AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 288

108TH CONGRESS, 1st Session | SENATE | REPORT 108–170

THE CRIMINAL SPAM ACT OF 2003

OCTOBER 22, 2003.—Ordered to be printed

Mr. HATCH, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany S. 1293]

The Committee on the Judiciary, to which was referred the bill (S. 1293) to criminalize the sending of predatory and abusive e-mail, having considered the same, reports favorably thereon, with an amendment in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

		Page
I.	Purpose and Summary	1
II.	Background and Need for the Legislation	2
III.	Discussion	2
IV.	Legislative History	5
V.	Votes of the Committee	5
VI.	Section-by-Section Analysis	5
VII.	Cost Estimate	6
VIII.	Regulatory Impact Statement	7
IX.	Changes in Existing Law	7

I. PURPOSE AND SUMMARY

The purpose of S. 1293, the "Criminal Spam Act of 2003," is to criminalize the sending of bulk commercial e-mail (commonly known as "spam") through fraudulent and deceptive means. The bill amends title 18, United States Code, to prohibit five principal techniques that spammers use to evade filtering software and hide their trails. Penalties for violations of the new criminal prohibitions include imprisonment, fines, and forfeiture of proceeds. Offenders may also be subject to civil enforcement actions brought by either the Department of Justice or by an Internet Service Provider ("ISP").

29–010

II. Background and Need for the Legislation

Sophisticated spammers send millions of e-mail messages quickly, at an extremely low cost, with no repercussions. The sheer volume of spam, which is growing at an exponential rate, is overwhelming entire network systems, as well as consumers' in-boxes. By the end of the year 2003, it is estimated that fifty percent of all e-mail traffic will be spam.

The rapid increase in the volume of spam has imposed enormous costs on our economy. A recent study by Ferris Research estimates that spam will cost U.S. businesses more than $10 billion in 2003 as a result of lost productivity and the need to purchase more powerful servers and additional bandwidth, configure and run spam filters, and provide help-desk support for spam recipients. The costs of spam are significant to individuals as well, including time spent identifying and deleting spam, inadvertently opening spam, installing and maintaining anti-spam filters, tracking down legitimate messages mistakenly deleted by spam filters, and paying for the ISPs' blocking efforts.

And there are other prominent and equally important costs of spam. It may introduce viruses, worms, and Trojan horses into personal and business computer systems, including those that support our national infrastructure. It has become the tool of choice for those who distribute pornography and indulge in fraud schemes. Rarely a minute passes without American consumers and their children being bombarded with e-mail messages promoting pornographic web sites, illegally pirated software, bogus charities, pyramid schemes and other "get rich quick" or "make money fast" scams.

Spam also offers fertile ground for deceptive trade practices. The Federal Trade Commission estimates that nearly 66 percent of spam contains some kind of deception, either in the content, the "subject" line, or the "from" line. And an astonishing 90 percent of spam involving investment and business opportunities contains indicia of false claims. This rampant deception has the potential to undermine Americans' trust of valid information on the Internet and threaten the future viability of all e-commerce.

ISPs are doing their best to shield customers from spam, blocking billions of unwanted e-mails each day, but the spammers are winning the battle. Among the barriers ISPs face when attempting to stop spam is that spammers use false and fraudulent means to avoid detection and identification. The Criminal Spam Act takes initial steps to address this problem.

III. Discussion

The Criminal Spam Act prohibits five deceptive techniques that spammers use to evade filtering software and get their unwanted e-mails into America's inboxes.

First, the bill prohibits hacking into another person's computer system and sending bulk spam from or through that system. This would criminalize the common spammer technique of obtaining access to other people's e-mail accounts on an ISP's e-mail network, for example by password theft or by inserting a "Trojan horse" program—that is, a program that unsuspecting users download onto

their computers and that then takes control of those computers—to send bulk spam.

Second, the bill prohibits using a computer system that the owner makes available for other purposes as a relay or retransmission point for bulk spam, with the intent of deceiving recipients as to the origins of the spam. This prohibition would criminalize another common spammer technique—the abuse of third parties' "open" servers, such as e-mail servers that have the capability to relay mail, or proxy servers that have the ability to generate or retransmit e-mail, such as "form" e-mail utilities on Web servers. Spammers commandeer these servers to send bulk commercial e-mail without the server owner's knowledge, either by "relaying" their e-mail through an "open" e-mail server, or by abusing an "open" proxy server's capability to generate or retransmit e-mails as a means to originate spam. In some instances the hijacked servers are even completely shut down as a result of tens of thousands of undeliverable messages generated from the spammer's e-mail list.

Third, the bill prohibits falsifying the header information that accompanies e-mail, and sending bulk spam accompanied by or containing that false header information. More specifically, the bill prohibits forging information regarding the origin of an e-mail message, the route through which the message penetrated, or attempted to penetrate, ISP filters, or information authenticating the user for network management or network security purposes—for example, as a "trusted sender" who abides by appropriate consumer protection rules. The last type of forgery will be particularly important in the future, as ISPs and legitimate marketers develop "white list" and similar rules and technologies whereby e-mailers who abide by self-regulatory codes of good practices will be allowed to send e-mail to users without being subject to anti-spamming filters. There is currently substantial interest among marketers and e-mail service providers in "white list" technology solutions to spam. However, such "white list" systems would be useless if outlaw spammers are allowed to counterfeit the authentication mechanisms used by legitimate e-mailers.

Fourth, the bill prohibits registering for multiple e-mail accounts or Internet domain names using information that falsifies the identity of the actual registrant, and sending bulk e-mail from those accounts or domains. This provision targets deceptive "account churning," a common outlaw spammer technique that works as follows: The spammer registers (usually by means of an automatic computer program, or by means of individuals located in other countries) for large numbers of e-mail accounts or domain names, using false registration information, then sends bulk spam from one account or domain after another. This technique stays ahead of ISP filters by hiding the source, size, and scope of the sender's mailings, and prevents the e-mail account provider or domain name registrar from identifying the registrant as a spammer and denying his registration request. Falsifying registration information for domain names also violates a basic contractual requirement for domain name registrations.

Fifth, the bill addresses another significant hacker spammer technique for hiding identity that is a common and pernicious alternative to domain name registration—hijacking unused Internet

Protocol ("IP") addresses and using them as launch pads for spam. Hijacking large blocks of IP address space is not difficult: Spammers simply falsely assert that they have the right to use that space, and obtain an Internet connection for the addresses. Hiding behind those addresses, they can then send vast amounts of spam that is extremely difficult to trace.

Penalties for violations of these prohibitions are graduated. Recidivist offenders under federal or state anti-hacking or spam laws and those who send spam in furtherance of another felony may be imprisoned for up to five years. Large-volume spammers, those who hack into another person's computer system to send bulk spam, those involved in offenses involving 20 or more falsified e-mail accounts or 10 or more falsified domain names or any combination thereof, those who cause more than $5,000 in "loss" as defined in 18 U.S.C. § 1030 during a one-year period, those who, as a result of the offense, obtain anything of value aggregating $5,000 or more during a one-year period, and spam "kingpins" who use others to operate their spamming operations may be imprisoned for up to three years. Other offenders may be fined and imprisoned for no more than one year.

Convicted offenders are also subject to forfeiture of proceeds and instrumentalities of the offense, and the U.S. Sentencing Commission is directed to consider sentencing enhancements for offenders who obtained e-mail addresses through improper means, such as harvesting and randomly generating e-mail addresses (in what is known colloquially as a "dictionary attack"), or who know that commercial e-mail addresses contain or advertise an Internet domain for which the registrant has provided false registration information.

In addition, as a supplement to criminal enforcement, the bill provides for civil enforcement by the Department of Justice and aggrieved ISPs against spammers who engage in conduct that the bill prohibits, as well as anyone who conspires with them.

Finally, because an effective solution to the spam problem requires the cooperation and assistance of our Nation's international partners, the Criminal Spam Act directs the Department of Justice and Department of State to report to Congress within 18 months regarding the status of their efforts to achieve international cooperation from other countries in investigating and prosecuting spammers worldwide.

In approving the Criminal Spam Act, the Committee determined that it does not raise concerns under the First Amendment. First, rather than targeting speech, the bill instead targets e-mailing techniques used to steal computer services and trespass on private computers and computer networks. Second, to the extent that the bill implicates any First Amendment interest, it addresses only commercial e-mail messages (because the overwhelming majority of predatory and abusive e-mail is commercial), and only when such messages are misleading by virtue of falsifying their point of origin. It therefore fails the first prong of the test set forth in the *Central Hudson Gas & Elec. Corp.* v. *Public Service Comm'n,* 447 U.S. 557, 566 (1980) (in commercial speech cases, court must first determine that the expression concerns lawful activity and is not misleading).

IV. Legislative History

During the past several Congresses, committees in both the House and the Senate have examined various issues raised by the proliferation of junk commercial e-mail. Additionally, government agencies, industry representatives, and other interested parties have participated in numerous public forums on spam, including a three-day "Public Spam Workshop" hosted by the FTC earlier this year.

On June 19, 2003, after extensive consultation with experts in this area, Senators Hatch, Leahy Schumer, Grassley, Feinstein, DeWine, and Edwards introduced S. 1293, the Criminal Spam Act of 2003.

V. Votes of the Committee

On September 25, 2003, the Committee on the Judiciary, with a quorum present, met in open session and ordered favorably reported the bill, S. 1293, by unanimous consent, with an amendment in the nature of a substitute sponsored by Senators Hatch and Leahy.

The substitute amendment made four changes to the bill: (1) Added proposed 18 U.S.C. § 1037(a)(5), which targets spammers who falsely represents the right to use five or more IP addresses, and intentionally initiate the transmission of spam from such addresses; (2) amended proposed 18 U.S.C. § 1037(a)(4), to clarify that the Government may prove its case by showing that the requisite number of e-mails went through "any combination of" falsely registered e-mail accounts or domain names; (3) narrowed the definition of "header information" in proposed 18 U.S.C. § 1037(e)(4), to address concerns that it was overbroad; and (4) made technical changes to the criminal forfeiture provisions, rendering them more consistent with existing laws. The substitute amendment was accepted by unanimous consent.

VI. Section-by-Section Analysis

Section 1. Short title

This bill may be cited as the "Criminal Spam Act of 2003".

Section 2. Prohibition against predatory and abusive commercial e-mail

This section targets the five principal techniques that spammers use to evade filtering software and hide their trails. It creates a new federal crime that prohibits hacking into a computer, or using a computer system that the owner has made available for other purposes, to send bulk commercial e-mail. It also prohibits sending bulk commercial e-mail that either conceals the true source, destination, routing or authentication information of the e-mail, or is generated from multiple e-mail accounts or domain names that falsify the identity of the actual registrant, or from Internet Protocol (IP) addresses that have been hijacked from their true assignees.

Penalties range from up to 5 years' imprisonment where the offense was committed in furtherance of any felony, or where the defendant was previously convicted of a similar federal or state offense, to up to 3 years' imprisonment where other aggravating fac-

tors exist, to up to 1 year of imprisonment where no aggravating factors exist, plus criminal forfeiture. The U.S. Sentencing Commission is directed to consider sentencing enhancements for offenders who obtained e-mail addresses through improper means, such as harvesting.

In addition, this section provides for civil enforcement by the Department of Justice and aggrieved Internet service providers against spammers who engage in the conduct described above. In appropriate cases, courts may grant injunctive relief, impose civil penalties, and award damages.

Section 3. Report and sense of Congress regarding international spam

Recognizing that an effective solution to the spam problem requires the cooperation and assistance of our international partners, this section asks the Administration to work through international fora to gain the cooperation of other countries in investigating and prosecuting spammers worldwide, and to report to Congress about its efforts.

VII. Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, October 1, 2003.

Hon. Orrin G. Hatch,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1293, the Criminal Spam Act of 2003.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

Elizabeth M. Robinson
(For Douglas Holtz-Eakin, Director).

Enclosure.

S. 1293—Criminal Spam Act of 2003

CBO estimates that implementing S. 1293 would have no significant cost to the federal government. Enacting the bill could affect direct spending and revenues, but CBO estimates that any such effects would not be significant. S. 1293 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

S. 1293 would make it illegal to use electronic mail to send deceptive or unauthorized messages regarding commercial products or services. Because the bill would establish a new federal crime, the government would be able to pursue cases that it otherwise would not be able to prosecute. However, we expect that S. 1293 would apply to a relatively small number of offenders, so any increase in costs for law enforcement, court proceedings, or prison operations would not be significant. Any such costs would be subject to the availability of appropriated funds.

Because those prosecuted and convicted under S. 1293 could be subject to civil and criminal fines, the federal government might collect additional fines if the legislation is enacted. Collections of civil fines are recorded in the budget as revenues. Criminal fines are recorded as revenues, then deposited in the Crime Victims Fund and later spent. CBO expects that any additional revenues and direct spending would not be significant because of the small number of cases involved.

In addition, persons prosecuted and convicted under the bill also could be subject to the seizure of certain assets by the federal government. Proceeds from the sale of such assets would be deposited in the Assets Forfeiture Fund and spent from that fund, mostly in the same year. Thus, enacting S. 1293 could increase both revenues deposited into the fund and direct spending from the fund. However, CBO estimates that any increased revenues or spending would not be significant.

The CBO staff contact for this estimate is Mark Grabowicz. This estimate was approved by Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

VIII. Regulatory Impact Statement

In compliance with paragraph 11(b)(1), rule XXVI of the Standing Rules of the Senate, the Committee, after due consideration, concludes that S. 1293 will not have significant regulatory impact.

IX. Changes in Existing Law

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by S. 1293, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

Part	Section
I. CRIMES	1

* * * * * * *

PART I—CRIMES

Chapter	Section
1. General provisions	1
* * * * * * *	
47. Fraud and false statements	1001

* * * * * * *

CHAPTER 47—FRAUD AND FALSE STATEMENTS

Sec.
1001. Statements or entries generally.

* * * * * * *

1036. Entry by false pretenses to any real property, vessel, or aircraft of the United States or secure area of any airport.
1037. Fraud and related activity in connection with electronic mail.

* * * * * * *

§ 1036. Entry by false pretense to any real property, vessel, or aircraft of the United States or secure area of any airport

(a) Whoever, by any fraud or false pretense, enters or attempts to enter—

(1) any real property belonging in whole or in part to, or leased by, the United States;

* * * * * * *

(c) As used in this section—

(1) the term "secure area" means an area access to which is restricted by the airport authority or a public agency; and

(2) the term "airport" has the meaning given such term in section 47102 of title 49.

§ 1037. Fraud and related activity in connection with electronic mail

(a) IN GENERAL.—Whoever, in or affecting interstate or foreign commerce, knowingly—

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer;

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages;

(3) falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages;

(4) registers, using information that falsifies the identity of the actual registrant, for 5 or more electronic mail accounts or online user accounts or 2 or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names; or

(5) falsely represents the right to use 5 or more Internet protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses;

or conspires to do so, shall be punished as provided in subsection (b).

(b) PENALTIES.—The punishment for an offense under subsection (a) is—

(1) a fine under this title, imprisonment for not more than 5 years, or both, if—

(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

(2) a fine under this title, imprisonment for not more than 3 years, or both, if—

(A) the offense is an offense under subsection (a)(1);

(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

(D) the offense caused loss to 1 or more persons aggregating $5,000 or more in value during any 1-year period;

(E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or

(F) the offense was undertaken by the defendant in concert with 3 or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

(c) FORFEITURE.—

(1) IN GENERAL.—The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States—

(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

(2) PROCEDURES.—The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

(d) CIVIL REMEDIES.—

(1) IN GENERAL.—The Attorney General, or any person engaged in the business of providing an Internet access service to the public aggrieved by reason of a violation of subsection (a), may commence a civil action against the violator in any appropriate United States District Court for the relief set forth in paragraphs (2) and (3). No action may be brought under this subsection unless such action is begun within 2 years of the date of the act which is the basis for the action.

(2) ATTORNEY GENERAL ACTION.—In an action by the Attorney General under paragraph (1), the court may award appropriate relief, including temporary, preliminary, or permanent injunctive relief. The court may also assess a civil penalty in an

amount not exceeding $25,000 per day of violation, or not less than $2 or more than $8 per electronic mail message initiated in violation of subsection (a), as the court considers just.

(3) OTHER ACTIONS.—In any other action under paragraph (1), the court may award appropriate relief, including temporary, preliminary, or permanent injunctive relief, and damages in an amount equal to the greater of—

(A) the actual damages suffered by the Internet access service as a result of the violation, and any receipts of the violator that are attributable to the violation and are not taken into account in computing actual damages; or

(B) statutory damages in the sum of $25,000 per day of violation, or not less than $2 or more than $8 per electronic mail message initiated in violation of subsection (a), as the court considers just.

(e) DEFINITIONS.—In this section:

(1) COMMERCIAL ELECTRONIC MAIL MESSAGE.—The term "commercial electronic mail message" means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website or online site operated for a commercial purpose).

(2) COMPUTER AND PROTECTED COMPUTER.—The terms "computer" and "protected computer" have the meaning given those terms in section 1030(e) of this title.

(3) DOMAIN NAME.—The term "domain name" means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority, and that is included in an electronic mail message.

(4) HEADER INFORMATION.—The term "header information" means the source, destination, and routing information attached to an electronic mail message, including the originating domain name, the originating electronic mail address, and technical information that authenticates the sender of an electronic mail message for network security or network management purposes.

(5) INITIATE.—The term "initiate" means to originate an electronic mail message or to procure the origination of such message, regardless of whether the message reaches its intended recipients, and does not include the actions of an Internet access service used by another person for the transmission of an electronic mail message for which another person has provided and selected the recipient electronic mail addresses.

(6) INTERNET ACCESS SERVICE.—The term "Internet access service" has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

(7) LOSS.—The term "loss" has the meaning given that term in section 1030(e) of this title.

(8) MESSAGE.—The term "message" means each electronic mail message addressed to a discrete addressee.

(9) MULTIPLE.—The term "multiple" means 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.

○