F I S C A L I M P A C T R E P O R T

SPONSOR HBEC **ORIGINAL DATE / LAST UPDATED** 02/11/15 **HB** 217/HEBCS

SHORT TITLE Data Breach Notification Act **SB**

ANALYST Daly

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY15	FY16	FY17	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total		>$100.0-$500.0	>$75.0-$125.0	$175.0-$625.0	Recurring	General Fund and other State Funds

(Parenthesis ( ) Indicate Expenditure Decreases)

SOURCES OF INFORMATION

LFC Files

Responses Received From

Department of Information Technology (DOIT)
Administrative Office of the Courts (AOC)
Attorney General's Office (AGO)
Taxation & Revenue Department (TRD)
Regulation & Licensing Department (RLD)
Human Services Department (HSD)
Children, Youth & Families Department (CYFD)

SUMMARY

Synopsis of Bill

The House Business & Employment Committee Substitute for House Bill 217 enacts the Data Breach Notification Act (the Act) as a consumer protection measure. It requires notice be given to persons who are affected by a security breach involving their personal identifying information (PII), and is directed at the use or breach of information (a) without the approval or direction of the card issuer; (b) that results in the compromised security and confidentiality of access device data; and (c) that creates a material risk of harm or actual harm to a cardholder.

The bill defines terms that include PII, which means a person's first name or initial and last name

in combination with one or more data elements (social security number, driver's license number, government-issued identification number, or account, credit or debit card number in combination with other information that would permit access to a person's financial account) when that information is not protected through encryption or redaction or is otherwise unreadable or unusable. It also defines "security breach" as the unauthorized acquisition of computerized data that compromise the security, confidentiality or integrity of PII maintained by a person. It does not define "person" as that term is used in the Act. (Section 2)

CS/HB 217 requires a person that owns or licenses computerized data elements that include PII to notify each New Mexico resident whose unencrypted PII is reasonably believed to have been subject to a security breach, generally within 45 days following discovery of the breach. The bill sets out required contents and methods of notification, including substitute methods if the cost of notification exceeds $100 thousand, if more than 50 thousand residents must be notified, or if no physical address is on record. Further, notice is not required if a person determines the breach does not give rise to a significant risk of identity theft or fraud. A person that maintains its own notice procedures that are otherwise consistent with the law is deemed to be in compliance. Notification may be delayed if a law enforcement agency determines it will impede a criminal investigation, or as necessary to determine scope of the breach and restore the data system's integrity, security and confidentiality. (Sections 6, 7 and 9)

In addition, if a single breach requires notification to more than one thousand residents, notification must be given to AGO and major consumer reporting agencies as described in this bill no later than 45 calendar days following discovery, and additional information must be provided to AGO within that same time period. Notice also must be given to merchant providers within ten business days when the breach involved credit or debit card numbers. (Sections 10 and 11)

HB 217 also includes specific requirements for:

- Disposal of records with PII (Section 3);
- Storage and protection of personal identifying information (Section 4); and
- Implementation of security measures with respect to service provider use of personal identifying information (Section 5).

It also exempts those subject to two federal laws: the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). (Section 8)

The bill authorizes AGO to bring an action in the name of the state for violations of the Act for injunctive relief and damages for actual costs or losses, including consequential financial losses. Knowing or reckless violations of the Act may result in a civil penalty of the greater of $5,000 or $10 per instance of failed notification, up to a maximum of $150,000. (Section 12)

FISCAL IMPLICATIONS

In its analysis of the original bill, which report appears to be relevant to the Committee Substitute, TRD reported increased compliance costs for TRD and other state agencies that accept credit cards for their services. As shown in the table above, TRD estimated the initial risk assessment and compliance check cost may range from $100 thousand to $500 thousand depending on the size and complexity of the agencies' business and IT infrastructure. For TRD

alone, those costs may range from $100 thousand to $250 thousand. Further, anticipated recurring Payment Card Industry (PCI) standards and other related compliance cost could be in the range of $75 to $125 thousand annually. Those costs are also reflected in the table.

However, TRD also warned that the remediation cost can only be calculated after the initial risk assessment and compliance check is completed. Typically, initial cost to become PCI compliant could be in the range 2 to 4 times the cost of assessment. Downstream compliance will also have an impact on TRD; for example, a vendor of TRD, connected to the TRD network, will be expected to be PCI compliant, and TRD needs to have a mechanism to mitigate such risk(s) and liability.

In addition, TRD expressed concern that banks and PCI may impose additional fines leading to hundreds of thousands of dollars for non-compliance, which could lead to terminating its ability to accept credit cards. Further, TRD advised the cost will vary significantly depending on where the agency is in terms of information security and compliance maturity: although card processing is completed by a third party for many state agencies, those agencies' existing infrastructure may not be compliant with PCI standards. For example, the bill requires encryption of PII data.

More generally, DOIT reports that in the case of a data breach involving a state agency's information system, the fiscal impact to the agency could be significant, in both money expended and resources necessary to respond. As a method to address that possibility, TRD suggested a set aside of up to $150 thousand (or insurance coverage) to mitigate inherent risks, including costs of notification upon breach and any civil penalties that might be imposed.

In its response to the original bill, which response appears relevant to the Committee Substitute, AOC reported a fiscal impact on it would be realized only if a breach occurred, and estimated it could incur costs of up to $100,000 per event, based on the notification provisions in Section 6, Subsection D (providing for mail notification and electronic notification). A substitute notification is allowed only if the cost of sending mail and electronic correspondence exceeds $100,000 or the number of residents to be notifies exceeds 50,000 or the person on record does not have an address on record. The Judicial Information Division, through its systems, holds PII for 2,606,650 criminal defendants for use in positive identification of defendants. JID also holds an estimated 500,000 civil records that may hold PII.

It should be noted that the HIPAA exemption in Section 8 removes HSD programs such as Medicaid from liability under HB 217.

SIGNIFICANT ISSUES

New Mexico is only one of three states that do not have a data breach law on the books. As noted by the AGO in its analysis of the original bill, this bill allows the AGO to pursue companies who do not take appropriate precautions when securing PII.

However, perhaps because the term "person" is not defined, there is confusion about whether CS/HB 217 applies to state agencies and other public bodies. For example, CYFD reports that it provides debit cards to providers for services they provide to children in care of the state for foster care, adoptions and childcare. Its files related to these cards contain providers' PII, but CYFD believes that because it is not a financial institution, the bill's provisions do not apply to these files.

Other responding agencies, after first questioning whether the term "person" includes them, then assume in their analyses it does.

DOIT comments:

> Although the state currently takes security and confidentiality very seriously, this law if enacted would require at minimum a review of the processes that currently protect this type of information. Current security rules do have standards and guidelines to protect PII, but DOIT could promulgate additional rules to address certain provisions of this Act. For example, as the state CIO, DOIT could set standards as to what is reasonable for state owned system in response to the mandate that reasonable measures be taken to protect and destroy PII. It notes, as well, that for many state owned systems that contain PII, there are already strict requirements in place that are set by the federal government, such as tax or health information.
>
> Overall, DOIT will continue to invest time and resources into security of state systems and PII. If CS/HB 217 is enacted, DOIT will work with all state agencies to ensure that processes are in place compliant with its requirements.

ADMINISTRATIVE IMPLICATIONS

TRD advised compliance with HB 217 may include:

1. Developing policies and procedures to address bill requirements.
2. Developing, implementing/modifying information technology and business processes to deal with credit card data.
3. Implementation/modification of information technology infrastructure to deal with secure processing, storing and disposal of credit card data.
4. Implementation of an adequate incident management program and related training for all employees.
5. Implementation of data breach notification and disclosure mechanism.
6. Periodic training, testing, validation of required internal information technology and business controls.

It also suggested that if the agencies' application was developed in COBOL, it may require a rewrite of the code to support encryption, or significant investment in secondary controls.

OTHER SUBSTANTIVE ISSUES

Companies which fall under the regulations of the federal Gramm-Leach-Bliley Act are subject to The Safeguards Rule which covers PII collected by "financial institutions," a term that is broadly defined in that act and includes not only banks, but, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguards Rule also applies to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care. Data breach notification is covered by this act but the act does not stipulate specific time frames. See Federal Trade

Commission, Bureau of Consumer Protection, here: http://www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule .

The National Conference of State reports that forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

DOIT reports it will continue to invest resources into security of the state systems and data it protects.

MD/je