

20141524e1

1 A bill to be entitled
2 An act relating to security of confidential personal
3 information; providing a short title; repealing s.
4 817.5681, F.S., relating to a breach of security
5 concerning confidential personal information in third-
6 party possession; creating s. 501.171, F.S.; providing
7 definitions; requiring specified entities to take
8 reasonable measures to protect and secure data
9 containing personal information in electronic form;
10 requiring specified entities to notify the Department
11 of Legal Affairs of data security breaches; requiring
12 notice to individuals of data security breaches under
13 certain circumstances; providing exceptions to notice
14 requirements under certain circumstances; specifying
15 contents and methods of notice; requiring notice to
16 credit reporting agencies under certain circumstances;
17 requiring the department to report annually to the
18 Legislature; specifying report requirements; providing
19 requirements for disposal of customer records;
20 providing for enforcement actions by the department;
21 providing civil penalties; specifying that no private
22 cause of action is created; amending ss. 282.0041 and
23 282.318, F.S.; conforming cross-references to changes
24 made by the act; providing an effective date.

25
26 Be It Enacted by the Legislature of the State of Florida:

27
28 Section 1. This act may be cited as the "Florida
29 Information Protection Act of 2014."

20141524e1

30 Section 2. Section 817.5681, Florida Statutes, is repealed.

31 Section 3. Section 501.171, Florida Statutes, is created to
32 read:

33 501.171 Security of confidential personal information.—

34 (1) DEFINITIONS.—As used in this section, the term:

35 (a) "Breach of security" or "breach" means unauthorized
36 access of data in electronic form containing personal
37 information. Good faith access of personal information by an
38 employee or agent of the covered entity does not constitute a
39 breach of security, provided that the information is not used
40 for a purpose unrelated to the business or subject to further
41 unauthorized use.

42 (b) "Covered entity" means a sole proprietorship,
43 partnership, corporation, trust, estate, cooperative,
44 association, or other commercial entity that acquires,
45 maintains, stores, or uses personal information. For purposes of
46 the notice requirements in subsections (3)-(6), the term
47 includes a governmental entity.

48 (c) "Customer records" means any material, regardless of
49 the physical form, on which personal information is recorded or
50 preserved by any means, including, but not limited to, written
51 or spoken words, graphically depicted, printed, or
52 electromagnetically transmitted that are provided by an
53 individual in this state to a covered entity for the purpose of
54 purchasing or leasing a product or obtaining a service.

55 (d) "Data in electronic form" means any data stored
56 electronically or digitally on any computer system or other
57 database and includes recordable tapes and other mass storage
58 devices.

20141524e1

59 (e) "Department" means the Department of Legal Affairs.

60 (f) "Governmental entity" means any department, division,
61 bureau, commission, regional planning agency, board, district,
62 authority, agency, or other instrumentality of this state that
63 acquires, maintains, stores, or uses data in electronic form
64 containing personal information.

65 (g)1. "Personal information" means either of the following:

66 a. An individual's first name or first initial and last
67 name in combination with any one or more of the following data
68 elements for that individual:

69 (I) A social security number;

70 (II) A driver license or identification card number,
71 passport number, military identification number, or other
72 similar number issued on a government document used to verify
73 identity;

74 (III) A financial account number or credit or debit card
75 number, in combination with any required security code, access
76 code, or password that is necessary to permit access to an
77 individual's financial account;

78 (IV) Any information regarding an individual's medical
79 history, mental or physical condition, or medical treatment or
80 diagnosis by a health care professional; or

81 (V) An individual's health insurance policy number or
82 subscriber identification number and any unique identifier used
83 by a health insurer to identify the individual.

84 b. A user name or e-mail address, in combination with a
85 password or security question and answer that would permit
86 access to an online account.

87 2. The term does not include information about an

20141524e1

88 individual that has been made publicly available by a federal,
89 state, or local governmental entity. The term also does not
90 include information that is encrypted, secured, or modified by
91 any other method or technology that removes elements that
92 personally identify an individual or that otherwise renders the
93 information unusable.

94 (h) "Third-party agent" means an entity that has been
95 contracted to maintain, store, or process personal information
96 on behalf of a covered entity or governmental entity.

97 (2) REQUIREMENTS FOR DATA SECURITY.—Each covered entity,
98 governmental entity, or third-party agent shall take reasonable
99 measures to protect and secure data in electronic form
100 containing personal information.

101 (3) NOTICE TO DEPARTMENT OF SECURITY BREACH.—

102 (a) A covered entity shall provide notice to the department
103 of any breach of security affecting 500 or more individuals in
104 this state. Such notice must be provided to the department as
105 expeditiously as practicable, but no later than 30 days after
106 the determination of the breach or reason to believe a breach
107 occurred. A covered entity may receive 15 additional days to
108 provide notice as required in subsection (4) if good cause for
109 delay is provided in writing to the department within 30 days
110 after determination of the breach or reason to believe a breach
111 occurred.

112 (b) The written notice to the department must include:

113 1. A synopsis of the events surrounding the breach at the
114 time notice is provided.

115 2. The number of individuals in this state who were or
116 potentially have been affected by the breach.

20141524e1

117 3. Any services related to the breach being offered or
118 scheduled to be offered, without charge, by the covered entity
119 to individuals, and instructions as to how to use such services.

120 4. A copy of the notice required under subsection (4) or an
121 explanation of the other actions taken pursuant to subsection
122 (4).

123 5. The name, address, telephone number, and e-mail address
124 of the employee or agent of the covered entity from whom
125 additional information may be obtained about the breach.

126 (c) The covered entity must provide the following
127 information to the department upon its request:

128 1. A police report, incident report, or computer forensics
129 report.

130 2. A copy of the policies in place regarding breaches.

131 3. Steps that have been taken to rectify the breach.

132 (d) A covered entity may provide the department with
133 supplemental information regarding a breach at any time.

134 (e) For a covered entity that is the judicial branch, the
135 Executive Office of the Governor, the Department of Financial
136 Services, or the Department of Agriculture and Consumer
137 Services, in lieu of providing the written notice to the
138 department, the covered entity may post the information
139 described in subparagraphs (b)1.-4. on an agency-managed
140 website.

141 (4) NOTICE TO INDIVIDUALS OF SECURITY BREACH.—

142 (a) A covered entity shall give notice to each individual
143 in this state whose personal information was, or the covered
144 entity reasonably believes to have been, accessed as a result of
145 the breach. Notice to individuals shall be made as expeditiously

20141524e1

146 as practicable and without unreasonable delay, taking into
147 account the time necessary to allow the covered entity to
148 determine the scope of the breach of security, to identify
149 individuals affected by the breach, and to restore the
150 reasonable integrity of the data system that was breached, but
151 no later than 30 days after the determination of a breach or
152 reason to believe a breach occurred unless subject to a delay
153 authorized under paragraph (b) or waiver under paragraph (c).

154 (b) If a federal, state, or local law enforcement agency
155 determines that notice to individuals required under this
156 subsection would interfere with a criminal investigation, the
157 notice shall be delayed upon the written request of the law
158 enforcement agency for a specified period that the law
159 enforcement agency determines is reasonably necessary. A law
160 enforcement agency may, by a subsequent written request, revoke
161 such delay as of a specified date or extend the period set forth
162 in the original request made under this paragraph to a specified
163 date if further delay is necessary.

164 (c) Notwithstanding paragraph (a), notice to the affected
165 individuals is not required if, after an appropriate
166 investigation and consultation with relevant federal, state, or
167 local law enforcement agencies, the covered entity reasonably
168 determines that the breach has not and will not likely result in
169 identity theft or any other financial harm to the individuals
170 whose personal information has been accessed. Such a
171 determination must be documented in writing and maintained for
172 at least 5 years. The covered entity shall provide the written
173 determination to the department within 30 days after the
174 determination.

20141524e1

175 (d) The notice to an affected individual shall be by one of
176 the following methods:

177 1. Written notice sent to the mailing address of the
178 individual in the records of the covered entity; or

179 2. E-mail notice sent to the e-mail address of the
180 individual in the records of the covered entity.

181 (e) The notice to an individual with respect to a breach of
182 security shall include, at a minimum:

183 1. The date, estimated date, or estimated date range of the
184 breach of security.

185 2. A description of the personal information that was
186 accessed or reasonably believed to have been accessed as a part
187 of the breach of security.

188 3. Information that the individual can use to contact the
189 covered entity to inquire about the breach of security and the
190 personal information that the covered entity maintained about
191 the individual.

192 (f) A covered entity required to provide notice to an
193 individual may provide substitute notice in lieu of direct
194 notice if such direct notice is not feasible because the cost of
195 providing notice would exceed \$250,000, because the affected
196 individuals exceed 500,000 persons, or because the covered
197 entity does not have an e-mail address or mailing address for
198 the affected individuals. Such substitute notice shall include
199 the following:

200 1. A conspicuous notice on the Internet website of the
201 covered entity if the covered entity maintains a website; and

202 2. Notice in print and to broadcast media, including major
203 media in urban and rural areas where the affected individuals

20141524e1

204 reside.

205 (g) Notice provided pursuant to rules, regulations,
206 procedures, or guidelines established by the covered entity's
207 primary or functional federal regulator is deemed to be in
208 compliance with the notice requirement in this subsection if the
209 covered entity notifies affected individuals in accordance with
210 the rules, regulations, procedures, or guidelines established by
211 the primary or functional federal regulator in the event of a
212 breach of security. Under this paragraph, a covered entity that
213 timely provides a copy of such notice to the department is
214 deemed to be in compliance with the notice requirement in
215 subsection (3).

216 (5) NOTICE TO CREDIT REPORTING AGENCIES.—If a covered
217 entity discovers circumstances requiring notice pursuant to this
218 section of more than 1,000 individuals at a single time, the
219 covered entity shall also notify, without unreasonable delay,
220 all consumer reporting agencies that compile and maintain files
221 on consumers on a nationwide basis, as defined in the Fair
222 Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing,
223 distribution, and content of the notices.

224 (6) NOTICE BY THIRD-PARTY AGENTS; DUTIES OF THIRD-PARTY
225 AGENTS; NOTICE BY AGENTS.—

226 (a) In the event of a breach of security of a system
227 maintained by a third-party agent, such third-party agent shall
228 notify the covered entity of the breach of security as
229 expeditiously as practicable, but no later than 10 days
230 following the determination of the breach of security or reason
231 to believe the breach occurred. Upon receiving notice from a
232 third-party agent, a covered entity shall provide notices

20141524e1

233 required under subsections (3) and (4). A third-party agent
234 shall provide a covered entity with all information that the
235 covered entity needs to comply with its notice requirements.

236 (b) An agent may provide notice as required under
237 subsections (3) and (4) on behalf of the covered entity;
238 however, an agent's failure to provide proper notice shall be
239 deemed a violation of this section against the covered entity.

240 (7) ANNUAL REPORT.—By February 1 of each year, the
241 department shall submit a report to the President of the Senate
242 and the Speaker of the House of Representatives describing the
243 nature of any reported breaches of security by governmental
244 entities or third-party agents of governmental entities in the
245 preceding calendar year along with recommendations for security
246 improvements. The report shall identify any governmental entity
247 that has violated any of the applicable requirements in
248 subsections (2)-(6) in the preceding calendar year.

249 (8) REQUIREMENTS FOR DISPOSAL OF CUSTOMER RECORDS.—Each
250 covered entity or third-party agent shall take all reasonable
251 measures to dispose, or arrange for the disposal, of customer
252 records containing personal information within its custody or
253 control when the records are no longer to be retained. Such
254 disposal shall involve shredding, erasing, or otherwise
255 modifying the personal information in the records to make it
256 unreadable or undecipherable through any means.

257 (9) ENFORCEMENT.—

258 (a) A violation of this section shall be treated as an
259 unfair or deceptive trade practice in any action brought by the
260 department under s. 501.207 against a covered entity or third-
261 party agent.

20141524e1

262 (b) In addition to the remedies provided for in paragraph
263 (a), a covered entity that violates subsection (3) or subsection
264 (4) shall be liable for a civil penalty not to exceed \$500,000,
265 as follows:

266 1. In the amount of \$1,000 for each day up to the first 30
267 days following any violation of subsection (3) or subsection (4)
268 and, thereafter, \$50,000 for each subsequent 30-day period or
269 portion thereof for up to 180 days.

270 2. If the violation continues for more than 180 days, in an
271 amount not to exceed \$500,000.

272
273 The civil penalties for failure to notify provided in this
274 paragraph apply per breach and not per individual affected by
275 the breach.

276 (c) All penalties collected pursuant to this subsection
277 shall be deposited into the General Revenue Fund.

278 (10) NO PRIVATE CAUSE OF ACTION.—This section does not
279 establish a private cause of action.

280 Section 4. Subsection (5) of section 282.0041, Florida
281 Statutes, is amended to read:

282 282.0041 Definitions.—As used in this chapter, the term:

283 (5) "Breach" has the same meaning as the term "breach of
284 security" as defined in s. 501.171 in s. ~~817.5681(4)~~.

285 Section 5. Paragraph (i) of subsection (4) of section
286 282.318, Florida Statutes, is amended to read:

287 282.318 Enterprise security of data and information
288 technology.—

289 (4) To assist the Agency for Enterprise Information
290 Technology in carrying out its responsibilities, each agency

20141524e1

291 head shall, at a minimum:

292 (i) Develop a process for detecting, reporting, and
293 responding to suspected or confirmed security incidents,
294 including suspected or confirmed breaches consistent with the
295 security rules and guidelines established by the Agency for
296 Enterprise Information Technology.

297 1. Suspected or confirmed information security incidents
298 and breaches must be immediately reported to the Agency for
299 Enterprise Information Technology.

300 2. For incidents involving breaches, agencies shall provide
301 notice in accordance with s. 501.171 ~~s. 817.5681~~ and to the
302 Agency for Enterprise Information Technology in accordance with
303 this subsection.

304 Section 6. This act shall take effect July 1, 2014.