

**§ 7703. Prohibition against predatory and abusive commercial e-mail**

**(a) Omitted**

**(b) United States Sentencing Commission**

**(1) Directive**

Pursuant to its authority under section 994(p) of title 28 and in accordance with this section, the United States Sentencing Commission shall review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for violations of section 1037 of title 18, as added by this section, and other offenses that may be facilitated by the sending of large quantities of unsolicited electronic mail.

**(2) Requirements**

In carrying out this subsection, the Sentencing Commission shall consider providing sentencing enhancements for—

(A) those convicted under section 1037 of title 18 who—

(i) obtained electronic mail addresses through improper means, including—

(I) harvesting electronic mail addresses of the users of a website, proprietary service, or other online public forum operated by another person, without the authorization of such person; and

(II) randomly generating electronic mail addresses by computer; or

(ii) knew that the commercial electronic mail messages involved in the offense contained or advertised an Internet domain for which the registrant of the domain had provided false registration information; and

(B) those convicted of other offenses, including offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children, if such offenses involved the sending of large quantities of electronic mail.

**(c) Sense of Congress**

It is the sense of Congress that—

(1) Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems; and

(2) the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes, including the tools contained in chapters 47 and 63 of title 18 (relating to fraud and false statements); chapter 71 of title 18 (relating to obscenity); chapter 110 of title 18 (relating to the sexual exploitation of children); and chapter 95 of title 18 (relating to racketeering), as appropriate.

(Pub. L. 108–187, § 4, Dec. 16, 2003, 117 Stat. 2703.)

**CODIFICATION**

Section is comprised of section 4 of Pub. L. 108–187. Subsec. (a) of section 4 of Pub. L. 108–187 enacted section 1037 of Title 18, Crimes and Criminal Procedure, and amended analysis for chapter 47 of Title 18. The

provisions of subsec. (b) of section 4 of Pub. L. 108–187 are also listed in a table relating to sentencing guidelines set out as a note under section 994 of Title 28, Judiciary and Judicial Procedure.

**§ 7704. Other protections for users of commercial electronic mail**

**(a) Requirements for transmission of messages**

**(1) Prohibition of false or misleading transmission information**

It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph—

(A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;

(B) a “from” line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading; and

(C) header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

**(2) Prohibition of deceptive subject headings**

It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (consistent with the criteria used in enforcement of section 45 of this title).

**(3) Inclusion of return address or comparable mechanism in commercial electronic mail**

**(A) In general**

It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that—

(i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and