

[First Reprint]

SENATE COMMITTEE SUBSTITUTE FOR
SENATE, No. 1037

STATE OF NEW JERSEY
211th LEGISLATURE

ADOPTED MARCH 8, 2004

Sponsored by:

Senator JOSEPH CONIGLIO

District 38 (Bergen)

Assemblyman JEFF VAN DREW

District 1 (Cape May, Atlantic and Cumberland)

Assemblyman PETER C. EAGLER

District 34 (Essex and Passaic)

Assemblyman KIRK CONOVER

District 2 (Atlantic)

Assemblywoman LINDA R. GREENSTEIN

District 14 (Mercer and Middlesex)

Co-Sponsored by:

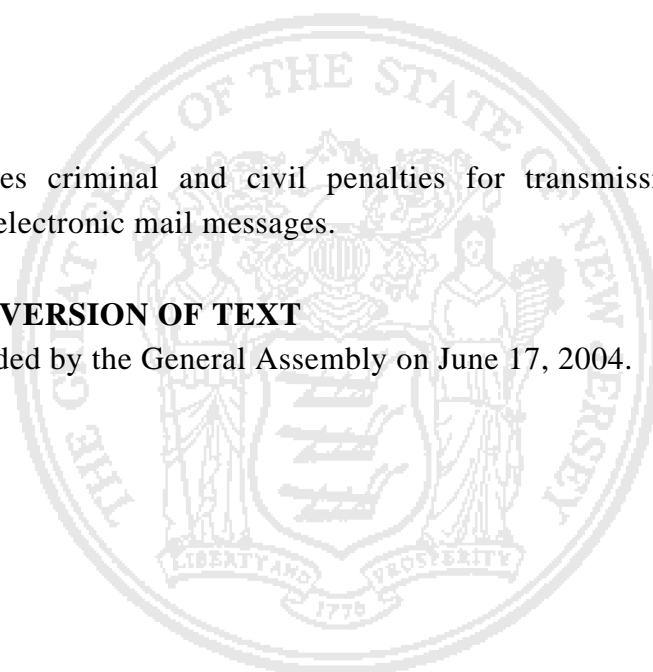
Assemblyman Baroni

SYNOPSIS

Establishes criminal and civil penalties for transmission of certain commercial electronic mail messages.

CURRENT VERSION OF TEXT

As amended by the General Assembly on June 17, 2004.



(Sponsorship Updated As Of: 6/25/2004)

1 AN ACT concerning the sending of certain ¹commercial¹ electronic
2 mail messages and supplementing chapter 20 of Title 2C of the
3 New Jersey Statutes.

4

5 **BE IT ENACTED** by the Senate and General Assembly of the State
6 of New Jersey:

7

8 1. This act shall be known and may be cited as the "New Jersey
9 ¹Can¹ Spam ¹**[Control]**¹ Act."

10

11 ¹[2. The Legislature finds and declares that:

12 a. Unsolicited commercial electronic mail messages, also referred
13 to as "spam," provide a means to reach large numbers of recipients at
14 very little cost to the sender;

15 b. Recent surveys have reported that almost two-thirds of the
16 billions of pieces of "spam" sent each week contain falsified e-mail
17 header or subject line information;

18 c. The transmission of billions of pieces of "spam" by high-volume
19 commercial senders, also referred to as "spammers," that are intended
20 to deceive or mislead recipients or to offend or invade the privacy of
21 recipients has grown into a costly problem for Internet Service
22 Providers (ISPs), businesses and consumers, reportedly costing
23 businesses and consumers \$10 billion per year;

24 d. "Spammers" increasingly rely on falsification and computer
25 hacking techniques to hide their commercial electronic mail messages
26 and get it through to consumers;

27 e. ISPs pay for the cost of the extra bandwidth, storage and
28 processing required to handle the high volume of "spam" from
29 commercial senders and ISPs and businesses pay for Internet filtering
30 software, which only partially blocks the receipt of "spam," and pay
31 their employees for sorting through the billions of pieces of "spam"
32 that get through Internet filters;

33 f. Consumers receiving "spam" not only pay increased costs
34 passed along by ISPs and businesses for handling or sorting through
35 "spam" but also spend large amounts of their own time deleting
36 "spam" on their personal home computers;

37 g. In response to the increasingly costly problems caused by
38 "spam" for businesses and consumers, over one half of the states have
39 enacted laws to impose a variety of penalties on the irresponsible use
40 of "spam;" in addition, the Federal Trade Commission has initiated
41 major administrative actions under existing consumer protection laws

EXPLANATION - Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and intended to be omitted in the law.

Matter underlined thus is new matter.

Matter enclosed in superscript numerals has been adopted as follows:

¹ Assembly floor amendments adopted June 17, 2004.

1 to prosecute "spammers" who engage in deceptive and fraudulent
2 practices; yet "spammers" are undeterred by and routinely flout these
3 federal and State civil enforcement mechanisms;

4 h. Criminal prohibitions would be an important new tool to
5 address the hacking and falsification techniques of these outlaw
6 "spammers;"

7 i. It is in the public interest for this State to enact its own law to
8 prohibit "spam" that is sent using falsification or hacking techniques
9 to reduce costs to businesses and consumers and to deter deceptive
10 and fraudulent practices by "spammers"; and

11 j. "Spam" that is sent using falsification or hacking techniques is
12 inherently deceptive and misleading and therefore falls outside of the
13 protections that the First Amendment ordinarily affords to commercial
14 speech.]¹

15

16 ¹2. The Legislature finds and declares that:

17 a. Unsolicited commercial electronic mail messages, also referred
18 to as "spam," provide a means to reach large numbers of recipients at
19 very little cost to the sender;

20 b. Recent surveys have reported that almost two-thirds of the
21 billions of pieces of "spam" sent each week contain falsified e-mail
22 headers or subject line information;

23 c. The transmission of billions of pieces of "spam" by high-volume
24 commercial senders, also referred to as "spammers," that are intended
25 to deceive or mislead recipients or to offend them or to invade their
26 privacy has grown into a costly problem for Internet service providers
27 (ISPs), businesses and consumers, reportedly costing businesses and
28 consumers \$10 billion per year;

29 d. "Spammers" increasingly rely on falsification and computer
30 hacking techniques to hide their commercial electronic mail messages
31 and get them through to consumers;

32 e. ISPs pay for the cost of the extra bandwidth, storage and
33 processing required to handle the high volume of "spam" from
34 commercial senders and ISPs and businesses pay for Internet filtering
35 software, which only partially blocks the receipt of "spam," and pay
36 their employees for sorting through the billions of pieces of "spam"
37 that get through Internet filters;

38 f. Consumers receiving "spam" not only pay increased costs
39 passed along by ISPs and businesses for handling or sorting through
40 "spam" but also spend large amounts of their own time deleting
41 "spam" on their personal home computers;

42 g. In response to the increasingly costly problems caused by
43 "spam" for businesses and consumers, over one half of the states have
44 enacted laws to impose a variety of penalties on the irresponsible use
45 of "spam;" in addition, the Federal Trade Commission has initiated
46 major administrative actions under existing consumer protection laws

1 to prosecute "spammers" who engage in deceptive and fraudulent
2 practices; yet "spammers" are undeterred by and routinely flout these
3 federal and state civil enforcement mechanisms;

4 h. Federal law now includes criminal prohibitions against the use
5 of falsified "spam" techniques and enactment of these prohibitions at
6 the State level would be an important new tool to address the hacking
7 and falsification techniques of these outlaw "spammers;"

8 i. It is in the public interest for this State to enact its own law to
9 prohibit "spam" that is sent using falsification or hacking techniques
10 in order to reduce costs to businesses and consumers and to deter
11 deceptive and fraudulent practices by "spammers"; and

12 j. "Spam" that is sent using falsification or hacking techniques is
13 inherently deceptive and misleading and therefore falls outside of the
14 protections that the First Amendment ordinarily affords to commercial
15 speech.¹

16
17 ¹[3. As used in this act:

18 "Act" means the "New Jersey Spam Control Act."

19 "Commercial electronic mail message" or "e-mail" means any
20 electronic mail message sent primarily for the purpose of commercial
21 advertisement, as defined in section 1 of P.L.1960, c.39 (C.56:8-1), or
22 promotion of a commercial product or service including, but not
23 limited to, the content on an Internet website or online site operated
24 for a commercial purpose.

25 "Computer" means an electronic, magnetic, optical,
26 electrochemical, or other high speed data processing device
27 performing logical, arithmetic, or storage functions, and includes any
28 data storage facility or communications facility directly related to or
29 operating in conjunction with such device, but such term does not
30 include an automated typewriter or typesetter, a portable hand held
31 calculator, or other similar device.

32 "Computer network" or "network" means any system or equipment
33 that provides communications between one or more computer systems
34 and input and output devices including, but not limited to, display
35 terminals and printers connected by telecommunication facilities and
36 shall include the Internet.

37 "Computer system" means a device or collection of devices,
38 including support devices and excluding calculators that are not
39 programmable and capable of being used in conjunction with external
40 files, one or more of which contain computer programs, electronic
41 instructions, input data and output data, that performs functions
42 including, but not limited to, logic, arithmetic, data storage and
43 retrieval, communication and control.

44 "Damage" means any impairment to the integrity or availability of
45 data, a program, a system or information, that causes loss aggregating
46 at least \$5,000 in value during any one-year period to one or more
47 individuals, causes physical injury to any person or threatens public
48 health or safety.

1 "Domain name" means any alphanumeric designation which is
2 registered with or assigned by any domain name registrar, domain
3 name registry, or other domain name registration authority, and that
4 is included in an electronic mail message.

5 "Felony" means any offense under any federal law or the law of this
6 State that is punishable by death or imprisonment for a term exceeding
7 one year. The term includes, but is not limited to, "crimes" as that
8 term is defined in N.J.S.2C:1-1 et seq.

9 "Financial institution" means a State or federally chartered bank,
10 savings bank or savings and loan association or any other financial
11 services company or provider including, but not limited to, broker-
12 dealers, investment companies, money market and mutual funds, credit
13 unions and insurers authorized to do business in this State.

14 "Header information" means the source, destination, routing
15 information, or information authenticating the sender, associated with
16 an electronic mail message including, but not limited to, the originating
17 domain name, originating electronic mail address, information
18 regarding any part of the route that an electronic mail message travels
19 or appears to travel on the Internet or on an online service, or other
20 authenticating information.

21 "Initiate the transmission" means to originate an electronic mail
22 message or to procure the origination of such message, regardless of
23 whether the message reaches its intended recipients, and does not
24 include the actions of an Internet service provider used by another
25 person for the transmission, routing, relaying, handling, or storing,
26 through an automatic technical process, of an electronic mail message
27 for which another person has provided and selected the recipient
28 electronic mail addresses.

29 "Internet" means the international computer network of both
30 federal and non-federal interoperable packet switched data networks.

31 "Internet protocol address" means the string of numbers by which
32 locations on the Internet are identified by routers or other computers
33 connected to the Internet.

34 "Internet service provider" means a service that enables users to
35 access content, information, electronic mail, or other services offered
36 over the Internet, and may also include access to proprietary content,
37 information, and other services as part of a package of services offered
38 to users. Such term does not include telecommunications services.

39 "Message" means each electronic mail message addressed to a
40 discrete addressee.

41 "Multiple" means more than 10 electronic mail messages during a
42 24-hour period, more than 100 electronic mail messages during a 30-
43 day period, or more than 1,000 electronic mail messages during a one-
44 year period.

45 "Protected computer" means a computer exclusively for the use of
46 State government or a financial institution or, in the case of a
47 computer not exclusively for such use, used by or for a financial

1 institution or State government and the conduct constituting the
2 offense affects that use by or for the financial institution or State
3 government; or a computer which is used in intrastate or interstate
4 communication.]¹

5
6 ¹3. As used in this act:

7 "Act" means the "New Jersey Can Spam Act."

8 "Commercial electronic mail message" or "commercial e-mail"
9 means any electronic mail message sent primarily for the purpose of
10 commercial advertisement, as advertisement is defined in section 1 of
11 P.L.1960, c.39 (C.56:8-1), or promotion of a commercial product or
12 service including, but not limited to, the content on an internet website
13 or online site operated for a commercial purpose.

14 "Computer" means an electronic, magnetic, optical,
15 electrochemical, or other high speed data processing device
16 performing logical, arithmetic, or storage functions, and includes any
17 data storage facility or communications facility directly related to or
18 operating in conjunction with such device, but such term does not
19 include an automated typewriter or typesetter, a portable hand held
20 calculator, or other similar device.

21 "Computer network" or "network" means any system or equipment
22 that provides communications between one or more computer systems
23 and input and output devices including, but not limited to, display
24 terminals and printers connected by telecommunication facilities and
25 shall include the internet.

26 "Computer system" means a device or collection of devices,
27 including support devices and excluding calculators that are not
28 programmable and capable of being used in conjunction with external
29 files, one or more of which contain computer programs, electronic
30 instructions, input data and output data, that performs functions
31 including, but not limited to, logic, arithmetic, data storage and
32 retrieval, communication and control.

33 "Domain name" means any alphanumeric designation that is
34 registered with or assigned by a domain name registrar, domain name
35 registry, or other domain name registration authority, as part of an
36 electronic mail address on the internet.

37 "Electronic mail service provider" means any person, including an
38 Internet service provider, that is an intermediary in sending and
39 receiving electronic mail and that provides to the public the ability to
40 send or receive electronic mail to or from an electronic mail account
41 or online user account.

42 "Felony" means any offense under any federal law or the law of this
43 State that is punishable by death or imprisonment for a term exceeding
44 one year. The term includes, but is not limited to, "crimes" as that
45 term is defined in N.J.S.2C:1-1 et seq.

46 "Header information" means the source, destination and routing
47 information attached to an electronic mail message, including the

1 originating domain name, originating electronic mail address and any
2 other information that appears in the line identifying or purporting to
3 identify a person initiating the message, and technical information that
4 authenticates the sender of an electronic mail message for network
5 security or network management services.

6 "Initiate" means, when used with respect to a commercial
7 electronic mail message, to originate or transmit the message or to
8 procure the origination or transmission of such message, and does not
9 include the actions that constitute routine conveyance of such
10 message.

11 "Internet" means the international computer network of both
12 federal and nonfederal interoperable packet switched data networks.

13 "Internet protocol address" means the string of numbers by which
14 location on the internet is identified by routers or other computers
15 connected to the internet.

16 "Loss" means any reasonable cost to any victim, including the cost
17 of responding to an offense, conducting a damage assessment, and
18 restoring the data, program or system, or information to its condition
19 prior to the offense, and any revenue lost, cost incurred, or other
20 consequential damages incurred because of interruption of service.

21 "Materially falsified" means altered or concealed in a manner that
22 would impair the ability of one of the following to identify, locate or
23 respond to a person who initiated an electronic mail message or to
24 investigate an alleged violation of this section:

25 (1) a recipient of the message;

26 (2) an Internet access service processing the message on behalf
27 of a recipient;

28 (3) a person alleging a violation of this section; or

29 (4) a law enforcement agency.

30 "Message" means each electronic mail message addressed to a
31 discrete addressee.

32 "Multiple" means more than 10 electronic mail messages during a
33 24-hour period, more than 100 electronic mail messages during a 30-
34 day period, or more than 1,000 electronic mail messages during a one-
35 year period.

36 "Procure" means intentionally to pay or provide other
37 consideration to another person to initiate the commercial e-mail, or
38 intentionally to induce another person to initiate the commercial e-mail
39 on the procurer's behalf.

40 "Protected computer" means a computer that is used in intrastate
41 or interstate communication.

42 "Routine conveyance" means the transmission, routing, relaying,
43 handling or storing through an automatic technical process, of an
44 electronic mail message for which another person has identified the
45 recipient or provided the recipient's address.¹

46

47 ¹[4. A person is guilty of a crime of the fourth degree if, with

1 regard to commercial electronic mail messages sent from or to the
2 facilities of an Internet service provider in this State, the person
3 knowingly:
4 a. uses a protected computer to relay or retransmit multiple
5 commercial electronic mail messages, with the intent to deceive or
6 mislead recipients, or any Internet service provider, as to the origin of
7 such messages;
8 b. falsifies header information in multiple commercial electronic
9 mail messages and intentionally initiates the transmission of such
10 messages;
11 c. registers, using information that falsifies the identity of the
12 actual registrant, for five or more electronic mail accounts or online
13 user accounts or two or more domain names, and intentionally initiates
14 the transmission of multiple commercial electronic mail messages from
15 any combination of such accounts or domain names; or
16 d. falsely represents the right to use five or more Internet protocol
17 addresses, and intentionally initiates the transmission of multiple
18 commercial electronic mail messages from such addresses; or
19 conspires to do so.]¹

20

21 ¹4. With regard to commercial electronic mail messages sent from
22 or to a protected computer in this State or that are sent using a
23 protected computer in this State, no person shall conspire to or
24 knowingly:

25 a. use a protected computer of another person to relay or
26 retransmit multiple commercial electronic mail messages with the
27 intent to deceive or mislead recipients or any electronic mail service
28 provider as to the origin of the messages;

29 b. materially falsify header information in multiple commercial
30 electronic mail messages and intentionally initiate the transmission of
31 the messages;

32 c. register, using information that materially falsifies the identity
33 of the actual registrant, for five or more electronic mail accounts or
34 on-line user accounts or two or more domain names, and intentionally
35 initiate the transmission of multiple commercial electronic mail
36 messages from one or more accounts or domain names or any
37 combination of accounts or domain names;

38 d. falsely represent the right to use five or more Internet protocol
39 addresses, and intentionally initiate the transmission of multiple
40 commercial electronic mail messages from the Internet protocol
41 addresses;

42 e. access a protected computer of another without authorization
43 and intentionally initiate the transmission of multiple commercial
44 electronic mail messages from or through the protected computer; or

45 f. violate the provisions of subsections a., b., c., d. or e. of this
46 section by providing or selecting addresses to which a message was
47 transmitted knowing that:

1 (1) the electronic mail addresses of the recipients were
2 obtained using an automated means from an Internet website or
3 proprietary online service operated by another person; and

4 (2) the website or online service included, at the time the
5 addresses were obtained, a notice stating that the operator of the
6 website or online service will not transfer addresses maintained by the
7 website or online service to any other party for the purposes of
8 initiating or enabling others to initiate electronic mail messages; or

9 g. violate the provisions of subsections a., b., c., d. or e. of this
10 section by providing or selecting electronic mail addresses of
11 recipients obtained using an automated means that generates possible
12 electronic mail addresses by combining names, letters or numbers into
13 numerous permutations.¹

14
15 ¹[5. A person who violates section 4 of this act is guilty of a crime
16 of the third degree if, with regard to commercial electronic mail
17 messages sent from or to the facilities of an Internet service provider
18 in this State:

19 a. the person knowingly registers, using information that falsifies
20 the identity of the actual registrant, for 20 or more electronic mail
21 accounts or online user accounts or 10 or more domain names, and
22 intentionally initiates the transmission of multiple commercial
23 electronic mail messages from such accounts or domain names; or
24 conspires to do so;

25 b. the volume of commercial electronic mail messages transmitted
26 in furtherance of an offence under subsections a. through d. of section
27 4 of this act exceeds 250 during any 24-hour period, 2,500 during any
28 30-day period, or 25,000 during any one-year period;

29 c. the person committing an offense under subsections a. through
30 d. of section 4 of this act causes loss to one or more persons
31 aggregating \$500 or more in value during any one-year period;

32 d. as a result of committing an offense under subsections a.
33 through d. of section 4 of this act, the person committing the offense
34 obtains anything of value aggregating \$500 or more during any one-
35 year period; or

36 e. an offense under subsections a. through d. of section 4 of this
37 act was undertaken by the defendant in concert with three or more
38 other persons with respect to whom the defendant occupied a position
39 of organizer or leader.]¹

40
41 ¹5. a. Except as otherwise provided in this section, a person who
42 violates the provisions of subsections a., b., c., d. or e. of section 4 of
43 this act is guilty of a crime of the fourth degree and may be fined not
44 more than \$1,000 or imprisoned for not more than one year, or both.

45 b. A person who violates the provisions of subsections a., b., c.,
46 d. or e. of section 4 of this act involving the transmission of more than
47 250 commercial electronic mail messages during any 24-hour period.

1 2,500 commercial electronic mail messages during any 30-day period,
2 or 25,000 commercial electronic mail messages during any one-year
3 period, is guilty of a crime of the third degree and may be fined not
4 more than \$10,000 or imprisoned not more than five years, or both.

5 c. A person who violates the provisions of subsections. c. or d. of
6 section 4 of this act involving 20 or more electronic mail accounts or
7 ten or more domain names and who intentionally initiates the
8 transmission of multiple commercial electronic mail messages from the
9 accounts or using the domain names is guilty of a crime of the third
10 degree and may be fined not more than \$10,000 or imprisoned not
11 more than five years, or both.

12 d. A person who violates the provisions of subsections a., b., c.,
13 d. or e. of section 4 of this act causing a loss of \$500 or more during
14 any one-year period is guilty of a crime of the third degree and may be
15 fined not more than \$10,000 or imprisoned not more than five years,
16 or both.

17 e. A person who violates the provisions of subsections a., b., c.,
18 d. or e. of section 4 of this act in concert with three or more other
19 persons as the organizer or leader of the action that constitutes the
20 violation of section 4 of this act is guilty of a crime of the third degree
21 and may be fined not more than \$10,000 or imprisoned not more than
22 five years, or both.

23 f. A person who violates the provisions of subsections a., b., c., d.
24 or e. of section 4 of this act in furtherance of a felony, or who has
25 previously been convicted of an offense under the laws of this State or
26 another state, or under any federal law, involving the transmission of
27 multiple commercial electronic mail messages is guilty of a crime of
28 the second degree and may be fined not more than \$25,000 or
29 imprisoned not more than 10 years, or both.

30 g. A person who violates the provisions of subsections f. or g. of
31 section 4 of this act is guilty of a crime of the fourth degree and may
32 be fined not more than \$5,000 or imprisoned not more than one year,
33 or both.¹

34
35 ¹[6. A person is guilty of a crime of the third degree if, with
36 regard to commercial electronic mail messages sent from or to the
37 facilities of an Internet service provider in this State, the person
38 knowingly accesses a protected computer without authorization, and
39 intentionally initiates the transmission of multiple commercial
40 electronic mail messages from or through such computer.]¹

41
42 ¹[7. A person who violates sections 4, 5 or 6 of this act in
43 furtherance of a felony, or who has previously been convicted of an
44 offense under the laws of this State or another state, or under any
45 federal law, involving transmission of multiple commercial electronic
46 mail messages or unauthorized access to a computer system, is guilty
47 of a crime of the second degree.]¹

1 ¹[8. a. The Attorney General, or any person engaged in the
2 business of an Internet service provider offering Internet service to the
3 public aggrieved by reason of a violation of sections 4, 5, 6 or 7 of this
4 act, may commence a civil action against the violator in any
5 appropriate court in this State for the relief set forth in subsections b.
6 and c. of this section. No action may be brought under this subsection
7 unless such action is begun within two years of the date of the act
8 which is the basis for the action.

9 b. In an action by the Attorney General under subsection a. of this
10 section, the court may award appropriate relief, including temporary,
11 preliminary, or permanent injunctive relief. The court may also assess
12 a civil penalty in an amount not exceeding \$25,000 per day of
13 violation, or not less than \$2 or more than \$8 per commercial
14 electronic mail message initiated in violation of sections 4, 5, 6 or 7 of
15 this act, as the court considers just.

16 c. In any other action under subsection a. of this section, the court
17 may award appropriate relief, including temporary, preliminary, or
18 permanent injunctive relief, and damages in an amount equal to the
19 greater of:

20 (1) the actual damages suffered by the Internet service provider as
21 a result of the violation, and any receipts of the violator that are
22 attributable to the violation and are not taken into account in
23 computing actual damages; or

24 (2) statutory damages in an amount not exceeding \$25,000 per
25 day of violation, or not less than \$2 or more than \$8 per commercial
26 electronic mail message initiated in violation of sections 4, 5, 6 or 7 of
27 this act, as the court considers just.]¹

28

29 ¹6. a. The Attorney General, or any person engaged in the
30 business of an electronic mail service provider offering electronic mail
31 service to the public aggrieved by reason of a violation of section 4 of
32 this act, may commence a civil action against the violator in the
33 Superior Court for the relief set forth in subsections b. and c. of this
34 section. No action may be brought under this subsection unless such
35 action is commenced within two years of the date of the act which is
36 the basis of the action.

37 b. In an action by the Attorney General under subsection a. of this
38 section, the court may award appropriate relief including temporary,
39 preliminary, or permanent injunctive relief. The court may also assess
40 a civil penalty in an amount not exceeding \$25,000 per day of
41 violation, or not less than two dollars or more than eight dollars per
42 commercial electronic mail message initiated in violation of section 4
43 of this act, as the court considers just.

44 c. In any civil action under subsection a. of this section, the court
45 may award appropriate relief, including temporary, preliminary, or
46 permanent injunctive relief, and damages in an amount equal to the
47 greater of:

1 (1) the actual damages suffered by an electronic mail service
2 provider as a result of the violation, and any monetary proceeds
3 received by the violator that are attributable to the violation and that
4 were not taken into account in computing actual damages; or

5 (2) statutory damages in an amount not exceeding \$25,000 per
6 day of violation, or not less than two dollars or more than eight dollars
7 per commercial electronic mail message initiated in violation of section
8 4 of this act, as the court considers just.¹

9
10 ¹[9.] 7.¹ A person who is convicted of an offense under
11 ¹[sections 4, 5, 6 or 7 of]¹ this act shall forfeit to the State:

12 ¹[(1)] a.¹ any property, real or personal, constituting or traceable
13 to gross proceeds obtained from ¹[such] the¹ offense; and

14 ¹[(2)] b.¹ any equipment, software, or other technology used or
15 intended to be used to commit or to facilitate the commission of
16 ¹[such] the¹ offense.

17
18 ¹[10.] 8.¹ This act shall take effect on the 120th day after
19 enactment.