HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 7085 PCB CJS 14-04 Security of Confidential Personal Information
SPONSOR(S): Judiciary Committee; Civil Justice Subcommittee; Metz
TIED BILLS: CS/HB 7087 **IDEN./SIM. BILLS:** CS/CS/SB 1524

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
Orig. Comm.: Civil Justice Subcommittee	10 Y, 1 N	Cary	Bond
1) Judiciary Committee	16 Y, 0 N, As CS	Cary	Havlicak

SUMMARY ANALYSIS

Current law requires that a person who conducts business in Florida and maintains personal information in a computerized data system must disclose a breach in the security of the data to affected residents of Florida no later than 45 days following a determination that unencrypted personal information was acquired.

This bill repeals the current law and creates the Florida Information Protection Act of 2014 (Act). The Act requires notice of a breach, if it affects 500 or more individuals in the state, to be given to the Department of Legal Affairs (DLA) in addition to being given to affected residents. The act also shortens the time limit for notice to 30 days with allowance for an additional 15 days with good cause, allows delay of notifications if a law enforcement agency requests that notice be delayed for investigation purposes, and provides the DLA with enforcement authority to civilly prosecute a violator of the terms of the Act under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA). The Act provides for penalties in addition to FDUTPA of $1000 for each day, up to 30 days, that the required notice of the breach is not given, and a penalty of $50,000 for each 30-day period thereafter that notice is not given, for up to 180 days, with an overall cap of $500,000.

The bill also requires covered entities to take all reasonable measures to dispose of personal information.

State government entities also must report a breach to the DLA, but are not liable for civil penalties and are not required to properly dispose of personal information by this bill. Counties and municipalities are not covered by the Act.

The fiscal impacts of this bill on state government and the private sector are unknown. The bill does not appear to have a fiscal impact on local government revenues or expenditures.

The bill has an effective date of July 1, 2014.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Current law requires that a person who conducts business in Florida and maintains personal information in a computerized data system must disclose a breach in the security of the data to any resident of this state subject to certain exceptions. When a disclosure is required, it must be made without unreasonable delay, and no later than 45 days following the determination that unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person and the acquired information materially compromises the security, confidentiality, or integrity of personal information.[1]

Current law provides that any person who fails to make the required disclosure within forty-five days is liable for an administrative fine in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days. The person is liable for up to $50,000 for each 30 day period the breach goes undisclosed up to 180 days.[2] If disclosure is not made within 180 days, the person is subject to an administrative fine of up to $500,000.[3]

The disclosure required must be made by all persons in the state in possession of computerized data, but the administrative sanctions described above do not apply in the case of computerized information in the custody of any governmental agency or subdivision. However, if the governmental agency or subdivision has entered into a contract with a contractor of third party administrator to provide governmental services, the contractor or third party administrator is a person to whom the administrative sanctions would apply. Nevertheless, that contractor or third party administrator found in violation of the non-disclosure restrictions does not have an action for contribution or set-off available against the employing agency or subdivision.[4]

Further, current law provides that any person who, on behalf of another business entity, maintains computerized data that includes personal information, must notify the business entity for whom the information is maintained of any breach of the security of the data within 10 days of the determination that a breach has occurred. This notification requirement applies if the personal information is reasonably believed to have been acquired by an unauthorized person. The administrative fines described above apply to a person who fails to disclose a security breach under this provision.

Finally, current law provides that in the event that notification is required of more than 1,000 persons at one time, the person must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices.[5]

Effect of Proposed Changes

The bill repeals current law regarding data breaches at s. 817.5681, F.S., and creates s. 501.171, F.S., known as the “Florida Information Protection Act of 2014” (Act).

The bill creates s. 501.171(1), F.S., to provide definitions. The bill defines the terms “breach,” “breach of the security of the system,” “personal information,” “unauthorized person,” and “person.”

The bill creates s. 501.171(2), F.S., to require a “covered entity” to provide notice of any breach of security once it is discovered. A covered entity is defined as a sole proprietorship, partnership,

[1] Section 817.5681(1)(a), F.S.
[2] Section 817.5681(1)(b)1., F.S.
[3] Section 817.5681(1)(b)2., F.S.
[4] Section 817.5681(1)(d), F.S.
[5] Section 817.5681(12), F.S.

corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information, including a governmental entity.[6] A breach of security is an unauthorized access of data in electronic form containing personal information. Personal information includes either 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, or an individual's first initial or name and last name in combination with any one or more of the following:

- Social security number;
- Driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
- 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;
- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

The bill creates s. 501.171(3), F.S., to require that a covered entity provide notice to the Department of Legal Affairs (DLA) of any breach, if it affects 500 or more individuals in the state, in security within 30 days after the determination of the breach or a reason to believe a breach had occurred. If the covered entity provides a written explanation of a good cause for delay, the covered entity may receive an additional 15 days. Written notice to the DLA must include:

- A synopsis of the events surrounding the breach;
- The number of individuals in this state who were or potentially have been affected by the breach;
- Any steps that have been taken to rectify the breach;
- Any services being offered by the covered entity to individuals, without charge, and how to use such services;
- A copy of the notice sent to the individuals affected; and
- The name, address, telephone number, and e-mail address of an employee of the covered entity from whom additional information may be obtained about the breach.

If requested by the DLA, the covered entity must provide:

- A police report, incident report, or computer forensics report;
- A copy of the policies in place regarding breaches; and
- Steps that have been taken to rectify the breach.

If the covered entity is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, the agency may post the information on their agency-maintained websites rather than providing written notice to the DLA.

The bill creates s. 501.171(4), F.S., to require that a covered entity, or the covered entity's agent, to provide notice to each individual in Florida whose personal information was accessed, or was reasonably believed to have been accessed, by a breach. Notification to affected individuals must be made as expeditiously as practicable and without unreasonable delay, but no later than 30 days after the determination of a breach unless:

- If a federal or state law enforcement agency determines that notice to individuals would interfere with a criminal investigation, in which case the notice will be delayed for any period that the law enforcement agency determines is reasonably necessary; or

[6] A governmental entity is not subject to the enforcement provisions of the Act or the requirements for disposal of individual records. Furthermore, counties and municipalities are not "governmental entities" for the purposes of the Act.

- 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 likely will not result in identity theft or any other financial harm to the individuals. 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 notice to an affected individual must be made by either written notice sent to the individual's mailing address or an e-mail sent to the individual's e-mail address and 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 to inquire about the breach and the personal information that the covered entity maintained about the individual.

If the cost of such notification would exceed $250,000, or if there are more than 500,000 affected individuals, or if the covered entity does not have an e-mail address or mailing address for the affected individuals, the covered entity may provide substitute notification. The substitute notification must include a conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website, and notification 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 covered entity to provide notification to individuals following a breach of security, the covered entity is deemed to comply with these requirements, provided the covered entity timely provides a copy of such notices to the DLA.

The bill creates s. 501.171(5), F.S., to require a covered entity to notify consumer credit reporting agencies if the covered entity must provide notification to more than 1,000 individuals at a single time.

The bill creates s. 501.171(6), F.S., to require a third-party agent to notify the covered entity in the event of a breach of a security system maintained by a third-party agent. Notification should be as expeditiously as practicable, but no later than 10 days after the determination of the breach or a reason to believe that a breach occurred. The covered entity is then responsible for the notice as if the breach had been to the covered entity's own system. Alternatively, an agent may provide notice on behalf of the covered entity, but if the third-party does not provide proper notice, it is a violation attributed to the covered entity, not the third-party agent.

The bill creates s. 501.171(7), F.S., to require the DLA to provide an annual report, by February 1, to the President of the Senate and the Speaker of the House describing the nature of any reported breaches of security by governmental entities or third-party agents of governmental entities in the preceding year along with recommendations for security improvements.

The bill creates s. 501.171(8), F.S., to require each covered entity or third-party agent to 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 retained. Such disposal must involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means. This provision does not apply to governmental entities.

The bill creates s. 501.171(9), F.S., to provide the DLA with a means to enforce the Act. Specifically, if a covered entity violates any requirement of the Act, it will be treated as an unfair or deceptive trade practice[7] in any action brought by the DLA. An unfair or deceptive trade practice is punishable by a civil

[7] Section 501.207, F.S., allows the DLA to bring (1) an action to obtain a declaratory judgment that an act or practice violates the Florida Deceptive and Unfair Trade Practices Act (FDUTPA); (2) an action to enjoin any person who has violated, is violating, or is likely to violate FDUTPA; and/or (3) an action on behalf of one or more consumers or governmental entities for the actual damages caused by an act or practice in violation of FDUTPA.

penalty of not more than $10,000 for each violation.[8] A civil penalty is "strictly construed and is not to be extended by construction."[9] Therefore, a single breach event would likely be considered a single violation under FDUTPA.[10] However, the Act provides additional penalties beyond a typical unfair or deceptive trade practice claim. In addition to the $10,000 per violation penalty under FDUTPA, the Act provides for a civil penalty 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. If notification is not made within 180 days, the total penalty may not exceed $500,000. All penalties will be deposited into the General Revenue Fund.

The bill creates s. 501.171(10), F.S., to provide that the bill does not create a private cause of action. The bill also amends ss. 282.0041 and 282.318, F.S., to update cross references in accordance with the Act.

The bill provides an effective date of July 1, 2014.

B. SECTION DIRECTORY:

Section 1 provides a name for the Act.

Section 2 repeals s. 817.5681, F.S., relating to breach of security concerning confidential personal information in third-party possession and administrative penalties.

Section 3 creates s. 501.171, F.S., relating to security of confidential personal information.

Section 4 amends s. 282.0041, F.S., relating to definitions.

Section 5 amends s. 282.318, F.S., relating to enterprise security of data and information technology.

Section 6 provides an effective date of July 1, 2014.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

The bill may have an unknown, positive impact on state revenues to the extent that the DLA enforces and collects civil penalties against violators of the Act.

2. Expenditures:

The bill appears to create an unknown increase in state government expenditures for the DLA. However, the DLA indicates that any additional duties required of consumer protection staff can be absorbed within existing appropriations for the next fiscal year.[11]

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

The bill does not appear to have any impact on local government revenues.

2. Expenditures:

[8] Section 501.2075, F.S.
[9] *3B TV, Inc. v. State, Office of Atty. Gen.*, 794 So.2d 744, 749 (Fla. 1st DCA 2001).
[10] *See id. See also* s. 501.171(9)(b) of the bill, which provides that a civil penalty must be applied per breach, and not per individual affected.
[11] *See* Department of Legal Affairs bill analysis for HB 7085 (on file with Judiciary Committee staff.)

The bill does not appear to have any impact on local government expenditures.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill creates a requirement to notify affected individuals of a breach. Because the reporting requirement is similar to that in current law, this requirement is not anticipated to have a fiscal impact on the private sector.

The bill creates a requirement to notify the state in the event of a breach. The requirement is new, but is expected to have a minimal impact on the private sector.

The bill contains civil penalties that may be assessed against individuals and entities in the private sector. The penalty can be as high as $500,000 for violations of the Act. It is unknown how often these penalties would be assessed and their impact on the private sector is thus unknown.

The bill mandates that businesses properly dispose of individual records. The fiscal impact of this requirement on the private sector is unknown. Many companies are already required by current state and federal law to take reasonable measures to properly dispose of certain personal information, and thus will not be impacted by this requirement in the bill. For example, the Fair Credit Reporting Act and the Federal Trade Commission require that businesses properly dispose of consumer information, and the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act require health care providers properly dispose of certain health information.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

The bill does not appear to require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not appear to create a need for rulemaking or rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On February 19, 2014, the Civil Justice Subcommittee adopted one amendment to the PCB and reported the bill favorably. The amendment provides a slightly revised structure and technical and stylistic changes throughout.

On April 4, 2014, the Judiciary Committee adopted one amendment and reported the bill favorably as a committee substitute. The amendment provides that certain requirements for a written notice to the DLA need only be submitted upon the request of the DLA, that a breach needs to affect 500 persons before it need be reported, and that a covered entity may receive an additional 15 days to file a report with good cause, along with other minor changes.

This analysis is drafted to the committee substitute as passed by the Judiciary Committee.