Slam Spam

This Act creates a new crime of initiation of deceptive commercial e-mail. The Act directs that any person who initiates a commercial e-mail that the person knew or should have known to be false or misleading that is sent from, passes through, or is received by a protected computer shall be guilty of the crime of initiation of deceptive commercial e-mail. This Act seems to be directed at the practice of a company or person surreptitiously using another company's commercial computer server to send or forward fraudulent electronic mail.

Submitted as:
Georgia
SB 62 (Enrolled version)
Status: Enacted into law in 2005.

Suggested State Legislation

Section 1. [*Short Title*.] This Act may be cited as the "Slam Spam Act."

Section 2. [*Legislative Findings*.]

(1) The [legislature] finds and declares that electronic mail has become an important and popular means of communication, relied on by millions of people on a daily basis for personal and commercial purposes. The low cost and global reach of electronic mail make it convenient and efficient. Electronic mail serves as a catalyst for economic development and frictionless commerce.

(2) The [legislature] further finds that the convenience and efficiency of electronic mail is threatened by an ever-increasing glut of deceptive commercial electronic mail. The senders of these electronic messages engage in a variety of fraudulent and deceptive practices to hide their identities, to disguise the true source of their electronic mail, and to evade the criminal and civil consequences of their actions. Deceptive commercial electronic mail imposes costs upon its ultimate recipients who are forced to receive, review, and delete unwanted messages and upon the electronic mail service providers forced to carry the messages.

(3) The [legislature] further finds that our state has a paramount interest in protecting its businesses and citizens from the deleterious effects of deceptive commercial electronic mail, including the impermissible shifting of cost and economic burden that results from the false and fraudulent nature of deceptive commercial electronic mail. This state's enforcement of this interest imposes no additional burden upon the senders of such electronic mail in relation to the laws of any other state, in that such enforcement requires nothing more than the senders' forbearance from active deception.

Section 3. [*Definitions*.] As used in this Act:

(1) "Advertiser" means a person or entity that advertises through the use of commercial e-mail.

(2) "Automatic technical process" means the actions performed by an e-mail service provider's or telecommunications carrier's computers or computer network while acting as an intermediary between the sender and the recipient of an e-mail.

(3) "Commercial e-mail" means any e-mail message initiated for the purpose of advertising or promoting the lease, sale, rental, gift, offer, or other disposition of any property, services, or extension of credit.

(4) “Computer” means an electronic, magnetic, hydraulic, electrochemical, or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve, or communicate computer programs, computer data, or the results of computer operations to or from a person, another computer, or another device. This term specifically includes, but is not limited to, mail servers and e-mail networks. This term does not include a device that is not used to communicate with or to manipulate any other computer.

(5) “Computer network” means a set of related, remotely connected computers and any communications facilities with the function and purpose of transmitting data among them through the communications facilities.

(6) “Computer operation” means computing, classifying, transmitting, receiving, retrieving, originating, switching, storing, displaying, manifesting, measuring, detecting, recording, reproducing, handling, or utilizing any form of data for business, scientific, control, or other purposes.

(7) “Computer program” means one or more statements or instructions composed and structured in a form acceptable to a computer that, when executed by a computer in actual or modified form, cause the computer to perform one or more computer operations. The term 'computer program' shall include all associated procedures and documentation, whether or not such procedures and documentation are in human readable form.

(8) “Data” includes any representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network.

(9) “Direct consent” means that the recipient has expressly consented to receive e-mail advertisements from the advertiser or initiator, either in response to a clear and conspicuous request for direct consent or at the recipient's own initiative.

(10) “Domain” means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as Act of an electronic address on the Internet.

(11) “Domain owner” means, in relation to an e-mail address, the actual owner at the time an e-mail is received at that address of a domain that appears in or comprises a portion of the e-mail address. The registrant of a domain is presumed to be the actual owner of that domain.

(12) “Electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system that affects interstate or foreign commerce, but does not include:

(A) Any wire or oral communication;

(B) Any communication made through a tone-only paging device;

(C) Any communication from a tracking device; or

(D) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

(13) “Electronic communication service” means any service which provides to its users the ability to send or receive wire or electronic communications.

(14) “Electronic communications system” means any wire, radio, electromagnetic, photo-electronic, photo-optical, or facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

(15) ”Electronic means” is any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:

(A) Any telephone or telegraph instrument, equipment, or facility, or any component thereof,

(i) Furnished to the subscriber or user by a provider of electronic communication service in the ordinary course of its business and used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(ii) Used by a provider of electronic communication service in the ordinary course of its business or by an investigative or law enforcement officer in the ordinary course of his or her duties; or

(B) A hearing aid or similar device being used to correct subnormal hearing to better than normal.

(16) “E-mail” means an electronic message that is sent to an e-mail address and transmitted between two or more telecommunications devices, computers, or electronic devices capable of receiving electronic messages, whether or not the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval. The term includes electronic messages that are transmitted through a local, regional, or global computer network.

(17) “E-mail address” means a destination, commonly expressed as a string of characters, to which e-mail can be sent or delivered. An e-mail address consists of a user name or mailbox, the “@” symbol, and reference to a domain.

(18) “E-mail service provider” means any person, including an Internet service provider, that is an intermediary in sending or receiving e-mail or that provides to end-users of the e-mail service the ability to send or receive e-mail.

(19) “Electronic storage” means:

(A) Any temporary, intermediate storage of wire or electronic communication incidental to its electronic transmission; and

(B) Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

(20) “False or misleading,” when used in relation to a commercial e-mail, means that:

(A) The header information includes an originating or intermediate e-mail address, domain name, or Internet protocol address which was obtained by means of false or fraudulent pretenses or representations;

(B) The header information fails to accurately identify the computer used to initiate the e-mail;

(C) The subject line of the e-mail is intended to mislead a recipient about a material fact regarding the content or subject matter of the e-mail;

(D) The header information is altered or modified in a manner that impedes or precludes the recipient of the e-mail or an e-mail service provider from identifying, locating, or contacting the person who initiated the e-mail;

(E) The header information or content of the commercial e-mail, without authorization and with intent to mislead, references a personal name, entity name, trade name, mark, domain, address, phone number, or other personally identifying information belonging to a third party in such manner as would cause a recipient to believe that the third party authorized, endorsed, sponsored, sent, or was otherwise involved in the transmission of the commercial e-mail;

(F) The header information or content of the commercial e-mail contains false or fraudulent information regarding the identity, location, or means of contacting the initiator of the commercial e-mail; or

(G) The commercial e-mail falsely or erroneously states or represents that the transmission of the e-mail was authorized on the basis of:

(i) The recipient's prior direct consent to receive the commercial e-mail; or

(ii) A preexisting or current business relationship between the recipient and either the initiator or advertiser.

(21) "Financial instruments" includes any check, draft, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction-authorizing mechanism, or marketable security, or any computer representation thereof.

(22) "Header information" means those portions of an e-mail message which designate or otherwise identify:

(A) The sender;

(B) All recipients;

(C) An alternative return e-mail address, if any; and

(D) The names or Internet protocol addresses of the computers, systems, or other means used to send, transmit, rotate or receive the e-mail message. The term does not include either the subject line or the content of an e-mail message.

(23) "Incident" means the contemporaneous initiation in violation of this Act of one or more commercial e-mails containing substantially similar content.

(24) "Initiate" or "initiator" means to transmit or cause to be transmitted a commercial e-mail, but does not include the routine transmission of the commercial e-mail through the network or system of a telecommunications utility or an e-mail service provider.

(25) "Internet protocol address" means the unique numerical address assigned to and used to identify a specific computer or computer network that is directly connected to the Internet.

(26) "Law enforcement unit" means any law enforcement officer charged with the duty of enforcing the criminal laws and ordinances of the state or of the counties or municipalities of the state who is employed by and compensated by the state or any county or municipality of the state or who is elected and compensated on a fee basis. The term shall include, but not be limited to, members of the state [department of public safety, municipal police, county police, sheriffs, deputy sheriffs], and agents and investigators of the state [Bureau of Investigation].

(27) "Minor" means any person under the age of [18 years].

(28) "Person" means a person as defined by [insert citation] and specifically includes any limited liability company, trust, joint venture, or other legally cognizable entity.

(29) "Preexisting or current business relationship," as used in connection with the sending of a commercial e-mail, means that the recipient has made an inquiry and has provided his or her e-mail address, or has made an application, purchase, or transaction, with or without consideration, regarding products or services offered by the advertiser.

(30) "Protected computer" means any computer that, at the time of an alleged violation of any provision of this Act involving that computer, was located within the geographic boundaries of this state.

(31) "Property" includes computers, computer networks, computer programs, data, financial instruments, and services.

(32) "Recipient" means any addressee of a commercial e-mail advertisement. If an addressee of a commercial e-mail has one or more e-mail addresses to which a commercial e-mail is sent, the addressee shall be deemed to be a separate recipient for each e-mail address to which the e-mail is sent.

(33) "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

(34) "Routine transmission" means the forwarding, routing, relaying, handling, or storing of an e-mail message through an automatic technical process. The term shall not include the sending, or the knowing participation in the sending, of commercial e-mail advertisements.

(35) "Services" includes computer time or services or data processing services.

(36) "Use" includes causing or attempting to cause:

(A) A computer or computer network to perform or to stop performing computer operations;

(B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; or

(C) A person to put false information into a computer.

(37) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner to verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.

(38) "Without authority" includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network.

Section 4. [*Crime of Deceptive Commercial E-mail, Penalties and Venue*.]

(1) Any person who initiates a commercial e-mail that the person knew or should have known to be false or misleading that is sent from, passes through, or is received by a protected computer shall be guilty of the crime of initiation of deceptive commercial e-mail.

(2) Any person convicted of a violation of this Section shall be guilty of a [misdemeanor] and punished by a fine of not more than [$1,000] or by imprisonment of [not more than 12 months], or both, except:

(A) Where the volume of commercial e-mail transmitted exceeded [10,000 attempted recipients in any 24 hour period];

(B) Where the volume of commercial e-mail transmitted exceeded [100,000 attempted recipients in any 30 day period];

(C) Where the volume of commercial e-mail transmitted exceeded [one million attempted recipients in any one-year period];

(D) Where the revenue generated from a specific commercial e-mail exceeded]$1,000];

(E) Where the total revenue generated from all commercial e-mail transmitted to any e-mail service provider or its subscribers exceeded [$50,000]; or

(F) Where any person knowingly hires, employs, uses, or permits any minor to assist in the transmission of commercial e-mail in violation of this Act, the person shall be guilty of a [felony] and punished by a fine of not more than [$50,000] or by imprisonment of not more than [five years], or both.

(3) For the second conviction under this Section within a [five-year period], as measured from the dates of previous arrests for which convictions were obtained to the date of the current arrest for which a conviction is obtained, the person shall be guilty of a [felony] and punished by a fine of not more than [$50,000] or by imprisonment of not more than [five years], or both. For the purpose of this subsection, the term "conviction" shall include a plea of nolo contendere.

(4) For the purpose of venue under this Act, any violation of this Act shall be considered to have been committed:

(A) In the county of the principal place of business in this state of the owner of an involved protected computer, computer network, or part thereof;

(B) In any county in which any person alleged to have violated any provision of this Act had control or possession of any proceeds of the violation or of any books, records, documents, or property which were used in furtherance of the violation;

(C) In any county in which any act was performed in furtherance of any transaction which violated this Act; and

(D) In any county from which, to which, or through which any use of an involved protected computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.

(5) The [Attorney General] shall have concurrent jurisdiction with the [district attorneys and solicitors-general] to conduct the criminal prosecution of violations of this Act.

Section 5. [*Standing to Assert a Civil Action for Violations of this Act*.]

(1) The following people shall have standing to assert a civil action under this Act:

(A) Any e-mail service provider whose protected computer was used to send, receive, or transmit an e-mail that was sent in violation of this Act; and

(B) A domain owner of any e-mail address to which a deceptive commercial e-mail is sent in violation of this Act, provided that the domain owner also owns a protected computer at which the e-mail was received.

(2) Any person who has standing and who suffers personal, property, or economic damage by reason of a violation of any provision of this Act may initiate a civil action for and recover the greater of:

(A) [Five thousand dollars] plus expenses of litigation and reasonable attorney's fees;

(B) Liquidated damages of [$1,000] for each offending commercial e-mail, up to a limit of [$2 million] per incident, plus expenses of litigation and reasonable attorney's fees; or

(C) Actual damages, plus expenses of litigation and reasonable attorney's fees.

(3) Any crime committed in violation of this Act shall be considered a separate offense.

(4) The provisions of this Act shall not be construed as limiting or precluding the application of any other provision of law which applies to any transaction or course of conduct which violates this Act.

(5) Nothing in this Act shall be construed to limit or restrict the adoption, implementation, or enforcement by an e-mail service provider or Internet service provider of a policy of declining to transmit, receive, route, relay, handle, or store certain types of e-mail.

(6) There shall be no cause of action under this Act against an e-mail service provider on the basis of its routine transmission of any commercial e-mail over its computer network.

Section 6. [*Investigations about Violations of this Act*].

(1) In any investigation of a violation of this Act involving the use of a computer in furtherance of the Act, the [Attorney General] or any [district attorney] shall have the power to administer oaths; to call any party to testify under oath at such investigation; to require the attendance of witnesses and the production of books, records, and papers; and to take the depositions of witnesses.

(2) The [Attorney General] or any such [district attorney] is authorized to issue a subpoena for any witness or a subpoena to compel the production of any books, records, or papers.

(3) In case of refusal to obey a subpoena issued under this section to any person and upon application by the [Attorney General] or [district attorney], the [superior court] in whose jurisdiction the witness is to appear or in which the books, records, or papers are to be produced may issue to that person an order requiring him or her to appear before the court to show cause why he or she should not be held in contempt for refusal to obey the subpoena. Failure to obey a subpoena may be punished by the court as contempt of court.

(4) Any law enforcement unit, the [Attorney General], or any [district attorney] who is conducting an investigation of a violation of this Act involving the use of a computer in furtherance of the Act may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage in an electronic communications system for [180 days] or less pursuant to a search warrant issued under the provisions of [insert citation] by a court with jurisdiction over the offense under investigation. Such court may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than [180 days] as set forth in this Act.

(5) (A) Any law enforcement unit, the [Attorney General], or any [district attorney] may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service, exclusive of the contents of communications, only when any law enforcement unit, the [Attorney General], or any [district attorney]:

(i) Obtains a search warrant as provided in [insert citation]

(ii) Obtains a court order for such disclosure under this section; or

(iii) Has the consent of the subscriber or customer to such disclosure.

(6) A provider of electronic communication service or remote computing service shall disclose to any law enforcement unit, the [Attorney General], or any [district attorney] the:

(A) Name;

(B) Address;

(C) Local and long distance telephone connection records, or records of session times and durations;

(D) Length of service, including the start date, and types of service utilized;

(E) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) Means and source of payment for such service, including any credit card or bank account number of a subscriber to or customer of such service when any law enforcement unit, the [Attorney General], or any [district attorney] uses a subpoena authorized by this Act or a grand jury or trial subpoena when any law enforcement unit, the [Attorney General], or any [district attorney] complies with this Act.

(7) Any law enforcement unit, the [Attorney General], or any [district attorney] receiving records or information under this Act shall not be required to provide notice to a subscriber or customer. A provider of electronic communication service or remote computing service shall not disclose to a subscriber or customer the existence of any search warrant or subpoena issued pursuant to this Act nor shall a provider of electronic communication service or remote computing service disclose to a subscriber or customer that any records have been requested by or disclosed to any law enforcement unit, the [Attorney General], or any [district attorney] pursuant to this Act.

(8) A court order for disclosure issued pursuant to this Act may be issued by any [superior court] with jurisdiction over the offense under investigation and shall only issue such court order for disclosure if any law enforcement unit, the [Attorney General], or any [district attorney] offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of an electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. A court issuing an order pursuant to this Act, on a motion made promptly by a provider of electronic communication service or remote computing service, may quash or modify such order, if compliance with such order would be unduly burdensome or oppressive on such provider.

(9) (A) Any records supplied pursuant to this Act shall be accompanied by the affidavit of the custodian or other qualified witness, stating in substance each of the following:

(A) The affiant is the duly authorized custodian of the records or other qualified witness and has authority to certify the records;

(B) The copy is a true copy of all the records described in the subpoena, court order, or search warrant and the records were delivered to the attorney or the attorney's representative;

(C) The records were prepared by the personnel of the business in the ordinary course of business at or near the time of the act, condition, or event;

(D) The sources of information and method and time of preparation were such as to indicate its trustworthiness;

(E) The identity of the records; and

(F) A description of the mode of preparation of the records.

(10) If the business has none or only part of the records described, the custodian or other qualified witness shall so state in the affidavit.

(11) If the original records would be admissible in evidence if the custodian or other qualified witness had been present and testified to the matters stated in the affidavit, the copy of the records shall be admissible in evidence. When more than [one person] has knowledge of the facts, more than [one affidavit] shall be attached to the records produced.

(12) No later than [30 days] prior to trial, a party intending to offer such evidence produced in compliance with this subsection shall provide written notice of such intentions to the opposing party or parties. A motion opposing the admission of such evidence shall be filed within [ten days] of the filing of such notice, and the court shall hold a hearing and rule on such motion no later than [ten days] prior to trial. Failure of a party to file such motion opposing admission prior to trial shall constitute a waiver of objection to such records and affidavit. However, the court, for good cause shown, may grant relief from such waiver.

Section 7. [*Severability*.] [Insert severability clause.]

Section 8. [*Repealer*.] [Insert repealer clause.]

Section 9. [*Effective Date.*] [Insert effective date.]