HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: PCB CJS 14-04 Security of Confidential Personal Information
SPONSOR(S): Civil Justice Subcommittee
TIED BILLS: PCB CJS 14-05 **IDEN./SIM. BILLS:** None

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
Orig. Comm.: Civil Justice Subcommittee		Cary	Bond

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 no later than forty-five days following a determination that unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person if the acquired information materially compromises the security, confidentiality, or integrity of personal information.

This Proposed Committee Bill (PCB) repeals the current law and creates the Florida Information Protection Act of 2014 (Act). The Act requires notice of a breach be given to the Department of Legal Affairs (DLA) in addition to being given to affected residents, shortens the time limit for notice to 30 days, 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 PCB 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 PCB. Counties and municipalities appear to be exempt from the Act.

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

The PCB 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 forty-five 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 the 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, although that contractor or third party administrator found in violation of the non-disclosure restrictions would 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, 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. The PCB defines the terms “breach,” “breach of the security of the system”, “personal information,” “unauthorized person,” and “person.” The PCB specifies what type of notice must be provided.[5]

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 basis6 of the timing, distribution and content of the notices.[6]

Effect of the PCB

The Proposed Committee Bill (PCB) repeals current law regarding data breaches at s. 817.5681, F.S., and creates s. 501.170, F.S., known as the “Florida Information Protection Act of 2014” (Act).

The PCB creates s. 501.170(1), F.S., to provide definitions.

[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(2)(a), F.S.
[6] Section 817.5681(12), F.S.

The PCB creates s. 501.170(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, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information, including a governmental entity.[7] 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;
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or
- Any other information from or about an individual that could be used to personally identify that person.

The PCB creates s. 501.170(3), F.S., to require that a covered entity provide notice to the Department of Legal Affairs (DLA), and also to each individual in Florida whose personal information was accessed, or the covered entity reasonably believes was accessed, as a result of the breach. If a third-party agent maintains the system that was breached, the third-party agent must notify the covered entity, who is responsible for the notification to the DLA and individuals.

The PCB creates s. 501.170(4), F.S., to require that such notification be made as expeditiously as practicable and without unreasonable delay. Notification to affected individuals must be made within 30 days unless, 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.

If notification to individuals must be made due to the breach likely resulting in identity theft or other financial harm, the covered entity must provide written notice to the DLA as promptly as possible, but in any event, within 30 days after determining that a breach occurred. Written notice to the DLA 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;
- 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 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 and the steps taken to rectify the breach and prevent similar breaches.

[7] 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 do not appear to be "governmental entities" for the purposes of the Act.

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.

If a federal or state law enforcement agency determines that such notices would interfere with a criminal investigation and provides a written request to that effect, the notification to affected individuals must be delayed for any period that the law enforcement agency determines is reasonably necessary.

The PCB creates s. 501.170(5), F.S., to require written notice to an individual to be by either a written notification sent to the postal address of the individual or an e-mail notification sent to the e-mail address of the individual 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 effective 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 the requirements of s. 501.170(5), F.S., as long as it provides notification to the DLA.

The PCB creates s. 501.170(6), F.S., to require a covered entity to notify consumer credit reporting agencies if the covered entity must provide notification to more than 1000 individuals at a single time.

The PCB creates s. 501.170(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 PCB creates s. 501.170(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.

The PCB creates s. 501.170(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 act or practice[8] in any action brought by DLA. An unfair or deceptive act or practice is punishable by a civil penalty of not more than $10,000 for each violation.[9] A civil penalty is "strictly construed and is not to be extended by construction."[10] Therefore, a single breach event would likely be considered a single violation under FDUTPA.[11] However, the Act provides additional penalties beyond a typical unfair or

[8] 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.
[9] Section 501.2075, F.S.
[10] *3B TV, Inc. v. State, Office of Atty. Gen.*, 794 So.2d 744, 749 (Fla. 1st DCA 2001).
[11] *See id. See also* s. 501.170(9)(b) of the PCB, which provides that a civil penalty must be applied per breach, and not per individual affected.

deceptive act or practice claim. In addition to the $10,000 per violation penalty under FDUTPA, the Act provides for a civil penalty of $1000 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, not to exceed $500,000. If notification is not made within 180 days, any person required to make notification but fails to do so is subject to a civil penalty of up to $500,000. All penalties will be deposited into the General Revenue Fund.

The PCB creates s. 501.170(10), F.S., to explicitly state that the PCB does not create a private cause of action.

The PCB amends ss. 282.0041 and 282.318, F.S., to update cross references in accordance with the Act.

The PCB 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. 501.170, 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 PCB may have an unknown, positive impact on state revenues to the extent that DLA enforces civil penalties against violators of the Act.

2. Expenditures:

   The PCB 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.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

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

2. Expenditures:

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

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The PCB 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 PCB 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 PCB 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 PCB mandates that businesses properly dispose of individual records in order to avoid having those records fall into the wrong hands. 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 PCB. 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 to properly dispose of certain health information.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

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

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

n/a