

Indeed, WLF finds it remarkable and troubling that the Commission did not specifically solicit public comment as to whether it should greatly expand the definition of "violations of law" to include non-criminal regulations. Rather, the Commission seems to have already made up its mind on this issue, and is merely requesting comment as to whether the reduction in the culpability score for having an effective compliance program should be increased a paltry one point from the current three points to four points, "given the heightened requirements [*viz.*, expanding the definition of "violation of law" to include civil and regulatory offenses] for an effective program to prevent and detect violations of law under the proposed amendment." 68 Fed. Reg. 75360 (emphasis added). If it is a "given" that the Commission will expand the definition to include non-criminal provisions, the reduction in the score should be increased from the current three points to at least five points, rather than four.

Expanding the definition of violation of law to include civil and administrative regulations and provisions would simply be a costly "make work" requirement that would only benefit those who devise and implement compliance programs, or otherwise counsel companies on their compliance programs and the sentencing guidelines. Expanding the definition would skew priorities and drain corporate resources that could be better devoted to improving a compliance program to detect and prevent criminal activity, conduct which presumably is the most harmful to society. While the Advisory Group's desire is to foster a culture of compliance with respect to *all* federal and state regulations that are applicable to organizations, WLF believes that companies, rather than the Commission, can best decide how to devise compliance programs that are cost-effective and meaningful,

As we noted in our prior submission to the Advisory Group in May 2002, commentators have questioned this "feel good" approach to developing sentencing policy.

One of the continuing debates about criminal punishment concerns the extent to which the precise determination of penalties within the criminal sentencing process effectively serves any utilitarian goal of public law enforcement or is merely political theater. Even if we grant the point that some criminal sanction is more useful than none, there remain the questions of whether and when it is worthwhile at the margin to devote resources to refinements in the formal criminal penalty determination system, except perhaps as required to preserve marginal deterrence.

Jeffrey S. Parker & Raymond A. Atkins, *Did the Corporate Criminal Sentencing Guidelines Matter? Some Preliminary Empirical Observations*, 42 J. Law & Econ. 423, 424 (Apr. 1999). The Commission should keep in mind as it develops and amend the guidelines that while punishment and deterrence are indeed the goals of sentencing, Congress mandated that punishment and fines that are imposed by courts should be "sufficient, *but not greater than necessary*" to comply with the purposes of punishment and deterrence. 28 U.S.C. § 3553(a) (emphasis added). Accordingly, the Commission's and the Advisory Group's rejection of optimal penalties policy, and the lack of empirical evidence to determine what punishments have been effective without causing overdeterrence or gratuitous punishment, runs counter to Congress's express policy of conservation of punishment.

## **2. Eliminating the Prohibition on Three-Point Reduction for Delaying Reporting of Offense.**

The Commission also requested public comment as to whether the current prohibition on the receipt of a three-point reduction under Section 8C2.5 for unreasonably delaying reporting an offense to

the proper authorities should be modified so that the organization could at least be considered for a reduction. 68 Fed. Reg. 75359. WLF agrees with this flexible approach that the organization should be considered for a reduction, and that the current rule should be eliminated. What some may regard as an unreasonable delay, may in fact be legitimate due to the company's desire to investigate the incident thoroughly to determine whether a violation has in fact occurred and the extent of the alleged violation.

**3. Changing Automatic Preclusion under Section 8C2.5(f) To a Rebuttal Presumption.**

The Commission also requests comment as to whether Subsection (f) of Section 8C2.5 should be amended as proposed to change the automatic preclusion of a three-point reduction if certain high-level individuals participated in, condoned, or were wilfully ignorant of the corporate offense, to one where there is a rebuttable presumption that the three-point reduction does not apply. 68 Fed. Reg. 75359. WLF supports this more flexible approach and believes that the corporation should be able to show on a case-by-case basis why it believes that its compliance program deserves a reduction. Accordingly, the automatic preclusion should be changed to a rebuttable presumption of preclusion.

**4. Other Areas of Sentencing Policy That Should Be Addressed.**

Finally, the Commission requests comment on any other areas of sentencing policy that should be addressed. WLF has requested the Commission on several occasions that it should review the application of prison sentences meted out for violations of environmental offenses under Part 2Q. Criminal enforcement of environmental laws of both individuals and corporations have been growing over the years, and raise serious issues both respect to penalties for corporations, as well as those imposed on individuals in the form of lengthy and unwarranted prison terms under Sections 2Q1.2 and 2Q1.3 of the guidelines. In many cases, the Department of Justice overcharges by adding money laundering and other charges to the underlying substantive environmental offenses in order to drive up the sentencing score, resulting in grossly excessive sentences for what otherwise would be minor regulatory offenses.

As noted, a federal judge was forced to impose a draconian 97-month sentence on first offenders, which was at the low end of the 97-127 month range as determined by the guidelines, for the "crime" of importing seafood in plastic bags instead of cardboard boxes under the Lacey Act. *See McNab v. United States*, 331 F.3d 1228 (11th Cir. 2003), *cert. denied*, 2004 U.S. LEXIS 1041; 72 U.S.L.W. 3535. This prison sentence, longer than that meted out to some drug dealers, is, by any reasonable person's standards, clearly "*greater than necessary*" to comply with the purposes of punishment and deterrence under 28 U.S.C. § 3553(a). There are many other examples of unjust and excessive prison sentences that have been and are being imposed under the guidelines which call out for serious reconsideration and revision by this Commission. At a minimum, the Commission should have its staff or an advisory group review this problem area.

***Conclusion***

WLF appreciates the opportunity to provide these comments and urges the Commission to carefully consider the full impact that its guidelines and the proposed amendments would have on organizations before proposing them to Congress.

U.S. Sentencing Commission  
March 15, 2004  
Page 6

Respectfully submitted,

Daniel J. Popeo  
General Counsel

Paul D. Kamenar  
Senior Executive Counsel

encl

Select '**Print**' in your browser menu to print this document.

©2004 Legal Times Online

Page printed from: <http://www.legaltimes.com>

[Back to Article](#)

---

## Lawyers Seeing Red Over Lobster Case

Tony Mauro  
Legal Times  
02-16-2004

A dispute that began with a shipment of Honduran lobsters into Alabama has turned into an international incident that is now before the Supreme Court, complete with high-powered law firm and interest group participation.

At its Feb. 20 private conference, the Court will consider whether to add *McNab v. United States*, No. 03-622, and *Blandford v. United States*, No. 03-627, to its docket. The cases raise delicate issues of federal court interpretation of foreign law at a time when the Supreme Court itself is taking a fresh look at the importance of international law in its own jurisprudence.

Honduran citizen David McNab, a lobster fleet owner, and Robert Blandford and two other American seafood importers were arrested in Alabama in 1999 for importing 70,000 pounds of Caribbean spiny lobsters, a few of which were undersized and all of which were in plastic bags — in violation of a Honduran regulation that required shipment in cardboard boxes.

The four were indicted in federal court in Alabama for violations stemming from the Lacey Act, which prohibits the import of fish or wildlife taken or sold in violation of U.S. or "any foreign law." The fact that the shipment violated Honduran regulations was the predicate for a range of criminal charges, including money laundering. McNab, Blandford, and a third defendant were convicted and sentenced to eight years in prison. The fourth was sentenced to two years.

Meanwhile, as part of their legal battle, the importers successfully challenged the validity of the regulations in Honduras.

On appeal in the U.S. courts, the lobstermen claimed that the change in Honduran law dictated reversal of their U.S. convictions. The government of Honduras filed a brief in the appeal, asserting that the laws had no force at the time of the arrest, but the U.S. Court of Appeals for the 11th Circuit affirmed the convictions by a 2-1 vote.

The 11th Circuit acknowledged that a nation's own officials are "among the most logical sources" for interpreting that nation's laws. But the court concluded that, when a foreign government changes its position about those laws, the United States is not bound by the new interpretation. Heeding the new interpretation, the 11th Circuit majority stated, would lead to the "endless task of redetermining foreign law."

The 11th Circuit also suggested that future defendants with "means and connections" in a foreign country could lobby that country's officials to invalidate their laws as a way of undermining U.S. prosecutions. Circuit Judge Charles Wilson wrote the opinion,

joined by Judge Frank Hull.

In dissent, Senior Judge Peter Fay said the current Honduran interpretation should prevail, adding that the process of legal change criticized by the majority "occurs routinely in our country."

Former D.C. Circuit nominee Miguel Estrada, a Honduran native who is a D.C. partner at Gibson, Dunn & Crutcher, represents McNab in his appeal to the Supreme Court. "The 11th Circuit is alone among the courts of appeals in refusing to accord deference to the construction of foreign law adopted by the authorized representatives of the foreign states," Estrada tells the Court.

Former Solicitor General Seth Waxman, now a D.C. partner at Wilmer, Cutler & Pickering, filed a brief in the case for the Honduran government. "Mr. McNab's actions did not violate any valid or enforceable law in Honduras," Waxman says in the brief, also noting that Honduras "desires to protect its citizens from misapplication of Honduran law."

The lengthy prison term for seemingly minor trade violations, as well as the appeals court's decision to not follow Honduran legal authority, has given the case high visibility in Honduras. And it has been framed in the United States as an international criminal law equivalent of the McDonald's too-hot coffee cup — an example of laws and punishment run amok.

"It's a classic case of over-criminalization — honest people being sent to prison for eight years for using plastic instead of cardboard," says Paul Kamenar, senior counsel at the Washington Legal Foundation, which filed the petition on behalf of Blandford.

An unusual coalition of groups — including the National Association of Criminal Defense Lawyers and the National Association of Manufacturers — also filed a brief, bemoaning the increasing use of criminal law to enforce economic regulations when no criminal intent is shown.

In a brief by Paul Rosenzweig, a lawyer at the Heritage Foundation, the groups tell the Supreme Court that the elimination of criminal intent requirements "allows the government to engage in grotesque over-charging such as that demonstrated here — pyramiding trivial civil infractions of uncertain (and now disavowed) foreign law into smuggling and money laundering offenses that carry astronomical and unjust domestic criminal penalties."

The Justice Department defends the conviction before the high court.

"If the laws were valid in Honduras during the time period covered by the indictment, the defendants violated the Lacey Act," the government's brief states. "Whatever changes in the laws occurred after the lobsters were imported into the United States illegally have no effect on the defendants' convictions."

Deputy Solicitor General Paul Clement signed the brief, which notes that Solicitor General Theodore Olson is recused in the McNab case. Before becoming solicitor general in 2001, Olson was a partner at Gibson, Dunn, the firm that represents McNab.



March 15, 2004

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

**Re: Comments in Proceeding BAC2210-40/2211-01**

Dear Mr. Courlander:

The Internet Commerce Coalition appreciates the chance to respond to the Sentencing Commission's request for comments regarding the guidelines that will apply to criminal spam sent in violation of 18 U.S.C. § 1037. The Internet Commerce Coalition's ("ICC's") members include major ISPs and e-commerce companies and associations: AT&T, BellSouth, Comcast, eBay, MCI, SBC, TimeWarner/AOL, and Verizon, the U.S. Telecomm Association, CompTel and the Information Technology Association of America.

Curbing and deterring spam is a major priority for the ICC and its members. The ICC worked actively to support passage of § 1307 as part of the CAN-SPAM Act, and provided extensive factual and technical information to the authors of this part of the legislation. Section 1037 prohibits the major falsification and hacking methods that professional spammers use to evade software that protects users and ISP networks from spam.

## **I. OVERVIEW OF THE SPAM PROBLEM**

Spam currently constitutes over half of all traffic on the Internet. It floods user inboxes, and burdens ISP and corporate networks. The economic costs of spam have been estimated to be nearly \$9 billion in 2002, according to a study by Ferris Research. Spam is also the leading complaint of Internet users regarding their Internet experience.

Most spam is sent in violation of federal and state fair trade practice laws, and civil spam laws. ICC members have sued well over 100 spammers, and the FTC has brought a large number of enforcement actions against spammers. These efforts have thus far not dissuaded professional spammers, who routinely employ falsification and hacking methods prohibited by from continuing to increase the volume of spam on the Internet. Many of the largest spammers continue to live in the United States sending out hundreds of millions of spam emails using these methods with relative impunity. Indeed, 8 of the top 10 spammers worldwide as measured by the anti-spam organization Spamhaus live in the United States. See <http://www.spamhaus.org>. Foreign governments and ISPs routinely complain about the huge volume of spam that comes from the U.S.

For these reasons, ICC members are convinced that criminal enforcement against professional spammers who rely on the hacking and falsification tactics prohibited by § 1037 is essential to reduce the spam problem. Large-scale professional falsification spammers and their co-conspirators are willing to risk the threat of civil litigation. However, if they perceive that continued violations create a meaningful risk of prosecution and significant prison time (not probation), we believe that U.S. spammers will find a different line of work, and the rising tide of spam will abate.

Section 1037 prohibits knowingly “initiating” illegal messages, and defines “initiate” as including both transmitting and procuring the transmission of the illegal emails. 15 U.S.C. § 7702(9). Spammers who use falsification tactics prohibited in § 1037 and the advertisers who knowingly procure and profit from their activities are fundamentally different from legitimate companies who use email for promotional purposes. These spammers and businesses who rely on spam regularly employ highly fraudulent and deceptive conduct such as computer hacking, wire and mail fraud, false and deceptive advertising, and misappropriating the identities of others in order to obtain computers, email accounts, Internet domains or Internet protocol addresses from which to spam, use of multiple bank accounts and use of sham corporations. These egregious activities are very similar to those of other criminal enterprises that are treated severely under the Sentencing Guidelines. They are also fundamentally different from the ways that legitimate businesses and individuals use email, so that there is little risk of the prohibitions in § 1037 being applied unjustly.

The worst of the advertisers who advertise by means of these outlawed techniques have a policy or practice of paying others to advertise their products and services in ways that violate § 1037. The entities often compensate spammers who send email on their behalf by paying for sales leads or by paying commission on actual sales. In addition to the knowledge of the illegal conduct, factors to consider in sentencing such individuals or corporations include whether the conduct appears to be grounded in either written or unwritten policy or established practice; whether there is evidence of similar conduct in a significant proportion of the defendant’s email campaigns; and whether the procurer had the ability to control the illegal spamming activity.

Because of the significant harm caused by and egregious tactics used by professional violators of § 1037, and the need for sufficient incentives for criminal prosecution of spammers, the ICC urges the Commission to set sufficiently strong penalties for violations of this statute.

## **II. ANSWERS TO THE COMMISSION’S QUESTIONS**

**(1) What are the appropriate guideline penalties for a defendant convicted under 18 U.S.C. § 1037?**

**(a) Should the new offense(s) be referenced in Appendix A (Statutory Index) to §§ 2B1.1 (Fraud, Theft, and Property Destruction), and 2B2.3 (Trespass), and/or to some other guideline(s)?**

It is our view that § 1037 offenses are properly referenced in Appendix A to § 2B1.1, the fraud, theft, and property destruction guideline. Spammer falsification and hacking tactics are most closely related to conduct covered in this guideline, and particularly to the penalty offense levels provided for computer hacking set forth in § 2B1.1(b)(13) that were implemented after the passage of the Homeland Security Act. On the other hand, the penalties for the more serious § 1037 offenses, including those involving highly organized sophisticated business operations and massive volumes, may deserve more severe penalties than those available for many of the hacking offenses. At the same time, some of the violations may be minor in nature. As a result, the guidelines provisions should not be so inflexible as to prevent probation sentences in some instances.

The trespass guideline, § 2B2.3, is far less suitable since the offense levels within this guideline are low and do not properly reflect the seriousness of § 1037 violations. There certainly may be situations where § 1037 offenses may be linked to offenses involving sexual exploitation of minors and obscenity (§§ 2G1.1, 2G1.2 and 2G1.3) and offenses involving criminal enterprises and racketeering (§ 2E1.1).

**(b) What is the appropriate base offense level for the new offense(s)?**

We believe that the base offense level of 6, which is used for § 2B1.1, would be an appropriate starting point for § 1037 offenses. This is particularly the case as just noted because there will be minor offenses that would properly be dealt with by probationary sentences.

**(c) Should the offense level vary depending on the seriousness of the offense (for example, should the base offense level for a regulatory violation under 18 U.S.C. § 1037 be the same as the base offense level for a more serious violation under that statute)?**

The statute makes it clear that offense levels should vary depending upon the seriousness of the offense and provides the Commission with clear directions in this regard. We take no position with reference to regulatory violations.

**(d) If 18 U.S.C. § 1037 is referenced to § 2B1.1, should special offense characteristics be added to that guideline that ensures application of the multiple victim enhancement at § 2B1.1(b)(2)(A)(I) or the mass marketing enhancement at § 2B1.1(b)(2)(A)(ii) to a defendant convicted of 18 U.S.C. § 1037? Should a defendant convicted under 18 U.S.C. § 1037 receive an enhancement under § 2B1.1(b)(2)(A)(i) or (ii) based on a threshold quantity of email messages involved in the offense, and if so, what is that threshold quantity? Another option which might be better is to create special offense characteristics for § 1037 offenses.**

We strongly recommend that special offense characteristics be used to enhance sentences for more serious and sophisticated violations of § 1037. First of all, the statute reflects Congress' intent that a threshold quantity of email messages – 2,500 per day, 25,000 per month or 250,000 per year – should be taken into account in determining enhancement of the defendant's sentence.

In order for Internet Service Providers to protect their network and subscribers, they have developed sophisticated techniques to eliminate spam messages before they get into the service.



Spammers typically destroy as much of the technical trail of their spamming as possible in order to avoid detection. Additionally, most ISPs along the trail through which a spam message travels typically do not preserve the relevant transmission logs for an extended period, due to the massive volumes of data involved in keeping track of the communications that cross their networks every day. Some companies (like AOL) may be able to provide evidence of the violation only by obtaining and storing consumer complaints, which have proven to be only a small fraction of the volume of email that a professional spammer actually transmitted or attempted to transmit. In AOL's experience, the volume of email actually sent by a spammer is several orders of magnitude larger than the volume of complaints received about that spammer. Recognizing these factors, Congress set the appropriate felony trigger for volume at 2,500 per day/25,000 per month and 250,000 per year. Proof of a continuing pattern of violations above this level should trigger an enhancement of the sentence beyond the baseline felony level.

Section 1037(a) and (b)(2) offenses should include at least the following special offense characteristics:

1. Increases to the base offense level for each of the factors listed in the statute: offense committed in furtherance of felonies; prior convictions; use of false account or domain name registrations; message volume; proof of victim loss or offender gain, including injuries to consumers caused by loss of access to accounts or equipment or because of identity theft; and major leadership role in the offense;
2. Increases to the base offense level for the use of sophisticated means; and
3. The addition of language to § 2B1.1(b)(8) (the provision which increases the offense level for relocating operations to evade law enforcement) to include specific language addressing evasion techniques spammers use to evade detection.

The sophisticated means enhancement should include using methods that evade secure email systems under development that authenticate senders or Internet domains used by a senders as legitimate by means of digital certificates. If a defendant cracks the security of a sender authentication technology or shares that information with others, or steals the identity of a trusted sender of email in order to send spam, an enhancement of at least 2 levels is warranted, and similar to the provisions of § 2B1.1(b)(9), if the resulting offense level is less than level 12, there should be an increase to that level.

**(e) Under what circumstances shall an offense under 18 U.S.C. § 1037 be considered to involve sophisticated means?**

As just noted, in light of the serious problems created by "professional spammer" falsification tactics, use of sophisticated means should trigger an enhancement. Section 1037(b) sets out a series of factors that reflect sophisticated means for committing the offense and that merit an enhancement for sophisticated means. These include sending a high volume of email and supervising others in the offense. Presence of these factors might trigger an enhancement to level 14 (15-21 months).

In addition, several other factors not specified in the statute reflect efforts to conceal the offense and would merit enhancements that might be similar to § 2B1.1(b)(8) of the Guidelines. These include:

- (a) destruction of email records by a spammer;
- (b) use of computer facilities outside the boundaries of the United States, a common method by which sophisticated spammers attempt to evade enforcement in the U.S.; and
- (c) use of shell corporations or multiple bank accounts to evade detection.

Each of these factors are sufficiently serious to warrant enhancements of 2 levels.

**(f) Consistent with the directive in section 4(b)(2) of the CAN-SPAM Act of 2003, should § 2B1.1 contain an enhancement for defendants convicted under 18 U.S.C. § 1037 who (i) obtain e-mail addresses through improper means, including the harvesting of e-mail addresses from the users of a website, proprietary service, or other online public forum without authorization and the random generating of e-mail addresses by computer; or (ii) 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?**

In our view, each of these factors also should trigger enhancements.

1. Harvesting email addresses by automated means, in violation of the rules of the online service or online forum where those addresses are posted, is a significant source of unwanted spam that penalizes the use of public fora such as personal or professional web pages, online marketplaces and Internet discussion fora. It chills free speech on the Internet and chills e-commerce in public fora.

2. Dictionary attacks occur through several ways. The first is a “phone book attack,” in which a spammer generates email addresses corresponding to all possible name and first initial combinations in the phone book of one or more large metropolitan areas. The second is a pure random alphanumeric attack—the spammer sends to every alphanumeric combination permitted, for example, in a 16 character AOL address prefix. The third method is sending email to “culled” lists originally generated using any of the two previous techniques, but where the spammer has run the list once and culled out the invalid addresses based on records of undeliverable emails. Dictionary attacks are in effective methods used to obtain a password to which to send spam and thereby to access target accounts for illicit purposes. Such attacks generate a very large number of emails sent to false addresses and significantly burden networks with returned emails. Given the seriousness of dictionary attacks, enhancements should be increases of up to 6 levels, comparable to § 2B1.1(b)13(A)(iii) offenses.

3. Advertising or including an Internet domain with false registration information is a common tool by which the spam kingpins who pay for spam to be sent out on their behalf evade detection. Use of any of these means might result in an increase of 5 offense levels.

**(g) Which adjustments should be considered directly pertinent to § 1037 offenses?**

There are adjustments in Chapter 3 that could be pertinent to § 1037 offenses. These include the vulnerable victim adjustment under § 3A1.1; the role in the offense aggravating and mitigating adjustments under §§ 3B1.1 and 3B1.2; the abuse of trust or use of special skill adjustment under § 3B1.3; and the obstruction or impeding the administration of justice adjustment under § 3C1.1. Unless they are utilized as special offense characteristics in § 2B1.1, these adjustments should be used to significantly increase offense levels (and, in the case of an individual with a minor role in the offense, or a minor duped into spamming activity by a sophisticated spammer, to decrease the levels). In order to ensure that the factors are used in calculating penalties, it might be preferable to incorporate these adjustments as special offense characteristics.

The vulnerable victim adjustment should apply, for example, where spammers impersonate an innocent person in the course of the violation—e.g., by hacking into another person's account and sending spam, falsely placing that person's email address in the "from" line of spam emails, or using another person's identification information in registering for an email account, domain name or to obtain their Internet Protocol address space. Such tactics smear another person's name, can cause that other person to lose good will or to lose access to the Internet, and even to receive death threats from outraged recipients of offensive spam.

**(2) What are the appropriate guideline penalties for offenses other than 18 U.S.C. § 1037 (such as those specified by section 4(b)(2) of the CAN-SPAM Act of 2003, i.e., offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children) that may be facilitated by the sending of a large volume of unsolicited e-mail?**

Specifically, should the Commission consider providing an additional enhancement for the sending of a large volume of unsolicited email in any of the following: § 2B1.1 (covering fraud generally and identity theft), the guidelines in Chapter Two, Part G, Subpart 2, covering child pornography and the sexual exploitation of children, and the guidelines in Chapter Two, Part G, Subpart 3, covering obscenity? Alternatively, should the Commission amend existing enhancements, or the commentary pertaining thereto, in any of these guidelines to ensure application of those enhancements for the sending of a large volume of unsolicited email? For example, should the Commission amend the enhancements, or the commentary pertaining to the enhancements, for the use of a computer in the child pornography guidelines, §§ 2G2.1, 2G2.2, and 2G2.4, to ensure that those enhancements apply to the sending of a large volume of unsolicited email?

As reflected earlier, violations of § 1037 that involve violations of other serious felony statutes should trigger an enhancement of the § 1037 that makes the offense level comparable to what it would have been if the sentencing guidelines for the other provisions would have been used.

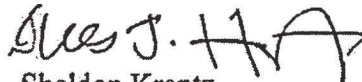
**(4) What types of penalties should be considered for violations by corporations?**

Section 1037 does not provide specific fine provisions for corporations. If § 2B1.1 will be utilized as the pertinent guideline, corporations will be sentenced under the provisions of §§ 8C2.3-8C2.9 in the absence of other directives. If these provisions are utilized for calculating organizational fines, it will be necessary to specify special offense characteristics for organizations in § 2B1.1 that will increase fine levels to appropriate levels. For large corporate violators, this will require that the total offense level would need to be set at levels of 20 or higher.

In ICC members' experience suing spammers, spammers who engage in conduct that violates § 1037 incorporate as part of a strategy of evading detection. There are usually few employees, all of whom are principals in the act of sending spam. More sophisticated outlaw spammers sometimes use corporate shells to transfer assets (e.g. e-mail lists) in the wake of civil lawsuits. Some spammers also cycle through lots of corporate identities to avoid the effects of recipient opt outs. Use of incorporation as a further form of falsification is very different than questions of whether a legitimate corporate entity has complied with this provision of law. Use of this falsification method should be treated as an enhancing factor, and should under no circumstances entitle a defendant to lesser punishment.

The provisions of § 8C1.1 should be used in situations where an entity has been created entirely or primarily for criminal purposes or to operate primarily by criminal means. Under § 8C1.1, when this occurs, the fine level is set at an amount that divests the entity of all of its net assets.

Respectfully submitted,



Sheldon Krantz

James J. Halpert

Piper Rudnick L.L.P.

1200 19<sup>th</sup> Street, N.W.

Washington, DC 20036

(202) 861-3900

Counsel to the Internet Commerce Coalition