HOUSE BILL 15

53RD LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2017

INTRODUCED BY

William "Bill" R. Rehm

AN ACT

RELATING TO CONSUMER PROTECTION; CREATING THE DATA BREACH NOTIFICATION ACT; REQUIRING NOTIFICATION TO PERSONS AFFECTED BY A SECURITY BREACH INVOLVING PERSONAL IDENTIFYING INFORMATION; REQUIRING SECURE STORAGE AND DISPOSAL OF DATA CONTAINING PERSONAL IDENTIFYING INFORMATION; REQUIRING NOTIFICATION TO CONSUMER REPORTING AGENCIES, THE OFFICE OF THE ATTORNEY GENERAL AND CARD PROCESSORS IN CERTAIN CIRCUMSTANCES; PROVIDING CIVIL PENALTIES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

SECTION 1. [NEW MATERIAL] SHORT TITLE.--This act may be cited as the "Data Breach Notification Act".

SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the Data Breach Notification Act:

A. "encryption" means the use of an algorithmic

underscored material = new
[bracketed material] = delete

process to transform data into a form in which data elements are rendered unusable without the use of a confidential process or key;

B. "personal identifying information":

(1) means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable:

(a) social security number;

(b) driver's license number;

(c) government-issued identification number;

(d) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or

(e) unique biometric data, including the person's fingerprint, voice print or retina or iris image; and

(2) does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public;

C. "security breach" means the unauthorized acquisition of computerized data that compromises the security,

underscored material = new
[bracketed material] = delete

confidentiality or integrity of personal identifying information maintained by a person. "Security breach" does not include the good-faith acquisition of personal information by an employee or agent of a person for a legitimate business purpose of the person; provided that the personal identifying information is not subject to further unauthorized disclosure; and

D. "service provider" means any person that receives, stores, maintains, processes or otherwise is permitted access to personal identifying information through its provision of services directly to a person that is subject to regulation.

SECTION 3. [NEW MATERIAL] DISPOSAL OF PERSONAL IDENTIFYING INFORMATION.--A person that owns or maintains records containing personal identifying information of a New Mexico resident shall arrange for proper disposal of the records when they are no longer reasonably needed for business purposes. As used in this section, "proper disposal" means shredding, erasing or otherwise modifying the personal identifying information contained in the records to make the personal identifying information unreadable or undecipherable.

SECTION 4. [NEW MATERIAL] SECURITY MEASURES FOR STORAGE OF PERSONAL IDENTIFYING INFORMATION.--A person that owns or maintains personal identifying information of a New Mexico resident shall implement and maintain reasonable security

underscored material = new
[bracketed material] = delete

procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure.

SECTION 5. [NEW MATERIAL] SERVICE PROVIDER USE OF PERSONAL IDENTIFYING INFORMATION--IMPLEMENTATION OF SECURITY MEASURES.--A person that discloses personal identifying information of a New Mexico resident pursuant to a contract with a service provider shall require by contract that the service provider implement and maintain reasonable security procedures and practices appropriate to the nature of the personal identifying information and to protect it from unauthorized access, destruction, use, modification or disclosure.

SECTION 6. [NEW MATERIAL] NOTIFICATION OF SECURITY BREACH.--

A. Except as provided in Subsection C of this section, a person that owns or maintains elements that include personal identifying information of a New Mexico resident shall provide notification to each New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach. Notification shall be made in the most expedient time possible, but not later than thirty calendar days following discovery of the security breach, except as provided in Section 9 of the Data Breach Notification

underscored material = new
[bracketed material] = delete

Act.

B. Notwithstanding Subsection A of this section, notification to affected New Mexico residents is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.

C. Any person that maintains or possesses computerized data containing personal identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach in the most expedient time possible following discovery of the breach.

D. A person required to provide notification of a security breach pursuant to Subsection A of this section shall provide that notification by:

(1) United States mail;

(2) electronic notification, if the person required to make the notification primarily communicates with the New Mexico resident by electronic means or if the notice provided is consistent with the requirements of 15 U.S.C. Section 7001; or

(3) a substitute notification, if the person demonstrates that:

(a) the cost of providing notification would exceed one hundred thousand dollars ($100,000);

underscored material = new
[bracketed material] = delete

(b) the number of residents to be notified exceeds fifty thousand; or

(c) the person does not have on record a physical address for the residents that the person or business is required to notify.

E. Substitute notification pursuant to Paragraph (3) of Subsection D of this section shall consist of:

(1) sending electronic notification to the email address of those residents for whom the person has a valid email address;

(2) posting notification of the security breach in a conspicuous location on the website of the person required to provide notification if the person maintains a website; and

(3) sending written notification to the office of the attorney general and major media outlets in New Mexico.

F. A person that maintains its own notice procedures as part of an information security policy for the treatment of personal identifying information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a security breach.

SECTION 7. [NEW MATERIAL] NOTIFICATION--REQUIRED

underscored material = new
[~~bracketed material~~] = delete

CONTENT.--Notification required pursuant to Subsection A of Section 6 of the Data Breach Notification Act shall contain:

A. the name and contact information of the notifying person;

B. a list of the types of personal identifying information that are reasonably believed to have been the subject of a security breach, if known;

C. the date of the security breach, the estimated date of the breach or the range of dates within which the security breach occurred, if known;

D. a general description of the security breach incident;

E. the toll-free telephone numbers and addresses of the major consumer reporting agencies;

F. advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and

G. advice that informs the recipient of the notification of the recipient's rights pursuant to the Fair Credit Reporting and Identity Security Act.

SECTION 8. [NEW MATERIAL] EXEMPTIONS.--The provisions of the Data Breach Notification Act shall not apply to a person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996.

SECTION 9. [NEW MATERIAL] DELAYED NOTIFICATION.--The

underscored material = new
[bracketed material] = delete

notification required by the Data Breach Notification Act may be delayed:

A. if a law enforcement agency determines that the notification will impede a criminal investigation; or

B. as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.

SECTION 10. [NEW MATERIAL] NOTIFICATION TO ATTORNEY GENERAL AND CREDIT REPORTING AGENCIES.--A person that is required to issue notification of a security breach pursuant to the Data Breach Notification Act to more than one thousand New Mexico residents as a result of a single security breach shall notify the office of the attorney general and major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the security breach in the most expedient time possible, and no later than thirty calendar days, except as provided in Section 9 of the Data Breach Notification Act. A person required to notify the attorney general and consumer reporting agencies pursuant to this section shall notify the attorney general of the number of New Mexico residents that received notification pursuant to Section 6 of that act and shall provide a copy of the notification that was sent to affected residents within forty-five calendar days following discovery of the security breach, except as provided in Section

underscored material = new
[bracketed material] = delete

9 of the Data Breach Notification Act.

SECTION 11. [NEW MATERIAL] ADDITIONAL NOTIFICATION REQUIREMENTS FOR BREACH OF CREDIT CARD OR DEBIT CARD NUMBERS.--A person that is required to issue notification of a security breach pursuant to the Data Breach Notification Act as a result of a security breach involving a credit card number or debit card number shall notify each merchant services provider to which the person transmitted the credit card number or debit card number. Notification pursuant to this section shall be made within ten business days following discovery of the security breach.

SECTION 12. [NEW MATERIAL] ATTORNEY GENERAL ENFORCEMENT--CIVIL PENALTY.--

A. When the attorney general has a reasonable belief that a violation of the Data Breach Notification Act has occurred, the attorney general may bring an action on the behalf of individuals and in the name of the state alleging a violation of that act.

B. In any action filed by the attorney general pursuant to the Data Breach Notification Act, the court may:

(1) issue an injunction; and

(2) award damages for actual costs or losses, including consequential financial losses.

C. If the court determines that a person violated the Data Breach Notification Act knowingly or recklessly, the

underscored material = new
[bracketed material] = delete

court may impose a civil penalty of the greater of twenty-five thousand dollars ($25,000) or, in the case of failed notification, ten dollars ($10.00) per instance of failed notification up to a maximum of one hundred fifty thousand dollars ($150,000).

underscored material = new
[bracketed material] = delete