

Finally, the Committee reviewed the proposed revisions to the organizational guidelines. The Committee opposes the elimination of the prohibition for the three-point reduction in the culpability score for an effective compliance program if the organization unreasonably delayed reporting an offense to appropriate governmental authorities after becoming aware of the offense. The Committee believes that the claim to have an effective compliance program is inconsistent with unreasonable delay in reporting the offense after its detection. The Committee generally supports the increase in the reduction of the culpability score under §8C.25(f) for an effective compliance program.

We appreciate the opportunity to present our views. If you need any additional information, please feel free to contact me at (713) 250-5177, or Judge William T. Moore, Jr., Chair of the Committee's Sentencing Guidelines Subcommittee, at (912) 650-4173.

Sincerely,

A handwritten signature in cursive script, appearing to read "Sim Lake".

Sim Lake

February 25, 2004

U.S. Sentencing Commission
One Columbus Circle, NE
Suite 2-500
Washington, DC 20002-8002
Attention: Public Affairs

Dear Commissioners:

The California County Issues HIPAA Workgroup is a collaborative statewide focus group created as an information and resource sharing forum for California counties as we face the challenge of applying the HIPAA Administrative Simplification Rules to our complex community healthcare delivery systems. Our membership of over 1,000 strives to resolve the unique implementation issues and myriad compliance problems with which counties are confronted.

The purpose of this letter is to express our collective support of the comments and concerns submitted by the Health Care Compliance Association with regard to the proposed changes to the Federal Sentencing Guidelines.

Sincerely,



Cheri Huber
Co-Chair
California County Issues HIPAA Workgroup

February 9, 2004

United States Sentencing Commission
One Columbus Circle, N.E., Suite 2-500
Washington, D.C. 20002-8002
Attention: Public Affairs

Re: Response to Request for Public Comment re: Proposed Amendments to the Sentencing Guidelines and Issues for Comment Published in the Federal Register on December 30, 2003, and January 14, 2004 (Proposal #2, "Effective Compliance Programs in Chapter 8")

To the United States Sentencing Commission:

Thank you for the opportunity to comment on the above-referenced proposal regarding the Federal Sentencing Guidelines for Organizations (FSGO). Before offering my commentary, I would like first to express my appreciation to the United States Sentencing Commission for creating an Ad Hoc Advisory Group that, from this outsider's perspective, appears to have conducted a focused and balanced review of the elements of an "effective program to prevent and detect violations of law" as set out in Chapter 8.

Focus of my commentary

My commentary in this letter focuses on §8B2.1.a.2 as designated in the proposal (the italicized portion of the quotation below), which (more than the original FSGO) seems formally to acknowledge the benefits that ethics can bring to compliance management:

To have an effective program to prevent and detect violations of law, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (c)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall –
1) exercise due diligence to prevent and detect violations of law; and
2) *otherwise promote an organizational culture that encourages a commitment to compliance with the law.*

The proposal's restrained reference to ethics is implied by the words, "promote an organizational culture," recalling the Advisory Group's August 21, 2002 "Request for Additional Public Comment" in which commentators were asked to remark on whether the revised FSGO should "encourage organizations to foster ethical cultures to ensure compliance." Indeed, the "Synopsis of Proposed Amendment" confirms that the implied

connection to ethics is intentional: “This proposed addition is intended to reflect the emphasis on ethics and values incorporated into recent legislative and regulatory reforms, as well as the proposition that compliance with all laws is the expected behavior within organizations” (p. 58). Much of the testimony before the Advisory Group in favor of incorporating ethics into the revised FSGO implied a claim that a “values-based” approach to business conduct management is in some way preferable to a “compliance-based” approach.

Perspective of my commentary

As a scholar-practitioner of organizational ethics and compliance, I have carefully studied the commentary, public hearings transcripts, and report that came out of the Ad Hoc Advisory Group’s work. Currently, I teach undergraduate and graduate students in a business school (full-time) and am employed by a professional services firm as a business advisor (part-time) to mainly large, publicly held corporations. In both contexts, I have been a “user” of compliance programs, subject to the compliance program provisions of my two employers. In the business advisory context, I have shared responsibility for compliance program management as a member of enterprise-wide compliance committees. I should note that I am solely responsible for the views expressed in this letter, and that they do not necessarily reflect the views of my employers.

My academic training is in philosophical ethics, and it therefore may not be surprising that I believe strongly in the importance of ethics to compliance management. However, as my commentary will reflect, I am quite cautious about the claim that a values-based approach is preferable to a compliance-based approach. The reasons for my cautiousness are that I think that, in practice, values-based compliance programs are vulnerable to 1) management-driven moral absolutism that can lead to management inflexibility regarding internal control, and 2) board and management moral complacency that arises from the belief that a values-based compliance program is sufficient to accomplish the objectives of law compliance or ethical conduct.

Recommendations for your consideration

As you are undoubtedly aware, the scope of the USSC’s responsibility for crime and sentencing policy is only a small part of its scope of influence on day-to-day business conduct management – as manifested by the unexpectedly widespread impact of the original FSGO on corporate compliance programs. Therefore, my recommendations to the USSC recognize that the USSC’s active influence on business practice transcends its formal responsibilities as a governmental agency. Neither recommendation contemplates any revision to the language of the proposal. Both recommendations pertain to the manner in which the USSC communicates about, educates on, and otherwise implements, the revised FSGO, within and beyond the formal scope of its responsibility.

First recommendation: Encourage the consideration of ethics in compliance management, but discourage the presumption that a values-based approach necessarily improves upon a compliance-based approach.

There is a widespread attitude that compliance is *needed*, while values are *nice to have*. This attitude belies the truth that values can be bad as well as nice, but it also suggests that law compliance is enough. The proposal seems to want to discourage organizations from gravitating toward a lowest common denominator, although by offering the distinction between the objective of law compliance and the promotion of ethical culture, it may instead reinforce undesirable attitudes.

The success of the original FSGO has been attributed in part to their brevity and resultant flexibility. The breadth of implementation possibilities allowed by the “effectiveness” criteria suggests that what will be a suitable compliance program for a given organization will have much to do with its particular situation: size, industry, history, location, structure, function, personnel, etc. This flexibility should similarly apply to whether a values-based approach is appropriate to the situation. Large organizations – meaning those with thousands of employees in multiple locations, possibly internationally – simply cannot claim with any credibility to share a finite set of core values, and should not be rewarded or have punishment mitigated for having the audacity to claim the impractical and impossible. Small organizations may lay a more credible claim to shared values, but the translation of those shared values into upholding the USSC’s objective of law compliance depends on who is in charge, the industry environment, the dynamic nature of law, and numerous other factors that need to be uniquely assessed relative to the situation. With its positive affirmation of the absolute importance of ethics, the USSC should continue to exercise a relative standard of compliance program “effectiveness” that is appropriate to the particulars of the situation.

Second recommendation: Look within and outside the seven criteria for effectiveness measures.

The FSGO – original and revised – provide a deceptively clear standard for compliance program effectiveness. In theory, the seven criteria can be checked off as either having or not having been met. In practice, because of their implementation flexibility, the criteria do not lend themselves to a scientific approach to program evaluation. Assessors must interpret whether a given practice or combination of practices fulfills one or more criteria, because the criteria are markedly general in relation to the specific potential practices being evaluated. The resistance of some who testified before the Advisory Group to incorporating reference to ethics in the FSGO was in some cases due to a practical concern that the introduction of ethics would obfuscate effectiveness measurement even further.

Ethical behavior is a function of intentions that may not be manifest in observable, measurable consequences. While the values-based approach emphasizes “self-chosen” standards, theoretically it is unclear whether the “self” in question is each individual within an organization, or each organization. In practice, however, it is clear that organizational values cannot be codified if they are specific to each individual self, meaning that core values are, out of necessity, constructions of management. Vain though attempts to understand management “intent” may be, the USSC must emphasize the

indispensability of human, non-scientific judgment in ascertaining the credibility – and therefore the effectiveness – of organizational compliance initiatives.

Conclusion

The values-based approach that receives implied attention in the proposal has had considerable success dissuading practitioners from the incorrect impression that, “If it’s legal, it’s ethical.” However, values-based management rhetoric today is likely to sound like, “If it’s values-based, or if we call it ‘ethics,’ it’s ethical.” Moreover, “If it’s ethical, it’s compliant.” Neither rhetorical claim is always true. Sometimes, the wrong spin on values may work against law compliance, while other times, law compliance may be inconsistent with ethical intent.

The USSC’s formal responsibility includes promoting law compliance, while its influence seems destined to continue to foster the perception that values-based approaches to compliance management are superior to compliance-based approaches. The real strength of values-based compliance management is its potential for promoting openness and supporting human judgment – strengths which have been attributed to the original FSGO and which I hope will apply equally to the revised FSGO.

* * *

Thank you again for your request for public comment and for your anticipated careful consideration thereof. A paper version of these remarks is currently under development, and I would be pleased to share it with you at some future date, if requested. Please do not hesitate to contact me should you wish to discuss this commentary.

Respectfully submitted,



Christopher Michaelson, Ph.D.
Lecturer, Legal Studies Department
The Wharton School of the University of Pennsylvania
650 Jon M. Huntsman Hall
3730 Walnut Street
Philadelphia, PA 19104-6340
(215) 573-4864
chrismic@wharton.upenn.edu

Mailing Address:
P.O. Box 1469
Minneapolis, MN 55440-1469



February 25, 2004

U.S. Sentencing Commission
One Columbus Circle, NE.
Suite 2-500
Washington, DC 20002-8002
Attention: Public Affairs

Subject: United States Sentencing Commission Proposed Changes

Dear Commissioners:

Thank you for offering this opportunity to respond to the proposed changes in the Federal Sentencing Guidelines. Allina Hospitals & Clinics, a family of hospitals, clinics and care services, believes the most valuable asset people can have is their good health. We provide a continuum of care, from disease prevention programs, to technically advanced inpatient and outpatient care, medical transportation, pharmacy and hospice services. Allina serves communities throughout Minnesota and western Wisconsin. We are a mission-driven organization with a solid commitment to compliance.

I appreciate that the Commission is placing an increased emphasis on the importance of compliance programs and the role of the Compliance Officer as a member of senior leadership. I completely support this effort. As the Compliance Officer at Allina, I am part of the Allina Leadership Team and report directly to our Chief Executive Officer. This structure permits me to be effective in my position.

Moreover, I agree with the many changes proposed by the Commission to provide additional guidance and direction to organizations regarding compliance programs and to emphasize the need for Compliance Officers to have sufficient authority and resources to oversee the organization's compliance program. While Allina supports the proposed changes to the Guidelines, we do have the following three concerns.

First, the proposed amendments suggest that the Compliance Officer of the organization is accountable for the effectiveness of the program. The proposed changes have added language to § 8B2.1(b)(2) which states that the high-level person responsible for the program (the Compliance Officer) has the responsibility to "ensure the implementation and effectiveness of

the program." This amendment does not recognize that a Compliance Officer cannot truly be responsible for the effectiveness of the program. Implementing and maintaining a compliance program is an integral part of running an effective organization. Operating leadership of an organization must embrace the program and assume accountability to ensure that the compliance program is working.

The role of the Compliance Officer is to create compliance strategies that, if implemented by operational leaders, will lead to an effective and efficient compliance program. It is not realistic to hold the Compliance Officer alone responsible for the overall success or failure of the compliance program. If there are failures, the responsibility may reside with the Compliance Officer or may reside with any number of other leaders within the organization. The proposed amendments could be interpreted as relieving operational leaders of their responsibility to ensure the organization is compliant.

We believe that the Guidelines should strengthen rather than weaken leadership accountability for an organization's compliance efforts. For the reasons stated above, we would recommend that the proposed amendment be modified as follows:

"Specific individuals(s) within high-level positions in the organization shall be assigned direct, overall responsibility to coordinate the design, oversee the implementation, and evaluate and report to management and the board on the effectiveness of the program to prevent and detect violations of laws."

Our second concern relates to the treatment of organizations that encounter trouble even though the organization has a compliance program in place. While the proposed changes are an improvement over the existing Guidelines, it is our view that the proposed changes could do more to promote effective compliance programs.

As drafted, the proposed amendments create a rebuttable presumption that the compliance program was ineffective. However, we would propose that a program is effective when an organization discovers and brings the offense to the attention of the government. The rebuttable presumption of ineffectiveness creates a disincentive for organizations to thoroughly investigate and disclose wrongful conduct. Conversely, a rebuttable presumption that the program is effective (where the organization has uncovered and disclosed the wrongdoing) creates incentives to both investigate and disclose – an approach that is more consistent with the overall emphasis on compliance in Chapter 8 of the Guidelines.

Finally, although we fully support the proposed amendment that requires the organization to take reasonable steps to "evaluate periodically the effectiveness of the organization's program," more guidance is needed to understand this requirement. The Commission should add clarifying language to indicate the high-level requirements for this evaluation.

U.S. Sentencing Commission
February 25, 2004
Page 3

In summary, Allina supports the proposed changes to the Guidelines and applauds the hard work of the Commission. The changes proposed by the Commission will help strengthen organizational compliance programs and the role of the Compliance Officer. We would strongly encourage the Commission, however, to revise the proposed Guidelines on the three important points discussed above.

Sincerely,

A handwritten signature in cursive script that reads "David Orbuch".

DAVID B. ORBUCH
Executive Vice President
Compliance and Public Policy
612-775-5819

ChevronTexaco Corporation
Law Department
6001 Bollinger Canyon Road, T3000
San Ramon, CA 94583-2324
Tel 925 842 1298
Fax 925 842 2022
WGDU@chevrontexaco.com

William G. Duck
Chief Corporate Counsel

March 1, 2004

ChevronTexaco

Michael Courlander
Public Affairs Officer
United States Sentencing Commission
One Columbus Circle, N.E., Suite 2-500
Washington, DC 20002-8002

Re: Response to Request for Public Comment on Proposed
Modifications to United States Sentencing Guidelines

Dear Mr. Courlander:

We appreciate the opportunity to comment on the Ad Hoc Advisory Group's recommended modifications to the United States Sentencing Guidelines.

We support the Ad Hoc Advisory Group's recommended modifications to §8B2.1(b)(5)(c). We believe the emphasis on promoting an "organizational culture" that encourages commitment to compliance and mechanisms that allow for "anonymous" reporting is well placed and appropriate. In addition, we would like to recognize the invaluable role Ombudspersons can play as part of a comprehensive approach to crime prevention and detection.

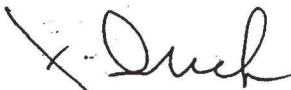
Chevron Texaco has numerous programs and processes in place to ensure legal compliance, including an Office of Ombuds that provides a confidential environment outside of formal reporting channels. Our Ombudspersons are neither an employee advocate nor member of management, but rather independent neutrals who can discuss matters informally and off the record.

Ombudspersons can play a critical role in encouraging employees to step forward and report violations that might otherwise go undetected. Our experience has shown that an essential "first step" for many employees is a confidential discussion with a trusted neutral advisor. For this reason, Ombudspersons in conjunction with other programs and processes can ensure that employees have a safe environment for discussing options without fear of retaliation.

We recognize the difficulty of keeping confidentiality under a formal reporting process and believe the Commission has correctly placed the emphasis on "anonymity" rather than "confidentiality" in the recommended modifications.

We appreciate the opportunity to provide these comments.

Yours truly,



—Wm. G. Duck

cc: Broderick W. Hill

**MARQUETTE**
UNIVERSITY

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 violations² 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 critique³ 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).