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

SPONSOR House Floor **ORIGINAL DATE** 02/04/14 **LAST UPDATED** 02/19/14 **HB** CS/224/HFlS

SHORT TITLE Data Breach Notification Act **SB**

ANALYST Cerny

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY14	FY15	FY16	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total		Indeterminate	Indeterminate			

(Parenthesis ( ) Indicate Expenditure Decreases)

SOURCES OF INFORMATION

LFC Files

Responses Received From
Regulation and Licensing Department (RLD)
Department of Information Technology (DoIT)
Children, Youth and Families Department (CYFD)
Attorney General's Office (AGO)
Human Services Department (HSD)
Taxation and Revenue Department (TRD)

SUMMARY

Synopsis of Bill

The House Floor substitute for the House Judiciary Committee for House Bill 224 creates a new act titled the "Data Breach Notification Act" as a consumer protection measure. The bill provides for notice to be given to persons who are affected by a security breach involving their personally identifying information (PII). The measure 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.

HB 224 substitute contains requirements for:

- Disposing of records with PII once they are no longer reasonably needed for business purposes;
- Storage and protection of PII;

- Disclosing PII information under a contract with a service provider;
- Notification of a security breach, including requirements as to forms of required notification and time limits for such notification to consumers, including for users of computerized data with PII even if the information is not owned or licensed by the user;
- Elements to be included in notification of security breach;
- Notification to attorney general and credit reporting agencies, if more than one thousand residents are affected, not later than fourteen days after discovery;
- If the breach if of credit card or debit card numbers, provides for additional notification requirements, including notification to each merchant services provider within ten business days after discovery;
- Exempts those subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability Act of 1996.

HB 224 makes provisions for a law enforcement agency to withhold notification when it will impede a criminal investigation. It authorizes the attorney general to bring an action in the name of the state for violations of the act. The court may issue an injunction and award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses.

HB 224 authorizes, for knowing or reckless violations of the act, the court to impose a civil penalty of the greater of $5 thousand or $10 dollars per instance of failed notification up to a maximum of $150 thousand.

HB 224 makes provision for a card issuer to file a civil complaint against a merchant services provider whose retention of access device data constitutes a breach. The court may award reasonable costs that a card issuer incurs for:

- Cancelling or reissuing an access device;
- Stopping payments or blocking financial transactions to protect any account of the cardholder;
- Closing, reopening or opening any affected financial institution account of a cardholder;
- Refunding or crediting a cardholder for any financial transaction not authorized and that occurred as a result of the breach; or
- Notifying affected cardholders

However HB 224 exempts merchant services providers from such actions if that provider maintains security procedures that are in compliance with industry security standards as defined in Section 13B of the bill.

HB224 also states that if a data breach occurs and the user of the PII breached has its own notification procedures and these procedures are consistent with the timing requirements of Section 6, then the user is deemed to be in compliance with the notice requirements as long as the procedures are followed.

HB 224 defines the following terms: “access device,” “access device data,” “authorization process,” “breach of access device data,” “card issuer,” “cardholder,” “encryption,” “financial institution,” “financial transaction,” “merchant services,” “merchant services provider,” “personal identifying information,” “security breach,” “service provider,” and “proper disposal.”

FISCAL IMPLICATIONS

No fiscal impact on HDS, RLD or DoIT.

However, DoIT analysis states that in the case of a data breach, the fiscal impact to the agency could be significant, in both money expended and resources necessary to respond.

CYFD analysis similarly notes: "If CYFD data involving personal identifiers is stolen through a security breach, there is the potential for future liability." Also, "In the event of a security breach occurring as the result of computer systems compromised by an outside entity, 1 FTE will be required to research and correct any security deficiencies identified as a result of the breach."

SIGNIFICANT ISSUES

AGO analysis states: "New Mexico is only one of four states that do not have a data breach law on the books. Should this law be passed it would allow for the Attorney General to pursue *companies* [italics added for clarity] for restitution for consumers and civil penalties."

There is confusion as to whether HB 224 addresses security breaches by only private companies or if it is intended to include state agencies and other public bodies as well.

DoIt analysis also states that "This Act would be applicable to the systems that the state maintains."

DoIt analysis also states that if this law is enacted, it 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 New Mexico Administrative Code (NMAC) Rules specifically addressing this law. The bill dictates that "reasonable" measures are taken to protect and destroy PII. As the state CIO, the DoIT could set standards as to what is reasonable for state-owned systems.

DoIt analysis states: "For many state-owned systems that contain PII, there are already strict requirements that are set by the federal government, such as tax or health information. Additionally, the federal government is looking at legislation that would have similar regulations as this."

CYFD analysis states: "CYFD contracts include requirements to protect personal information as required by HIPPA and contract confidentiality clauses**."** If HB 224 is enacted, "CYFD will also require notification from contractors, vendors and third party providers of any data breach or loss involving personal identifying information."

HSD analysis states: "None for HSD. By exempting organizations that are subject to HIPAA, the committee substitute eliminates the original bill's primary issue."

PERFORMANCE IMPLICATIONS

DoIt analysis states "Overall, DoIT will continue to invest time and resources into security of state systems and PII. With this legislation, DoIT will work with all state agencies to ensure that processes are in place to respond to the requirements of this law. This bill may require DoIT to adapt its contract template that is used for all IT professional services contracts and Architecture requirements for IT Systems to better protect the state in the case of a Data Breach."

TRD analysis speaks to the performance implications of this bill: "As the Taxation and Revenue Department (TRD) collects and processes many elements of data considered personal identifying information, TRD will establish policies, procedures, and systems to comply. Procedures and processes should be set up to ensure that in the event of a security breach, the requirements of notification can be performed quickly. The Revenue Processing Division would need to review its procedures and policies on maintaining and protecting account information for taxpayers. They would also need to be concerned about the district offices who take the payment information over the phone to make tax payments. A strict set of rules and procedures should be developed and monitored to protect TRD from punitive damages."

OTHER SUBSTANTIVE ISSUES

Companies which fall under the regulations of The Gramm-Leach-Bliley Act are subject to The Safeguards Rule which covers PII collected by "financial institutions," a term that is broadly defined in the act and includes not only banks, 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 Health Insurance Portability Act of 1996 (HIPA) similarly protects PII related to health information and contains provision for both civil and criminal penalties for violations of its Privacy Rule(http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html) .

According to HSD analysis, the breach-related provisions of the Health Insurance Portability and Accountability ACT (HIPAA) and the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, which apply to HSD programs such as Medicaid, are more stringent than those of HB 224. The breach related provisions of personal identifying information (PII) data received from the Social Security Administration, the Internal Revenue Service, the Office of Child Support Enforcement, and the Centers for Medicare and Medicaid Services are more stringent than those of HB 224.

The National Conference of State Legislators (http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx) reports that forty-six 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.

AMENDMENTS

Depending on the intent of the legislation, the bill perhaps should be amended to clarify whether government agencies and other public bodies are subject to the statute.

DoIt Analysis recommends the following amendment to HB 224:

> The bill defines a security breach as ‘acquisition of...’ In many cases, entities will not be able to determine whether data were acquired/exfiltrated or not. The definition may be amended to ‘access to and/or acquisition of..’ or in the alternative, include a provision that in the event the entity cannot determine whether data were acquired but there is evidence of inappropriate access to the data, they are required to notify.” (N.B. “Data exfiltration is the unauthorized transfer of data from a computer.)

TRD analysis states: “This bill should not be limited to New Mexico residents only.”

CAC/jl