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

SPONSOR HJC **ORIGINAL DATE** 02/14/17 **LAST UPDATED** 03/10/17 **HB** 15/HJCS/aHFl#1/ aSPAC

SHORT TITLE Data Breach Notification Act **SB**

ANALYST Daly

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY17	FY18	FY19	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total		NFI	NFI			

(Parenthesis ( ) Indicate Expenditure Decreases)

SOURCES OF INFORMATION

LFC Files

Responses Received From (on Original Bill)

Department of Information Technology (DoIT)
Administrative Office of the Courts (AOC)
Office of the Attorney General (OAG)
Children, Youth & Families Department (CYFD)
Commission of Public Records (CPR)
Crime Victims Reparations Commission (CVRC)
Higher Education Department (HED)
Human Services Department (HSD)
New Mexico Corrections Department (NMCD)
New Mexico Retiree Health Care Authority (NMRHCA)
Public Employee Retirement Association (PERA)
Public Schools Insurance Authority (PSIA)
Regulation & Licensing Department (RLD)
Secretary of State (SOS)
Taxation & Revenue Department (TRD)

SUMMARY

Synopsis of SPAC Amendment

The Senate Public Affairs Committee amendment to the House Judiciary Committee Substitute for House Bill 15, as amended, clarifies in Section 7(G) that the notification to be given under that subsection to a person who is affected by a security breach is the affected persons's rights under the federal Fair Credit Reporting Act.

Synopsis of HFl#1Amendment

The House Floor Amendment # 1 to the House Judiciary Substitute for House Bill15 makes a non-substantive correction on page 5, line 21: it deletes the second comma.

Synopsis of Original Bill

The House Judiciary Committee Substitute for House Bill 15 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 that information (a) without the approval or direction of the cardholder or person impacted; (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 or person.

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, or unique biometric data, including fingerprints, voice print, or retina or iris image) 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)

HB 15 requires a person that owns or maintains 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 or sufficient contact information is on record. (Section 6)

Notice is not required, however, if the data owner or maintain or 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 bill 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 also must be given to OAG 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. (Section 10)

HB 15 also includes specific requirements for:

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

The bill exempts those subject to two federal laws: the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It also exempts the State of New Mexico and its political subdivisions (Sections 8, 12)

The bill authorizes OAG 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 $25,000 or $10 per instance of failed notification, up to a maximum of $150,000. (Section 11)

FISCAL IMPLICATIONS

Because the State (and its political subdivisions) is exempted in Section 12, no fiscal impact to the State is anticipated.

SIGNIFICANT ISSUES

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

TECHNICAL ISSUES

In its analysis of the original bill, TRD suggested these technical changes which may be applicable to this substitute:

- inserting "permanently" before "unreadable" now on page 4, line 5 to ensure proper disposal of PII is rendered permanently unusable; and
- expanding the definition of "security breach" to include possession and transmittal as well as acquisition now on page 3, line 7.

OTHER SUBSTANTIVE ISSUES

The HIPAA exemption in Section 8 removes HSD programs such as Medicaid and NMRHCA from liability under HB 15: HIPAA establishes national standards to protect individuals' medical records and other personal health information. Additionally, companies which fall under the regulations of the federal Gramm-Leach-Bliley Act (and are exempted in Section 8 as well) 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.

MD/al/jle