By the Committee on Commerce and Tourism; and Senator Thrasher

577-03111-14 20141524c1

A bill to be entitled

An act relating to security of confidential personal information; providing a short title; repealing s. 817.5681, F.S., relating to a breach of security concerning confidential personal information in third-party possession; creating s. 501.171, F.S.; providing definitions; requiring specified entities to take reasonable measures to protect and secure data containing personal information in electronic form; requiring specified entities to notify the Department of Legal Affairs of data security breaches; requiring notice to individuals of data security breaches under certain circumstances; providing exceptions to notice requirements under certain circumstances; specifying contents and methods of notice; requiring notice to credit reporting agencies under certain circumstances; requiring the department to report annually to the Legislature; specifying report requirements; providing requirements for disposal of customer records; providing for enforcement actions by the department; providing civil penalties; specifying that no private cause of action is created; amending ss. 282.0041 and 282.318, F.S.; conforming cross-references to changes made by the act; providing an effective date.

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

Section 1. <u>This act may be cited as the "Florida Information Protection Act of 2014."</u>

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 Section 817.5681, Florida Statutes, is repealed.

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

501.171 Security of confidential personal information.—

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

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

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

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

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

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

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

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

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

(I) A social security number.

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

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

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

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

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

2. The term does not include information about an

individual that has been made publicly available by a federal, state, or local governmental entity or information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

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

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

(3) NOTICE TO DEPARTMENT OF SECURITY BREACH.—

(a) A covered entity shall give notice to the department of any breach of security, as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach had occurred.

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

1. A synopsis of the events surrounding the breach.

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

3. Any services related to the breach being offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.

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

5. The name, address, telephone number, and e-mail address of the employee of the covered entity from whom additional

information may be obtained about the breach, and the steps taken to rectify the breach and prevent similar breaches.

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

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

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

3. Any steps that have been taken to rectify the breach.

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

(4) NOTICE TO INDIVIDUALS OF SECURITY BREACH.—

(a) A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c).

(b) If a federal, state, or local law enforcement agency

determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.

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

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

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

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

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

1. The date, estimated date, or estimated date range of the

breach of security.

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

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

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

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

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

(g) Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies individuals in accordance with any rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Under this paragraph, the covered entity must

provide notice to the department under subsection (3).

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

(6) NOTICE BY THIRD-PARTY AGENTS; DUTIES OF THIRD-PARTY AGENTS.—In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security. Upon receiving notice from a third-party agent, a covered entity shall provide notices required under subsections (3) and (4). A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements.

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

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

(9) ENFORCEMENT.—

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

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

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

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

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

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

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

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

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

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

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

282.318 Enterprise security of data and information technology.—

(4) To assist the Agency for Enterprise Information Technology in carrying out its responsibilities, each agency head shall, at a minimum:

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

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

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

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