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 breach of security concerning confidential personal information in third-party possession; creating s. 501.170, F.S.; providing definitions; requiring specified entities to take reasonable measures to protect and secure data in electronic form containing personal information; requiring specified entities to notify the Department of Legal Affairs of data security breaches; requiring notice to individuals of data security breaches in certain circumstances; providing exceptions to notice requirements in certain circumstances; specifying contents of notice; requiring notice to credit reporting agencies in certain circumstances; requiring the department to report annually to the Legislature; 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; providing an effective date.

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

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

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 Section 817.5681, Florida Statutes, is repealed.

Section 3. Section 501.170, Florida Statutes, is created to read:

501.170 Security of confidential personal information.—

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

(a) "Breach of security" means unauthorized access of data in electronic form containing personal information.

(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 notification requirements of subsections (3)-(6), the term includes a governmental entity.

(c) "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.

(e) "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.

(f)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) Social security number.

(II) 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) 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.

(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.

(VI) Any other information from or about an individual that could be used to personally identify that person; or

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. "Personal information" 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.

(g) "Customer records" means any material, regardless of the physical form, on which 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.

(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 OF SECURITY BREACH.—

(a) A covered entity shall give notice of any breach of security following discovery by the covered entity. Notice of the breach of security shall be provided to the department and 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.

(b) In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall promptly notify the covered entity of the breach of security. Upon receiving notification from a third-party agent, a covered entity shall provide notification as required under subsection (3).

(4) NOTIFICATION REQUIREMENTS.—

(a) A notification required under subsection (3) with respect to a breach of security 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. Notification to the affected individuals must be made within 30 days after the determination of the breach or reason to believe a breach had occurred, unless subject to a delay authorized under paragraph (d).

(b) Upon determining that a breach occurred, a covered entity must provide written notice to the department as promptly as possible, but within 30 days after the determination. Such notice must be given to the department even for breaches involving paragraph (c) or paragraph (d). Written notice must include:

1. A synopsis of the events surrounding the breach.

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

report.

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

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

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

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

7. A copy of the notice sent to the individual.

8. 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.

In lieu of providing the written notice to the department, the judicial branch, the Executive Office of the Governor, the Department of Financial Services, and the Department of Agriculture and Consumer Services may post the information described in subparagraphs 1.-7. on their agency-managed websites.

(c) If a federal or state law enforcement agency determines that the notification required under this subsection would interfere with a criminal investigation, the notification shall be delayed upon the written request of the law enforcement agency for any period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a

subsequent written request, revoke such delay or extend the period set forth in the original request made under this paragraph by a subsequent request if further delay is necessary.

(d) Notwithstanding paragraph (a), notification to the affected individuals is not required if, after an appropriate investigation and written consultation with relevant federal and state 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.

(5) METHOD AND CONTENT OF NOTIFICATION.—

(a) A covered entity required to provide notification to an individual under subsection (3) shall be in compliance with such requirement if the covered entity provides such notice by one of the following methods:

1. Written notification sent to the postal address of the individual in the records of the covered entity.

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

(b) Regardless of the method by which notification is provided to an individual under paragraph (a) with respect to a breach of security, such notification shall include:

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:

a. The breach of security.

b. The personal information that the covered entity maintained about the individual.

(c) A covered entity required to provide notification to an individual under subsection (3) may provide substitute notification in lieu of the direct notification required by paragraph (a) if such direct notification is not feasible because the cost of providing notice would exceed $250,000, the affected individuals exceed 500,000 persons, or the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notification shall include the following:

1. A conspicuous notice on the Internet website of the covered entity, if such covered entity maintains a website.

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

(d) A covered entity that is in compliance with any federal law that requires such covered entity to provide

notification to individuals following a breach of security is deemed to comply with this section as long as it promptly provides the information required by paragraph (4)(b) to the department.

(6) CREDIT REPORTING AGENCIES.—If a covered entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons 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 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

(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 subsection (2), subsection (3), subsection (4), or subsection (5) in the preceding calendar year.

(8) REQUIREMENTS FOR DISPOSAL OF INDIVIDUAL RECORDS.—Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of 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 act or 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 civil penalties provided for in paragraph (a), a covered entity that violates this section shall be liable for a civil penalty not to exceed $500,000, as follows:

1. In the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days.

2. If notification is not made within 180 days, any person required to make notification under subsection (3) who fails to do so is subject to a civil penalty of up to $500,000.

The civil penalties for failure to notify provided in this paragraph shall 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 provided in s. 501.170 ~~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. 501.170 ~~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.