like a pro rata share of network operating costs, the amounts paid to third party vendors who attempt to block unwanted email, or the costs of employees on staff to remediate email campaigns. However, none of these costs are properly attributable to a particular defendant, as the service provider will incur these fixed costs no matter what any particular sender does.

It may be possible to link the sender's email with variable losses directly attributable to the email. Such losses might arise, for instance, if the defendant's email causes a service provider's network to go down, or requires a service provider's employees to work overtime to remediate a system problem. However, only a small percentage of email campaigns will cause these variable losses; hence, such losses may or may not be reasonably foreseeable to the defendant. In any event, collecting and presenting technical evidence of this nature will be a costly endeavor for prosecutors, victims and the court system.

Prosecutors and judges may also be tempted to consider an email recipient's lost time and annoyance, but these "harms" are not obviously cognizable under the fraud guidelines, which, by their own terms, are limited to "pecuniary losses." To be sure, a business victim might claim lost employee productivity from each individual recipient as a pecuniary loss, but determining such losses would create difficult assessments about the number of recipients who actually saw the email in their in-boxes and imprecise judgments about how much time was spent and how to cost-account for that time. Already, experts do not agree on how to calculate these economic costs,[4] and some courts have rejected lost employee productivity entirely as a cognizable loss from spam.[5]

Meanwhile, under the loss table, defendants are entitled to a credit for the fair market value of property returned and services rendered to victims before the offense was detected.[6] As discussed earlier, some recipients may find MCEMM valuable and take advantage of some of the offers they receive. Thus, so long as a defendant's email offered legitimate goods or services, the sentencing court might confront legally and factually complicated questions as to how to credit the defendant for goods and services provided to "victims."

Finally, courts might also confront difficult questions in determining how to apply the mass-marketing enhancement. The amount of the enhancement depends on the number of "victims."[7] "Victim," in turn, is anyone who has suffered an "actual loss" for purposes of the

[4] *See, e.g.*, Saul Hansell, *Diverging Estimates of the Cost of Spam*, N.Y. TIMES, July 28, 2003, at C1.
[5] *See* Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003). The *Hamidi* case considered this issue in the context of a common law trespass to chattels claim.
[6] USSG § 2B1.1, comment. (n.3(E)).
[7] USSG § 2B1.1(b)(2).

loss table calculation.[8] As the foregoing discussion illustrates, determining who suffers an actual loss from an MCEMM campaign will prove to be a difficult exercise.

In short, quantifying the loss in any individual case will likely prove contentious and costly. And – even after courts have resolved the chief legal questions in this area – in light of the idiosyncrasies of the loss definition and the difficulties of developing evidence of spam-related loss, the public will still lack any basis to conclude that sentences for spam violations actually distinguish between defendants based on the true gravity of their offenses.

(3) The Fraud Guideline May Lead to Unduly Severe Sentences for Spam Violations.

Spam violations are not necessarily serious criminal offenses. As noted above, § 1037 may be violated even by a sender promoting legitimate goods and services that some recipients actually want. While spam violations can involve culpable behavior (e.g., concealing the origin of an email campaign), the statute's focus on improper marketing means – rather than improper marketing content or any unjust enrichment by the sender – places spam violations rather low on the culpability scale in comparison with the full range of socially undesirable behavior. Congress recognized the relatively benign nature of § 1037 violations by setting low maximum sentences of one and three years, depending on the violation.[9]

Yet, sentencing § 1037 violations pursuant to the fraud guideline would punish many defendants more seriously than is warranted by the crime's nature. First, it is likely that spam defendants would routinely be subject to the sophisticated means enhancement.[10] This sets a minimum offense level of twelve, which, for first-time offenders, would result in a sentence of 10-16 months. Putting this in a comparative perspective, even a low-volume sender whose messages caused no quantifiable injury would be subject to a mandatory penalty roughly equivalent to the penalty meted out to a person who embezzled $30,000 or defrauded victims of a like amount. In our view, we should not equate spam violations with these more serious offenses.

Even if the Commission decided that the sophisticated means enhancement should not routinely apply to spam violators – and, at a minimum, we urge the Commission to do so – the fraud guideline might still treat many senders too harshly. Consider a low-volume defendant who sends one email to 500,000 recipients. A court considering lost employee productivity and a pro rata share of fixed costs might calculate the losses at $0.10 per recipient,[11] for a total loss of $50,000. In this case, the fraud guideline (including a six-level mass-marketing enhancement) would set the offense level at 18, requiring a minimum 27-month sentence for a first-time

[8] USSG § 2B1.1, comment. (n.1).

[9] A five-year maximum applies if the spam violation occurred in connection with another felony, or if the defendant has a relevant prior conviction.

[10] USSG § 2B1.1(b)(8).

[11] Ferris Research published a cost analysis of spam concluding that employees receive 3.85 spam emails per day on average and that this volume costs employers $9.90 per employee per month. *See* Spam Control: Problems and Opportunities, Ferris Research, Jan. 2003, at 16-17, *available at* http://www.ferris.com/rep/200301/report.pdf, Although the Ferris research report provides an illustrative data point for our critique, we do not endorse its methodology, and we suspect that it overstates losses substantially.

offender. Not only does this sentence seem high when compared to other offenses in a similar sentencing range (e.g., embezzlement of $200,000), but it also comes close to the statutory maximum of three years. In other words, application of the fraud guideline may leave little room to distinguish between egregious and minor violators

Guidance to judges (through appropriate commentary in § 2B1.1) might help to avoid some of these problems, but, in some instances, in the interests of clarity and fairness, it is better to create a whole new guideline than to jerry-rig an old guideline for a new purpose. We believe that spam violations represent precisely such an instance.

## II. The Commission Should Adopt a Simple New Guideline for CAN-SPAM Offenses.

As between the fraud guideline and the trespass guideline, we think the trespass guideline is the better analogy for spam violations for three reasons. First, many spam violations are analogous to common law trespass to chattels, because the onslaught of the sender's email can temporarily dispossess a victim of its "chattel" (i.e., the hardware used to operate a computer network).[12] Second, the trespass guideline excludes the problematic mass-marketing and sophisticated means enhancements. Third, the trespass base offense is lower, leaving more room to differentiate among defendants.

Unfortunately, the trespass guideline also incorporates by reference the fraud loss table for some offenses. Because no guideline referencing the loss table is an appropriate model for spam violations, we propose that spam violations be governed by a new spam-specific guideline.

Although the loss table taints the trespass guidelines, the closeness of the analogy makes the guidelines a useful starting point. Therefore, we propose a base offense level of four, identical to the base offense level for trespass. However, instead of using the fraud loss table, we propose increasing offense levels based on the aggregate number of recipients targeted by the sender in his or her MCEMM campaigns during the relevant time period.

This metric has three advantages. First, it is much simpler to calculate than loss. Indeed, the relevant evidence can be obtained directly from the defendant's records, potentially relieving victims of the burden of developing complex data for the government. Second, the amount of emails the sender tried to send is a reasonable proxy for victim harms. The more emails sent, the more likely it is that the sender caused some victims real harm at some point (e.g., by causing a recipient's server to crash). Third, the sender cannot foresee or prevent idiosyncratic victim losses, but the sender can control the number of recipients. Therefore, this metric will avoid sentencing discrepancies among senders who engaged in the same conduct, but who caused different degrees of "loss" as a result of chance (e.g., through sheer bad luck, one sent MCEMM to a network server at a time of unusual vulnerability, causing the server to go down).

To minimize litigation burdens, the spam guideline should include relatively few categories. For instance, the "volume table" might look like this:

[12] *See* Restatement (Second) of Torts, §§ 217-218 (1965).

| Number of Intended Recipients Of Illicit Email in a 12 Month Period[13] | Increase in Level |
|---|---|
| | |
| 250,000 or less | no increase |
| More than 250,000 | add 3 |
| More than 1,000,000 | add 6 |
| More than 10,000,000 | add 9 |
| More than 100,000,000 | add 12 |
| More than 1,000,000,000 | add 15 |

We believe a base offense level of four plus this volume table adequately distinguishes egregious and minor violations.[14] A sender targeting a billion recipients will receive the statutory maximum of three years, while a low-volume sender is treated more leniently.

Our proposal assumes simple § 1037 violations, i.e., the violations were not themselves conducted in furtherance of a scheme to defraud, distribute unlawful pornography, or commit any other crime. For aggravated spam violations, we believe that sentencing courts could and should take the linked offenses into account at sentencing as relevant conduct under the appropriate guidelines.

## III. Conclusion

The guideline applicable to spam violations should be simple for courts to apply, but should also provide for meaningful distinctions among spam violators in at least rough proportion to the harm they have caused. We do not believe any guideline referencing the fraud loss table does that. Therefore, we believe that the Commission should develop a separate guideline for § 1037 violations that uses a volume table based on the number of intended recipients.

Respectfully submitted,

Professor Michael O'Hear
Assistant Professor of Law

Professor Eric Goldman
Assistant Professor of Law

[13] A relevant time period should be defined for purposes of this table. We follow the statute's use, in a slightly different context, of an annual aggregation of MCEMM during the highest volume one-year period. *See* 18 U.S.C. § 1037(b)(2)(C).

[14] There is, of course, nothing scientific about the cut-off points. They are intended to achieve meaningful differentiation at sentencing between the dabbler in spam, the professional, and the truly big-time player. The volume table is also intended to ensure that the full-range of statutorily available penalties (zero to three years in most cases) is, in fact, used, thus recognizing Congress's implicit belief that there are real differences in culpability among different spam violators. Wide ranges reduce the likelihood that a defendant will find himself or herself standing on (or falling off) a "cliff," i.e., just above or below a cut-off point. Still, there is admittedly some inevitable arbitrariness when cut-off points are defined. Thus, the fact that a given defendant's volume happens to be at the very top (or very bottom) of a range might, in conjunction with other factors, be made a basis for upward (or downward) departure in exceptional cases.