The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Commerce and Tourism

BILL:	SB 1524
INTRODUCER:	Senator Thrasher
SUBJECT:	Security of Confidential Personal Information
DATE:	March 21, 2014 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Siples	Hrdlicka	CM	**Pre-meeting**
2.			RC	

I. Summary:

SB 1524 creates the "Florida Information Protection Act of 2014." The bill requires notice be given to affected customers and the Department of Legal Affairs (DLA) when a breach of security of personal information occurs. The bill requires such notice to be given within 30 days of the discovery of the breach, unless delayed at the request of law enforcement for investigative purposes. The bill provides enforcement authority to the DLA under the Florida Deceptive and Unfair Trade Practices Act to civilly prosecute violations. A violator of the bill's provisions may also be subject to civil penalties, similar to current law, if breach notification is not provided timely. State governmental entities are required to provide notification of security breaches to the DLA, but are not liable for civil penalties for failure to timely report the security breaches.

The bill requires the DLA to submit an annual report to the Legislature, by February 1 of each year, detailing any reported breaches of security by governmental entities or their third-party agents for the preceding year, along with any recommendations for security improvement. The report must also identify any governmental entity that has violated the breach notification provisions.

The bill requires customer records, both physical and electronic, to be disposed in a manner that protects personal information from being disclosed. This provision does not apply to governmental entities.

The bill repeals s. 817.5681, F.S., which contains the current law requirements for breach notification.

II. Present Situation:

Data breaches may be caused by computer hacking, malware, physical loss of portable devices, or inadvertent exposure of confidential data on websites or in e-mail.[1] There have been a number of high profile data breaches in the last few years.[2] In 2013, nationwide, there were more than 600 data breaches compromising more than 91 million consumer records.[3] Most states, including Florida, have laws that require disclosure to consumers when a breach of security occurs.[4]

Current Florida Law on Data Breaches

Current law provides that any person[5] doing business in this state who also maintains computerized data in a system that includes personal information must adhere to certain procedures if there is a breach of the system.[6]

A notification of the breach[7] must be provided to any resident of this state whose unencrypted personal information[8] was, or is reasonably believed to have been, acquired by an unauthorized person.[9] The notification must be made without unreasonable delay but no later than 45 days following the determination of the breach. Notification of the breach may be delayed upon request of a law enforcement agency if such agency determines that notification will impede the

[1] Gina Stevens, Cong. Research Serv., *Data Security Breach Notification Laws*, R42475 (Apr. 10, 2012), *available at* https://www.fas.org/sgp/crs/misc/R42475.pdf (last visited Mar. 10, 2014).
[2] Target suffered a data breach that affected more than 40 million customers. *See* http://www.washingtonpost.com/business/economy/target-data-breach-what-you-should-know/2013/12/19/e00e3326-68e2-11e3-ae56-22de072140a2_story.html (last visited Mar. 10, 2014); Adobe Acrobat's breach affected 2.9 million customers. *See* http://www.usatoday.com/story/cybertruth/2013/10/03/adobe-loses-29-mil-customer-records-source-code/2919229/ (last visited Mar. 10, 2014); Neiman-Marcus recently had a data breach and indicated that it may ultimately affect more than 100 million customers. *See* http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html?_r=0 (last visited Mar. 10, 2014).
[3] Identity Theft Resource Center, Data Breach Category Summary (Feb. 20, 2014), *available at* http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html (last visited Mar. 7, 2014). This includes data breaches in several industries, including financial, business, educational, government, and health care sectors.
[4] National Conference of State Legislatures, "State Security Breach Notification Laws," (Jan. 21, 2014), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Mar. 7, 2014). Alabama, Kentucky, New Mexico, and South Dakota do not have their own data breach notification laws.
[5] "Person" includes individuals, children, firms, associations, joint adventures, partnerships, estates, trusts, business trusts, syndicates, fiduciaries, corporations, and all other groups or combinations. *See* s. 1.01(3), F.S. The law also applies to a governmental agency or subdivision.
[6] *See generally* s. 817.5681, F.S...
[7] Section 817.5681(4), F.S., defines "breach" as an unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information.
[8] Section 817.5681(5), F.S., defines "personal information" as an individual's first name, first initial and last name, or any middle name and last name, in combination with one or more of the following, when not encrypted: social security number, driver's license number or Florida Identification Card number, and account number, credit card number, or debit card number, in combination with any required security code or password that would permit access to an individual's financial account. This does not include publicly available information that is lawfully made available from government records or widely distributed media.
[9] Section 817.5681(7), F.S., defines "unauthorized person" as any person who does not have permission from, or a password issued by, the person who stores the computerized data to acquire such data, but does not include any individual to whom the personal information pertains.

investigation.[10] Notification is not required if, after an appropriate investigation or consultation with relevant governmental law enforcement agencies, it is determined that the breach has not and will not likely result in harm to the individuals whose personal information has been compromised.[11]

A person is deemed to be in compliance with this law if the person's provides notification pursuant to the person's own breach notification procedures that are consistent with this law or if the person provides notification in accordance with the rules, regulations, procedures, or guidelines established by the person's primary or functional federal regulator.

A person who fails to provide timely notification, as required by statute, is liable for an administrative fine of up to $500,000, as follows:[12]

- $1,000 per day, each day the breach goes undisclosed for up 30 days, and thereafter $50,000 for each 30-day period or portion thereof for up to 180 days.
- If notification is not made within 180 days, a person who failed to make a required disclosure of a breach is subject to an administrative fine of up to $500,000.

A person, who maintains computerized personal information on behalf of another entity, must notify that business within 10 days of discovery of a data breach. The two parties may come to an agreement on who will provide notice to the affected individuals. However, if no agreement is reached, then the entity having the direct relationship with the affected individuals will be responsible for complying with the notification procedures required by law. If a person fails to notify a business entity of a breach within 10 days, that person will be subject to administrative sanctions similar to those discussed above.[13]

Notice may be written, or it may be provided electronically if the notice that is provided is consistent with applicable federal law, including the consumer's affirmative consent to electronic records.[14] Substitute notice maybe given if a person demonstrates that the cost of providing notice would exceed $250,000, more than 500,000 individuals require notification of the breach, or there is a lack of sufficient contact information. Substitute notice must include an email or email notice, conspicuous posting on the business owner's web page, and notification to major statewide media.

Finally, current law provides that in the event that more than 1,000 individuals require notification at a single time, the person must also notify all consumer reporting agencies that

[10] Section 817.5681(3), F.S. The notification time period required under law begins when the law enforcement agency notifies the person maintaining the database that notification will not compromise the investigation.
[11] Section 817.5681(10), F.S. The determination must be documented in writing and maintained for 5 years.
[12] Sections 817.5681(1)(b)-(d), F.S. The administrative sanctions apply per breach and not per individual affected by the breach. These provisions do not apply to a governmental entity, unless it has entered into a contract with a contractor or third-party administrator to provide governmental services. In that case, the provisions would apply to the contractor or third-party administrator.
[13] Section 817.5681(2), F.S. Administrative sanctions include $1,000 for each day the breach goes unreported for up to 30 days and; thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days; and after 180 days, an administrative fine of up to $500,000.
[14] Section 817.5681(6), F.S. 15 U.S.C. s. 7001, provides the guidelines for electronic records and signatures in commerce, including consumer disclosures, consumer consent guidelines, and retention of records.

compile and maintains files on consumers on a nationwide basis of the timing, distribution, and content of the notices.[15]

Federal Law

There is no single federal law that governs notification of a data or security breach.[16] There are regulations that govern federal governmental agencies, such as the Federal Information Security Management Act of 2002,[17] which provides security requirements for all applicable federal government agencies. Additionally, federal agencies must comply with a memorandum that directed the agencies to develop a breach notification policy and provided the necessary elements of such policies.[18]

With regard to the private sector, industry-specific regulations have been implemented.[19] For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[20] requires certain covered entities[21] to comply with privacy and security standards to protect individually identifiable health information.[22] The Health Information Technology for Economic and Clinical Health Act[23] extended the privacy and security standards of HIPAA to the business associates of HIPAA-covered entities.[24] It also directed the Department of Health and Human Services to issue regulations to covered entities that provide for notification in cases of breaches of unsecured protected health information, and the Federal Trade Commission was directed to issue regulations to certain web-based businesses to notify customers when the security of their health information is breached.

Under the Gramm-Leach-Bliley Act,[25] financial institutions are required to secure and protect consumers' nonpublic personal information. The act required banking agencies to develop guidelines for the security, integrity, and confidentiality of customer information. One of the guidelines recommends that financial institutions implement a risk-based response system, including breach notification procedures. The guidelines prohibit delaying or forgoing customer notification because of embarrassment or inconvenience.[26]

---

[15] Section 817.5681(12), F.S.
[16] Stevens, *supra* note 1, at 7.
[17] 44 U.S.C. s. 3541, et seq.
[18] Memorandum from Clay Johnson III, Deputy Director for Management, Office of Management and Budget, Executive Office of the White House, to the Heads of Executive Departments and Agencies, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," M-07-16 (May 22, 2007), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf (last visited Mar. 17, 2014).
[19] Stevens, *supra* note 1, at 7.
[20] Pub. Law 104-191 (Aug. 21, 1996).
[21] Covered entities include health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically.
[22] Stevens, *supra* note 1, at 11-13.
[23] Pub. Law No. 111-5 s. 13400 (Feb. 17, 2009).
[24] Stevens, *supra* note 1, at 13-17.
[25] Pub. Law No. 106-102 (Nov. 12, 1999).
[26] Stevens, *supra* note 1, at 17-20.

The Data Security Act of 2014 was introduced in the U.S. Senate in January 2014. The bill provides breach notification procedures, enforcement, and preemption of state laws with regard to the security of consumer information.[27]

III. Effect of Proposed Changes:

Section 1 provides that the bill may be cited as the "Florida Information Protection Act of 2014."

Section 2 repeals s. 817.5681, F.S., which outlines the current procedures for notification when a breach of security involving personal information occurs. The substance of this section has been moved to the newly created s. 501.171, F.S.

Section 3 creates s. 501.171, F.S., to provide the procedure for protection and security of sensitive personal information[28] in the possession of covered entities.[29] Covered entities, governmental entities, and third-party agents are required to take reasonable measures to protect and secure electronic data containing personal information. When the security of a data system is breached, a covered entity must provide notice to the DLA and effected individuals unless otherwise provided in the bill. If a covered entity fails to provide the required notices, it may face civil penalties.

Notice to the Department of Legal Affairs

The bill provides that entities subject to the provisions of the bill must provide written notice of any breach of security to the DLA within 30 days after the determination of the breach or reason to believe a breach had occurred. Notice to the DLA is not required in current law. The notice must include:

- A synopsis of the events surrounding the breach;
- A police report, incident report, or computer forensics report;
- The number of individuals in this state who were or potentially have been affected by the breach;

[27] S. 1927 (113th Congress). This bill was referred to the Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance, and a hearing was held by that committee on Feb. 3, 2014. *See also* Alina Selyukh, "U.S. Retailers at Senate Hearing: Hackers Have Upper Hand," Reuters, (Feb. 4, 2014), *available at* http://www.reuters.com/article/2014/02/04/us-usa-hacking-congress-idUSBREA121I620140204 (last visited Mar. 10, 2014).

[28] The bill expands the definition of "personal information." "Personal information" means an individual's first name or first initial and last name in combination with one of the following: a social security number; driver license or identification card number, passport number, military identification number, or other number issued by a governmental entity used to verify identity; a financial account number or credit or debit card number, in combination with any required security code, access code, or password needed to permit access to the financial account; an individual's medical history, mental or physical condition, or medical treatment or diagnosis; an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer; or any other information from or about an individual that could be used to personally identify that person. A user name or e-mail address, in combination with a password or security question and answer is also considered "personal information." Information that is publicly available from a federal, state, or local governmental entity or information that is encrypted, secured, or modified by a method or technology that removes personally identifiable information is not considered "personal information."

[29] A "covered entity" is a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For the provisions of this bill detailing the requirements for notification when there is a breach of security, disposal of customer records, and enforcement, this term also includes governmental entities.

- A copy of the policies in place regarding breaches;
- Any steps that have been taken to rectify the breach;
- Any services being offered by the covered entity to individuals, without charge, and instructions as to how to use such services;
- A copy of the notice sent to individuals affected or potentially affected by the breach;
- 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
- Whether the notice to individuals is being made pursuant to federal law or pursuant to state law.

For breaches of security occurring within the judicial branch, the Executive Office of the Governor, the Department of Financial Services, and the Department of Agriculture and Consumer Services, the notice of the breach of security may be posted to an agency-managed website in lieu of the written notice to the DLA.

Notice to Individuals

A covered entity must provide notice to each individual in Florida whose personal information was, or is reasonably believed to have been, accessed as a result of a breach. Notice must be provided as quickly as possible, taking into account the time needed to determine the scope of the breach of security, to identify affected individuals, and to restore reasonable integrity of the data system that was breached. However, notice must be provided within 30 days of determination of the breach unless:

- Notice is delayed upon the written request of a federal or state law enforcement agency for a reasonably necessary period, if the agency determines that notice to individuals would interfere with a criminal investigation; or
- Notice is waived after an appropriate investigation and written consultation with relevant federal and state law enforcement agencies, if the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm. Such a determination must be documented in writing and maintained for at least 5 years and must be provided to the DLA within 30 days of such a determination.

The bill shortens the amount of time a covered entity has to notify affected individuals of the breach from 45 days to 30 days.

The notice to affected individuals must be made by either written notice sent to the individual's mailing address or by e-mail sent to the individual's e-mail address. The notice must include:

- The date, estimated date, or estimated date range of the breach of security;
- A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security; and
- Information that the individual can use to contact the covered entity about the breach of security and the individual's personal information maintained by the covered entity.

Similar to current law, this notice may be substituted in lieu of direct notice to the individual if the cost of providing notice will exceed $250,000, the number of affected individuals exceeds 500,000, or the covered entity does not have an e-mail address or mailing address for the affected

individuals. The substitute notice must include a conspicuous notice on the Internet website of the covered entity, if the entity maintains a website, and notice in print and broadcast media, including major media in urban and rural areas where the affected individuals reside.

If a covered entity is in compliance with a federal law that requires the entity to provide notification to individuals following a breach of security, the covered entity is deemed to comply with the notice requirements of this bill.

The bill provides that in the event that more than 1,000 individuals require notification at a single time, the person must also notify all consumer reporting agencies that compile and maintains files on consumers on a nationwide basis of the timing, distribution, and content of the notices. This requirement is similar to current law.

Notice by Third-Party Agents[30]

If the data system is maintained by a third-party agent, the third party agent must promptly notify the covered entity in the event of a breach of security.[31] The covered entity is responsible for providing notice to affected individuals in the same manner as required if the breach had been to its own system.

Annual Report

The DLA is required to submit a report, by February 1 of each year, 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 their third-party agents in the preceding calendar year, along with any recommendations for security improvements. The report must identify any governmental entity that has violated the provisions of this bill.

Disposal of Records

Each covered entity or third-party agent must take all responsible measures to dispose or arrange for the disposal of customer records[32] containing personal information within its custody and control when such records are no longer to be retained. This requirement applies to both electronic and physical customer records.

Enforcement

A violation of the provisions of the bill will be treated as unfair or deceptive trade practice in any action brought by the DLA.[33] A covered entity or third-party agent that fails to comply with the

[30] A "third-party agent" is an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.
[31] Current law requires notification to the covered entity within 10 days.
[32] "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.
[33] Section 501.207, F.S., provides that the DLA may bring an action to obtain declaratory judgment that an act or practice violates the Florida Deceptive and Unfair Trade Practices Act (FDUTPA), an action to enjoin a person who has violated or is

breach notification provisions of this bill may also be liable for a civil penalty, not to exceed $500,000, as follows:

- $1,000 per day, each day the breach goes undisclosed for up 30 days, and thereafter $50,000 for each 30-day period or portion thereof for up to 180 days.
- If notification is not made within 180 days, a covered entity who failed to make a required disclosure of a breach is subject to civil penalties not to exceed $500,000.

The civil penalties apply per breach and not per affected individual. The civil penalties are the same as the administrative fines that are in current law. The penalties collected will be deposited into the General Revenue Fund.

This bill does not create a private cause of action.

Sections 4 and 5 amend ss. 282.0041 and 282.318, F.S., to update cross references.

Section 6 provides that the act shall take effect on July 1, 2014.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

The fiscal impact on the private sector is expected be minimal. The provisions related to notification of a security breach to affected individuals is similar to the notification required by current law. However, the time frame for the notification has been reduced from 45 days in current law to 30 days in the bill. The notification to the DLA is a new requirement, but the cost is expected to be minimal.[34]

---

likely to violate FDUTPA, or an action on behalf of consumers or governmental entities for actual damages caused by a violation of FDUTPA.

[34] Department of Legal Affairs, *Senate Bill 1524 Analysis*, (Mar. 17, 2014) (on file with the Senate Commerce and Tourism Committee).

The bill contains civil penalties for noncompliance with its provisions. The civil penalty amounts remain at the same level as current law. It is unknown how often businesses may be subject to the civil penalties for noncompliance.

The bill mandates that businesses properly dispose of customer records containing personal information. The fiscal impact of this requirement is unknown. However, many businesses may already be required to properly dispose of customer records under other laws, such as the HIPAA and the Gramm-Leach-Bliley Act.

C. Government Sector Impact:

The bill may have an unknown positive impact on state revenues to the extent the DLA enforces civil penalties against violations of the act.

The bill requires the DLA to enforce the bill's provisions, collect reports of breaches of security information from covered entities, and produce an annual report to the Legislature. However, the DLA indicates that any costs and expenditures can be absorbed into its current appropriations.[35]

The Department of Agriculture and Consumer Services does not to expect the bill to have an impact on its agency.[36]

The Department of Highway Safety and Motor Vehicles indicates that there will be an indeterminate fiscal impact in the event of a security breach for the mailing and media notification costs. Additionally, approximately 40 hours of programming will be needed to implement changes made by this bill. The cost is estimated to be $1,600.[37]

The bill may have an indeterminate fiscal impact on the State Courts System. However, any increase in judicial workload will likely by absorbed within existing resources. There may be a slight increase in revenues to the State Courts System's trust fund from civil filing fees for enforcement actions by the DLA.[38]

VI. Technical Deficiencies:

None.

[35] *Id*.
[36] Department of Agriculture and Consumer Services, *Senate Bill 1524 Analysis*, (Mar. 11, 2014) (on file with the Senate Commerce and Tourism Committee).
[37] Department of Highway Safety and Motor Vehicles, *2014 Agency Bill Analysis, Senate Bill 1524*, (Mar. 4, 2014) (on file with the Senate Commerce and Tourism Committee). The cost estimate is based on 40 hours of programming at a rate of $40 per hour.
[38] Office of the State Courts Administrator, *2014 Judicial Impact Statement, Senate Bill 1524*, (Mar. 20, 2014) (on file with the Senate Commerce and Tourism Committee).

VII. Related Issues:

Although the bill does not specifically provide that the covered entity must be conducting business in this state, the Florida Long-Arm statute[39] may provide courts with the authority to assert personal jurisdiction over a nonresident covered entity. The statute enumerates a number of actions that a person or his or her representative may take that would submit that person to the jurisdiction of Florida courts. Those actions include, among other things, operating, conducting, engaging in, or carrying on a business venture in this state or having an office or agency in this state; committing a tortious act within this state; or breaching a contract in this state by failing to perform acts required by the contract to be performed in this state. A person may also become subject to the jurisdiction of a Florida court if the person is engaged in substantial and not isolated activity within Florida.

VIII. Statutes Affected:

This bill repeals section 817.5681 of the Florida Statutes.

This bill creates section 501.171 of the Florida Statutes.

This bill amends the following sections of the Florida Statutes: 282.0041 and 282.318.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.

[39] Section 48.193, F.S.