

Senate Bill 276

By: Senators Albers of the 56th, Beach of the 21st, Ligon, Jr. of the 3rd, Thompson of the 14th, McKoon of the 29th and others

A BILL TO BE ENTITLED
AN ACT

1 To amend Article 34 of Chapter 1 of Title 10 of the Official Code of Georgia Annotated,
2 relating to identity theft, so as to enact the "Georgia Personal Data Security Act"; to improve
3 systems and procedures for providing and regulating notifications of data breaches affecting
4 Georgia residents; to revise legislative findings and declarations; to modify definitions; to
5 modify when notices of certain security breaches are required and to provide for the contents
6 of such notices; to require certain entities to maintain certain data security procedures; to
7 require that certain notices of a data breach be sent to certain officials of this state; to provide
8 for enforcement by the Attorney General; to provide for civil penalties; to provide for
9 designations; to provide for related matters; to repeal conflicting laws; and for other
10 purposes.

11 BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

12 style="text-align:center">**SECTION 1.**

13 Article 34 of Chapter 1 of Title 10 of the Official Code of Georgia Annotated, relating to
14 identity theft, is amended by revising Code Sections 10-1-910 through 10-1-912 and
15 designating the same as Part 1 of said article and by adding new Code Sections 10-1-912.1
16 through 10-1-912.4 at the end of said part to read as follows:

17 style="text-align:center">"Part 1

18 10-1-910.

19 This part shall be known and may be cited as the 'Georgia Personal Data Security Act.'

20 10-1-910.1.

21 The General Assembly finds and declares as follows:

22 (1) The privacy and financial security of individuals is increasingly at risk due to the ever
 23 more widespread collection of personal information by both the private and public
 24 sectors;

25 (2) Credit card transactions, magazine subscriptions, real estate records, automobile
 26 registrations, consumer surveys, warranty registrations, credit reports, and Internet
 27 websites are all sources of personal information and form the source material for identity
 28 thieves;

29 (3) Identity theft is one of the fastest growing crimes committed in this state. Criminals
 30 who steal personal information such as social security numbers use the information to
 31 open credit card accounts, write bad checks, buy cars, purchase property, and commit
 32 other financial crimes with other people's identities;

33 (4) Implementation of technology security plans and security software as part of an
 34 information security policy may provide protection to consumers and the general public
 35 from identity thieves;

36 (5) Information brokers should clearly define the standards for authorized users of its
 37 data so that a breach by an unauthorized user is easily identifiable;

38 (6) Identity theft is costly to the marketplace and to consumers; and

39 (7) Victims of identity theft must act quickly to minimize the damage; therefore,
 40 expeditious notification of unauthorized acquisition and possible misuse of ~~a person's~~ an
 41 individual's personal information is imperative.

42 10-1-911.

43 As used in this ~~article~~ part, the term:

44 (1) 'Breach of the security of the system' means unauthorized acquisition of ~~an~~
 45 ~~individual's electronic~~ data that compromises the security, confidentiality, or integrity of
 46 personal information of ~~such an~~ an individual maintained by an information broker or data
 47 ~~collector~~ a covered entity. Good faith acquisition ~~or use~~ of personal information by an
 48 employee or agent of ~~an information broker or data collector for the purposes of such~~
 49 ~~information broker or data collector~~ a covered entity for a legitimate purpose of the
 50 covered entity is not a breach of the security of the system, provided that the personal
 51 information is not used for a purpose unrelated to the business or subject to further
 52 unauthorized disclosure.

53 (2) 'Covered entity' means a data collector, sole proprietorship, partnership, corporation,
 54 trust, estate, cooperative, association, or other commercial entity that acquires, maintains,
 55 stores, or uses personal information; provided, however, that an entity's status as public,
 56 private, for profit, or nonprofit shall not affect its designation as a covered entity.

57 ~~(2)~~(3) 'Data collector' means any state or local agency or subdivision thereof, including
 58 any department, bureau, authority, public university or college, academy, commission,
 59 or other government entity; ~~provided, however, that the term 'data collector' shall not~~
 60 ~~include any governmental agency whose records are maintained primarily for traffic~~
 61 ~~safety, law enforcement, or licensing purposes or for purposes of providing public access~~
 62 ~~to court records or to real or personal property information.~~

63 ~~(3) 'Information broker' means any person or entity who, for monetary fees or dues,~~
 64 ~~engages in whole or in part in the business of collecting, assembling, evaluating,~~
 65 ~~compiling, reporting, transmitting, transferring, or communicating information~~
 66 ~~concerning individuals for the primary purpose of furnishing personal information to~~
 67 ~~nonaffiliated third parties, but does not include any governmental agency whose records~~
 68 ~~are maintained primarily for traffic safety, law enforcement, or licensing purposes.~~

69 (4) 'Encrypted' means transformed as data through the use of an algorithmic process into
 70 a form in which there is a low probability of assigning meaning without use of a
 71 confidential process or key or secured by another method that renders the data unreadable
 72 or unusable.

73 ~~(4)~~(5) 'Notice' means:

74 (A) Written notice to an individual's mailing address listed in the records of the
 75 covered entity;

76 (B) Telephone notice;

77 (C) Electronic notice, if the notice provided is consistent with the provisions regarding
 78 electronic records and signatures set forth in Section 7001 of Title 15 of the United
 79 States Code; or

80 (D) Substitute notice, if the ~~information broker or data collector~~ covered entity
 81 demonstrates that the cost of providing notice would exceed ~~\$50,000.00~~ \$250,000.00,
 82 that the affected class of individuals to be notified exceeds ~~100,000~~ 500,000, or that the
 83 ~~information broker or data collector~~ covered entity does not have sufficient contact
 84 information to provide written or electronic notice to such individuals. Substitute
 85 notice shall consist of all of the following:

86 (i) E-mail notice, ~~if the information broker or data collector~~ to each individual for
 87 whom the covered entity has an e-mail address ~~for the individuals to be notified;~~

88 (ii) Conspicuous posting of the notice on the ~~information broker's or data collector's~~
 89 ~~covered entity's~~ website page, if the ~~information broker or data collector~~ covered
 90 entity maintains one; and

91 (iii) Notification to major state-wide media;

92 provided, however, that in cases involving personal information of a minor, notice shall
 93 be made to the minor's parents or legal guardian. ~~Notwithstanding any provision of this~~

94 ~~paragraph to the contrary, an information broker or data collector that maintains its own~~
 95 ~~notification procedures as part of an information security policy for the treatment of~~
 96 ~~personal information and is otherwise consistent with the timing requirements of this~~
 97 ~~article shall be deemed to be in compliance with the notification requirements of this~~
 98 ~~article if it notifies the individuals who are the subjects of the notice in accordance with~~
 99 ~~its policies in the event of a breach of the security of the system.~~

100 ~~(5) 'Person' means any individual, partnership, corporation, limited liability company,~~
 101 ~~trust, estate, cooperative, association, or other entity. The term 'person' as used in this~~
 102 ~~article shall not be construed to require duplicative reporting by any individual,~~
 103 ~~corporation, trust, estate, cooperative, association, or other entity involved in the same~~
 104 ~~transaction.~~

105 (6) 'Personal information' means an individual's first name or first initial and last name
 106 in combination with any one or more of the following data elements, when either the
 107 name or the data elements are not encrypted or redacted:

108 (A) ~~Social~~ A social security number that is not encrypted or redacted; or

109 (B) An individual's first and last name or first initial and last name in combination with
 110 one or more of the following data elements that are not encrypted or redacted:

111 ~~(B)~~(i) Driver's license number, or state identification card number, passport number,
 112 military identification number, or other similar number issued on a government
 113 document used to verify identity;

114 ~~(C)~~(ii) Account number, credit card number, or debit card number, if circumstances
 115 exist wherein such a number could be used without additional identifying information,
 116 access codes, or passwords;

117 ~~(D)~~(iii) Account passwords or personal identification numbers or other access codes;
 118 or

119 (iv) Student information, including grades, disciplinary history, and standardized test
 120 scores;

121 (v) Information related to medical treatment, diagnosis, or history;

122 (vi) An individual's health insurance policy number or subscriber identification
 123 number and any unique identifier used by a health insurer to identify the individual;
 124 or

125 ~~(E)~~(vii) Any of the items contained in subparagraphs (A) through (D) of this
 126 paragraph divisions (i) through (vi) of this subparagraph when not in connection with
 127 the individual's first and last name or first initial and last name, if the information
 128 compromised would be sufficient to perform or attempt to perform identity theft
 129 against the person individual whose information was compromised.

130 The term 'personal information' does not include publicly available information that is
131 lawfully made available to the general public from federal, state, or local government
132 records.

133 (7) 'Redacted' means rendered as data to be unreadable or truncated so that no more than
134 the last four digits of an identification number are accessible as part of the data.

135 (8) 'Third-party agent' means an individual or entity that has been contracted to maintain,
136 store, or process personal information for or on behalf of a covered entity.

137 10-1-912.

138 ~~(a) Any information broker or data collector that maintains computerized data that includes~~
139 ~~personal information of individuals shall give notice of any breach of the security of the~~
140 ~~system following discovery or notification of the breach in the security of the data to any~~
141 ~~resident of this state whose unencrypted personal information was, or is reasonably~~
142 ~~believed to have been, acquired by an unauthorized person. The notice shall be made in~~
143 ~~the most expedient time possible and without unreasonable delay, consistent with the~~
144 ~~legitimate needs of law enforcement, as provided in subsection (c) of this Code section, or~~
145 ~~with any measures necessary to determine the scope of the breach and restore the~~
146 ~~reasonable integrity, security, and confidentiality of the data system. A covered entity that~~
147 maintains physical or computerized data that include personal information of individuals
148 shall give notice of a breach of the security of the system to any resident of this state whose
149 personal information was, or is reasonably believed to have been, accessed as a result of
150 such breach. Such notice shall be made as expeditiously as practicable and without
151 unreasonable delay, taking into account the time necessary to allow the covered entity to
152 determine the scope of such breach, to identify individuals affected by such breach, and to
153 restore the reasonable integrity of the data system that was breached, but no later than 45
154 days after the determination of such breach or reason to believe such breach occurred,
155 unless subject to a delay authorized under subsection (c) of this Code section.

156 ~~(b) Any person or business that maintains computerized data on behalf of an information~~
157 ~~broker or data collector that includes personal information of individuals that the person~~
158 ~~or business does not own shall notify the information broker or data collector of any breach~~
159 ~~of the security of the system within 24 hours following discovery, if the personal~~
160 ~~information was, or is reasonably believed to have been, acquired by an unauthorized~~
161 ~~person. In the event of a breach of the security of the system, which system is maintained~~
162 by a third-party agent for a covered entity, the third-party agent shall notify the covered
163 entity of such breach as expeditiously as practicable but no later than 72 hours after the
164 determination of such breach or reason to believe such breach has occurred. The
165 third-party agent shall provide the covered entity with all information that the covered

166 entity needs to comply with its notice requirements under this Code section and Code
 167 Section 10-1-912.2.

168 (c) The notification required by this Code section may be delayed if a law enforcement
 169 agency determines that the notification will compromise a criminal investigation. The
 170 notification required by this Code section shall be made after the law enforcement agency
 171 determines that it will not compromise the investigation.

172 (d)(1) Notwithstanding any provision of this part to the contrary, a covered entity that
 173 maintains its own notification procedures as part of an information security policy for the
 174 treatment of personal information shall be deemed to be in compliance with the
 175 notification requirements of this part if such covered entity notifies the individuals who
 176 are the subjects of the notice in accordance with its policies in the event of a breach of the
 177 security of the system.

178 (2) A covered entity that is regulated pursuant to a state or federal law and that maintains
 179 and follows procedures for a breach of the security of the system pursuant to the laws,
 180 rules, regulations, guidance, or guidelines established by a state or federal regulator is
 181 deemed to be in compliance with this part.

182 (3) Notwithstanding subsection (a) of this Code section, notice to individuals whose
 183 personal information has been accessed is not required if, after an appropriate
 184 investigation and consultation with relevant federal, state, or local law enforcement
 185 agencies, the covered entity reasonably determines that a breach of the security of the
 186 system has not and will not likely result in identity theft or any other financial harm to
 187 such individuals. Such a determination must be documented in writing and maintained
 188 for at least five years. The covered entity shall provide the written determination to the
 189 Attorney General within 30 days after the determination not to notify has been made.

190 ~~(d)~~(4) In the event that an information broker or data collector a covered entity discovers
 191 circumstances requiring notification pursuant to this Code section of more than 10,000
 192 1,000 residents of this state at one time, the information broker or data collector covered
 193 entity shall also notify, without unreasonable delay, all consumer reporting agencies that
 194 compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C.
 195 Section 1681a, of the timing, distribution, and content of the notices.

196 10-1-912.1.

197 Each notice to an individual shall be titled 'Notice of Data Breach' and shall include the
 198 following:

199 (1) The date, estimated date, or estimated date range of the breach of the security of the
 200 system, if such information is possible to determine at the time the notice is provided;

- 201 (2) How data were accessed, if such information is possible to determine at the time the
 202 notice is provided;
 203 (3) What data were or are reasonably believed to have been accessed;
 204 (4) What potential harm may arise;
 205 (5) Ways in which the individual may seek to reduce or eliminate harm;
 206 (6) A telephone number where the individual may obtain additional information related
 207 to such breach; and
 208 (7) The toll-free telephone numbers and addresses of the major credit reporting agencies.

209 10-1-912.2.

210 (a) For any breach of the security of the system for which notice to an individual is
 211 required under this part, a covered entity shall provide written notice to the Attorney
 212 General and the Governor that shall include:

- 213 (1) A copy of each notice to an individual required under this part;
 214 (2) The number of individuals who are residents of this state and were or potentially have
 215 been affected by such breach;
 216 (3) Any services related to such breach being offered or scheduled to be offered, without
 217 charge, by the covered entity to individuals; and
 218 (4) The name, address, telephone number, and e-mail address of the employee or agent
 219 of the covered entity from whom additional information may be obtained about such
 220 breach.

221 (b) As provided for under subsection (a) of this Code section, a covered entity shall, upon
 222 request, provide the following information to the Attorney General or Governor:

- 223 (1) A police report, incident report, or computer forensics report;
 224 (2) A copy of the policies in place regarding a breach of the security of the system; and
 225 (3) Steps that have been taken to remedy the breach of the security of the system.

226 10-1-912.3.

227 Each covered entity shall maintain reasonable safeguards to protect and secure personal
 228 information.

229 10-1-912.4.

- 230 (a) The Attorney General shall be authorized to enforce the provisions of this part.
 231 (b) The Attorney General shall have the authority to investigate alleged violations of this
 232 part, including all investigative powers available under Part 2 of Article 15 of this chapter,
 233 the 'Fair Business Practices Act of 1975,' including, but not limited to, the power to issue
 234 investigative demands and subpoenas as provided in Code Sections 10-1-403 and 10-1-404.

- 235 (c) If the Attorney General determines, after notice and hearing, that a covered entity has
236 violated this part, the Attorney General may take any or all of the following actions:
- 237 (1) Issue an administrative order imposing a civil penalty not to exceed \$500.00 for each
238 resident of this state who did not receive the required notice, provided that the total civil
239 penalty shall not exceed \$250,000.00 per each breach of the security of the system;
- 240 (2) Issue an order compelling the covered entity to provide any notice required under this
241 part; or
- 242 (3) Issue an order providing for the recovery of the Attorney General's reasonable costs
243 in maintaining the action.
- 244 (d) Any hearing and administrative review in connection with alleged violations of this
245 part shall be conducted in accordance with the procedure for contested cases pursuant to
246 Chapter 13 of Title 50, the 'Georgia Administrative Procedure Act.' Any covered entity
247 that has exhausted all administrative remedies available and is aggrieved or adversely
248 affected by a final order or action of the Attorney General shall have the right of judicial
249 review in accordance with such chapter.
- 250 (e) The Attorney General may file in the superior court of the county in which the covered
251 entity maintains its principal place of business a certified copy of or the final order of the
252 Attorney General, whether or not the order was appealed. Thereafter, the court shall render
253 a judgment in accordance with the order and notify the parties. The judgment shall have
254 the same effect as a judgment rendered by the court.
- 255 (f) Without regard as to whether the Attorney General has issued any orders under this
256 Code section, upon a showing by the Attorney General in any superior court of competent
257 jurisdiction that a covered entity has violated or is about to violate this part, a rule
258 promulgated under this part, or an order of the Attorney General, the court may enter or
259 grant any or all of the following relief:
- 260 (1) A civil penalty not to exceed \$500.00 for each resident of this state who did not
261 receive the required notice, provided that the total civil penalty shall not exceed
262 \$250,000.00 per each breach of the security of the system;
- 263 (2) An order compelling the covered entity to provide any notice required under this part;
- 264 (3) An order providing for the recovery of the Attorney General's reasonable costs in
265 maintaining the action; and
- 266 (4) Other relief the court deems just and reasonable.
- 267 (g) Except as otherwise expressly provided in this Code section, nothing in this Code
268 section shall be construed to restrict or expand any other authority or jurisdiction of the
269 Attorney General.
- 270 (h) Nothing in this part either creates a private right of action or affects any private right
271 of action existing under other law, including, but not limited to, under contract or tort.

272 (i) No provision of this part shall constitute a waiver of sovereign immunity.

273 (j) The provisions of this part are not exclusive and do not relieve a covered entity from
274 compliance with all other applicable provisions of law."

275 **SECTION 2.**

276 Said article is further amended by designating Code Sections 10-1-913 through 10-1-915 as
277 Part 2 of said article.

278 **SECTION 3.**

279 All laws and parts of laws in conflict with this Act are repealed.