

TO:

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

I. INTRODUCTION:

The United States Sentencing Commission has requested public comment regarding implementation of Public Law 108-187, the CAN-SPAM Act of 2003. 69 F.R. 2169 (14 January 2004). This commentary is submitted accordingly.

II. COMMENTATOR'S BACKGROUND & CONTACT INFORMATION:

Background: The Commentator, Kenneth H. Ryesky, Esq., is an attorney at law in East Northport, NY, and is an Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York.

Contact Information: Kenneth H. Ryesky, Esq., P.O. Box 926, East Northport, NY 11731. Telephone: 631/266-5854 (vox), 631/266-3198 (fax). E-mail: khresq@sprintmail.com.

Disclaimer: The comments herein reflect the Commentator's personal views, and do not necessarily represent the official position of any organization or institution with which the Commentator is or has been associated, affiliated, employed or retained.

III. CLASSIFICATION OF NEW OFFENSES:

Violations of 18 U.S.C. § 1037 have attributes germane to, inter alia, USSG § 2B1.1 (Fraud, Theft, and Property Destruction), and USSG § 2B2.3 (Trespass). It would serve well to basically classify these new offenses under USSG § 2B1.1, for the harms typically associated with such offenses entail diminution of the victims' data storage capacity, whether in the victims' personal computers or in the victims' e-mail accounts, and also entail quantifiable and unquantifiable expenses out of the pockets of the e-mail recipients, the enforcement authorities, and society as a whole. As more fully discussed below, appropriate tie-in with USSG § 2B2.3 trespass-type attributes of the offense should be accomplished through enhancements, where appropriate. The base level of the offense should vary with the seriousness of the offense.

IV. SOPHISTICATED MEANS:

The use of computer technology has a certain degree of complexity, and is commonly thought of as a "sophisticated means" of committing offenses. But some uses are more "sophisticated" than others. The "sophisticated means" entailing falsification of entities, identities and locations, such that detection of, apprehension of, or information concerning the perpetrator is clearly contemplated in USSG § 2B1.1(b)(8). The law enforcement authorities, the recipients of the illegal e-mails, and the administrators of the systems through which the illegal e-mails are transmitted all have the need and the right to know the identity and whereabouts of the perpetrator. The § 2B1.1(b)(8) enhancements are most relevant to the new offenses set forth in 18 U.S.C. § 1037 and other provisions of Public Law 108-187, and should be applied thereto.

V. ENHANCEMENTS:

Certain factors cause violations of 18 U.S.C. § 1037 to be especially egregious, harmful and destructive. Enhancements should be provided in such instances, including but not limited to the following:

A. The violator knew or should have known that the recipient specifically objected or would object to the receipt of the unsolicited e-mail. This is especially relevant where the violator failed to act upon one or more victims's opting out under 15 U.S.C. § 7704(a)(5), or any "Do Not E-Mail" registry that may be established pursuant to 15 U.S.C. § 7708 or otherwise.

B. The E-mail involved was particularly large, lengthy or capacious. Inasmuch as many e-mail users' accounts entail kilobyte capacity limitations, the use of an e-mail message of 100 KB is more obviously egregious than the use of an e-mail message of 1 KB. There should be a graduated scale of enhancements for size of the illegally-transmitted message involved. As an example, a message of 5 or more KB should warrant a 1 level enhancement; 10 KB, 2 levels; 20 KB, 3 levels; 50 KB, 4 levels; 100 KB, 5 levels; 200 KB, 6 levels. The size of the message should include any attachments. Serial messages should be aggregated together for the purpose of this enhancement. An unsolicited message transmitted from the same sender to the same recipient address within 24 hours or less after a previous message should be considered a serial message for the purpose of aggregating the messages for this enhancement.

C. The E-mail involved a virus. The use of e-mail to spread viruses has already been amply demonstrated to cause global damage. An e-mail sent in violation of 18 U.S.C. § 1037 that also contains a computer virus, or otherwise intentionally facilitates the spread of a computer virus, is particularly egregious, and warrants an enhancement of at least 6 levels.

D. The e-mail involved wrongfully used a trademark, trade name, or other intellectual property. Many deceptive e-mails improperly use trademarks, trade names or other intellectual property, including names of proprietary pharmaceuticals, corporations, publications or websites. This warrants some sort of enhancement, especially where the rightful owner of the intellectual property has previously objected. Unfortunately, many intellectual property owners such as pharmaceutical manufacturers have not taken a proactive stance against the use of their trademarks and trade names, obviously finding some positive benefit from the negative publicity.

Pfizer's reluctance to go after those who use its proprietary name "Viagra" is one example. Though Pfizer, in this example, may derive benefit from the bandying about of the name of its drug on the streets and in cyberspace, the public is harmed where the product being purveyed is not actually Pfizer's product as implicitly claimed. Accordingly, some enhancement for the wrongful use of a trademark, trade name or other intellectual property should apply even where the owner of the intellectual property has been less than zealous in protecting its rights.

E. The recipient's conduct realized income or revenue that was improperly omitted from a tax return. Under the American taxation system, which depends upon members of the public complying without being compelled to do so by action of a government agent, there is a strong imperative that the tax laws be enforced, lest the public sentiments wax cynical and the voluntary compliance deteriorate. The public needs to see that there are negative consequences for failing to comply with the tax laws. Accordingly, any violation of 18 U.S.C. § 1037 is aggravated where the defendant has received money or other property in the course of his or her conduct and has failed to pay his or her legal share of the taxes imposed upon the transaction. Moreover, the knowledge that one's violation of 18 U.S.C. § 1037 may carry greater penalties where there has been a tax violation in the process can be expected to help induce voluntary tax compliance, even if such compliance comes about after detection of the 18 U.S.C. § 1037 violation, but before the deadline for filing the tax return. There should be an enhancement where the conduct involving the illegal e-mail also entailed a tax violation or a tax loss to the government, whether or not the violator was also prosecuted for Internal Revenue Code or state tax code violations. Such enhancements should be commensurate with the tax loss involved, and in consonance with the Tax Table set forth in USSG §2T4.1.

F. The defendant improperly obtained the e-mail address(es). This includes, but is not necessarily limited to, harvesting of e-mail addresses from the users of a Web site, proprietary service, or other online public forum without authorization and the random generating of e-mail addresses by computer; or knew that the commercial e-mail messages involved in the offense contained or advertised an internet domain for which the registrant of the domain had provided false registration information.

G. The illegal e-mail consisted of or contained sexually-oriented material. This is obviously a most aggravating factor, for which an enhancement is surely warranted. Children are especially vulnerable victims of pornography, accordingly, enhancement of the sentence is especially warranted where one or more children were the recipient.

H. The conduct entailed the transmission of a large volume of unlawful e-mail. There should be a graduated scale of enhancements, according to the volume of e-mail sent in the course of the conduct. 18 U.S.C. § 1037 is couched in terms of "multiple" electronic mail messages, and, with respect to § 1037, subparagraph 1037(d)(3) defines "multiple" with respect to electronic mail messages as more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period. There are, however, other provisions of the Can Spam Act that can be violated with a single e-mail message, including, for example, 15 USCS § 7704(d), which requires that sexually oriented material be labeled as such in the subject heading. With respect to such other provisions, initial the threshold for "a large volume" of unlawful e-

mail should be, if not lower, at the standard set forth in 18 U.S.C. § 1037(d)(3). Further enhancements should obtain at other thresholds beyond the initial, e.g., 2 level enhancement for more than 100 messages in a 24-hour period, 3 level enhancement for more than 250 messages in a 24-hour period, 4 level enhancement for more than 500 messages in a 24-hour period, et cetera.

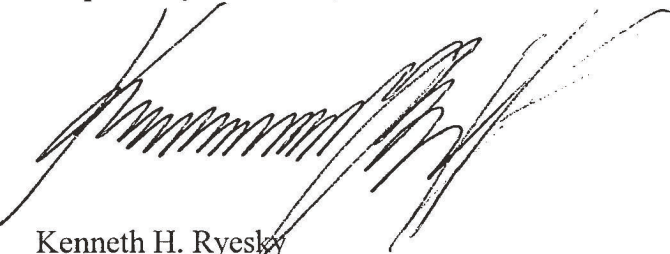
I. The conduct entailed the violation of other federal or state laws. Some "spam" e-mails are sent in the course of conduct that violates other laws. In addition to the taxation issues discussed in Paragraph E above, unsolicited e-mail has been known to contravene, inter alia, the 39 U.S.C. § 1302 prohibition against chain letters scams, or the illegal prescription and dispensation of medications. These all are aggravating circumstances that warrant enhancement of the level of the offense for sentencing purposes.

VI. CONCLUSION:

The transmission of unlawful electronic mail is a serious crime because it imposes vast financial and social burdens upon society as a whole, and upon the recipients of the e-mail, and upon the systems through which the unlawful e-mail is sent. Moreover, unlawful electronic mail is frequently used as a means to facilitate other activities that are wrongful and/or illegal in their own right. The financial transactions done in connection with unlawful electronic mail are frequently hidden and unreported for purposes of tax administration, thus frustrating the tax collection process and imposing additional burden upon the taxpaying public.

Accordingly, it is important to punish those convicted of offenses involving unlawful transmission of electronic mail, and to tailor such punishment to the degree of harm caused, including harm in collateral related areas. Appropriate enhancements to the level of the offense are thus imperative.

Respectfully submitted,



Kenneth H. Ryesky
22 January 2004

Alex Barylo
11114 Greiner Rd
Philadelphia, PA 19116

United States Sentencing Commission,
One Columbus Circle, NE., Suite 2-500,
Washington, DC 20002-8002,

Attention: Public Affairs.

- Should deceptive spammers get an "enhancement," i.e., a little more prison time, if they employ "sophisticated means" to send the spam?

YES

- Should the method the offender used to gather the targeted addresses be a consideration in sentencing? Under one proposal, spammers could face an enhancement for harvesting e-mail addresses from Web forums, or generating them randomly.

NO

- Should criminals who commit fraud, identify theft, child porn trafficking or other serious crimes be sentenced more severely if they sent unsolicited bulk e-mail in the course of the crime?

DEFINITELY!!!

January 20, 2004

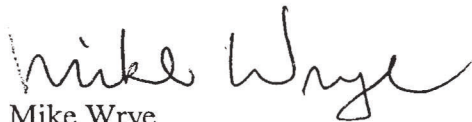
United States Sentencing Commission
One Columbus Circle, NE, Suite 2-500
Washington, DC 20002-8002

Attention: Public Affairs,

Subject: Spammer Sentencing Guidelines

Sentences for spamming should focus on high fines and little jail time. Take the profits out of spamming, but don't make the taxpayers support them during extended prison stays. Save the jails for violent people. Charge the spammers \$10 for each message they send and \$100 for each e-mail address they steal.

Thanks,

A handwritten signature in black ink that reads "Mike Wrye". The signature is written in a cursive, flowing style.

Mike Wrye
Orlando, FL

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

ATTN: Public Affairs

Recently, the following questions were posted in an article located at URL:
<http://www.securityfocus.com/news/7846> to which I have attached my responses which are formatted in two parts; a Yes/No response, followed by additional verbatim, expounding upon my position.

Q: Should deceptive spammers get an "enhancement," i.e., a little more prison time, if they employ "sophisticated means" to send the spam?

A: Yes.

Deception, in my opinion, not only includes using measures that conceal origin, but also those that hide content. The use of misspellings to evade content filters is becoming commonplace, and demonstrates that the sender already knows that the targets being emailed do not want to receive the message. An excellent example is the following misspellings of "Viagra" which include, but are not limited to, "Vigara," "Viarga," and "Vaigra." It should be mandated that **every individual advertisement or solicitation be prefixed with an ADV** as the first three characters of the subject, and that not using this identifier constitutes deception.

Q: Should the method the offender used to gather the targeted addresses be a consideration in sentencing? Under one proposal, spammers could face an enhancement for harvesting e-mail addresses from Web forums, or generating them randomly.

A: Yes

Harvesting techniques and randomly generated email addresses will automatically target people who do not want to receive any UCE.

Q: Should criminals who commit fraud, identify theft, child porn trafficking or other serious crimes be sentenced more severely if they sent unsolicited bulk e-mail in the course of the crime?

A: Yes

The UCE should always remain a separate offense. Sending child pornography and performing fraudulent activities should constitute an "offense enhancement" just as the use of deceptive headers and email address generation techniques.

In summary; **all unsolicited email should be double opt-in only**. This requires that an individual submit his email address to a particular marketer, then that marketer must send a confirmation to


that email address which must be answered. This will prevent unscrupulous persons from submitting the email addresses of other individuals, and will also prevent people who don't want to receive any email from having to opt-out from millions of possible emailing lists. In addition, all opt-in confirmations should have "OPT-IN?" as the first seven characters of the subject.

Spam is a **threat to national security** because of the bandwidth stolen (technological impact), the time wasted managing it (economic impact), and the aggravation it causes invokes a significant amount of collective bad will (health and possible criminal impact). Since national security is involved, spammers should be reclassified as saboteurs. This would also allow our military to reclassify spammers as "targets of opportunity" which makes those who reside overseas, legitimate military targets.

It is also important to distinguish that not only are the spammers guilty of criminal activity, but so are the businesses (and people) who employ them. The person who actually authorizes payment to a spammer should be held equally accountable for the crimes committed by the spammer because they are soliciting and financing the spammer's criminal activity.

It should also be required that ISPs give the option to their subscribers to be able to set up and upload IP and IP range blocks & country domain blocks. People who don't know anyone in China should be able to block the ".CN" domain without being forced to purchase special software.

In addition to prison time, spammers should be hit with draconian and mandatory minimum sentencing to include both prison time and financial penalties. Spammers maintaining American citizenship should be expatriated to a country from which they sent email. I propose a sentence of 1 year in prison and \$1,000 fine per each individual email recipient who did not authorize the marketer to solicit his business. For a spammer who sends a mere 100 UCEs to people who do not want to receive them, the spammer and the person who hired him should be sentenced to 100 years in prison and \$100,000 fine. The only way to terminate the spamming plague on society is to make examples.



TOM STATON

TOMSTAT@HOTMAIL.COM

2173 SANTA ANITA DR
LEXINGTON KY 40516

March 1, 2004

Via Hand-Delivery

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

Re: Comments of the Institute of Makers of Explosives; U.S. Sentencing Commission; Sentencing Guidelines for U.S. Courts; Notice, 68 Fed. Reg. 75340 (Dec. 30, 2003). Issues for Comment 11: Hazardous Materials

Dear Sir or Madam:

IME is pleased to provide comments on the above-captioned Federal Register Notice.

IME is the safety association of the commercial explosives industry. Our mission is to promote safety and security and the protection of employees, users, the public and the environment; and to encourage the adoption of uniform rules and regulations in the manufacture, transportation, storage, handling, use and disposal of explosive materials used in blasting and other essential operations.

IME represents all U.S. manufacturers of high explosives and other companies that distribute explosives or provide other related services. Over 2.5 million metric tons of explosives are consumed annually in the United States of which IME member companies produce over 95 percent. These products are used in every state in the Union and are distributed worldwide. The value of these products is estimated to be in excess of \$1 billion annually. The ability to manufacture, transport, store, and use these products safely and securely is critical to this industry. Accordingly, IME is interested in any changes to the U.S. Sentencing Guidelines that have the potential to impact the transportation of hazardous materials.

We submit the following comments on the above-captioned notice.

(1) A New Guideline Should be Created to Address Offenses Involving HAZMAT Transportation

IME agrees in principle with the concern expressed by the U.S. Department of Justice ("DOJ"), that the current sentencing guideline applicable to hazardous materials (§2Q1.2 *Mishandling of Hazardous or Toxic Substances or Pesticides; Recordkeeping, Tampering, and Falsification; Unlawfully Transporting Hazardous Materials in Commerce*), is not adequately suited to hazardous materials ("HAZMAT")-related transportation offenses.

As noted in the Federal Register notice, the §2Q1.2 Guidelines clearly are intended to cover offenses under the various U.S. environmental protection statutes and associated regulations and could, conceivably, be difficult to meaningfully apply to Department of Transportation (“DOT”)-regulated HAZMAT transportation offenses. For example, the only mention of transportation offenses in the §2Q1.2 Guidelines is at (b)(4); “If the offense involved transportation, treatment, storage, or disposal without a permit or in violation of a permit, increase by 4 levels.” §2Q1.2(b)(4). Clearly, this provision is directed at environmental *permitting* violations rather than the types of transportation-related offenses possible under DOT HAZMAT regulations. Where such offenses do not involve permitting, the Guideline is even less relevant as an appropriate tool.

Given the specificity of the current §2Q1.2 Guidelines to violations of environmental statutes, and the narrow, tailored structuring of the guideline to correspond to “typical” environmental recordkeeping and permitting requirements, and environmental “release” events, we believe there is substantial merit to DOJ’s recommendation that the §2Q1.2 Guidelines not be the sole frame of reference for sentencing violations of DOT HAZMAT requirements.

Accordingly, IME supports the alternative noted in the Federal Register Notice that a new guideline be created to more adequately and specifically address offenses involving the transportation of hazardous materials.

(2) An Appropriate Base Level For Offenses Involving the Transportation of Hazardous Materials Should Be Conservative Given the Diversity of Potential Hazards Posed by the Transportation of Commercial HAZMAT

As the Commission is no doubt aware, the transportation of hazardous materials is an essential, integral component of industrial and commercial activity and is ubiquitous throughout the United States (“U.S.”) and internationally. In addition, the quantity and variety of hazardous materials that are daily shipped in legitimate commerce in the U.S. is enormous, including widely recognizable materials such as gasoline to less obvious HAZMAT substances such as automotive airbags, various cosmetics, and a number of common food additives. Likewise, the relative potential danger – in a criminal context – posed by the myriad materials classified as HAZMAT varies as widely as the nature of the materials themselves.

While IME’s expertise in the area of HAZMAT transportation is limited to the transportation of explosives and related products, it is essential that the Commission fully appreciate the diversity and volume of these and other materials that are transported as HAZMAT. Similarly, the Commission should understand the potential (or lack thereof) that such materials might “provide a ‘target-rich’ environment for terrorists” or others with criminal intent. 68 Fed. Reg. at 75377. Any sentencing guidelines addressing hazardous materials offenses will necessarily and unavoidably have extraordinarily broad potential applicability and impact.



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.