

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

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

2

3 Section 2. [*Legislative Findings.*]

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

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

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

23

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

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

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

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

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

43 (5) "Computer network" means a set of related, remotely connected computers and any
44 communications facilities with the function and purpose of transmitting data among them 36
45 through the communications facilities.

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

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

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

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

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

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

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

- 71 (A) Any wire or oral communication;
- 72 (B) Any communication made through a tone-only paging device;
- 73 (C) Any communication from a tracking device; or
- 74 (D) Electronic funds transfer information stored by a financial institution in a
75 communications system used for the electronic storage and transfer of funds.

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

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

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

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

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

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

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

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

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

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

106 (19) "Electronic storage" means:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

142 (A) The sender;

143 (B) All recipients;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

195
196 Section 4. [*Crime of Deceptive Commercial E-mail, Penalties and Venue.*]

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

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

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

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

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

209 (D) Where the revenue generated from a specific commercial e-mail exceeded
210 [\$1,000];

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

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

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

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

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

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

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

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

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

236
237 Section 5. [*Standing to Assert a Civil Action for Violations of this Act.*]

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

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

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

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

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

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

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

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

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

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

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

261
262 Section 6. [*Investigations about Violations of this Act.*]

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

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

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

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

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

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

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

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

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

297 (A) Name;

298 (B) Address;

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

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

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

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

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

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

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

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

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

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

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

337 (E) The identity of the records; and

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

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

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

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

352

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

354

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

356

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