HOUSE JUDICIARY COMMITTEE SUBSTITUTE FOR
HOUSE BILL 224

51ST LEGISLATURE - STATE OF NEW MEXICO - SECOND SESSION, 2014

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 AN ACTION FOR CIVIL LIABILITY BY CARD ISSUERS FOR A BREACH OF ACCESS DEVICE DATA; 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:

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

A. "access device" means a credit card, debit card or other commercial instrument a cardholder receives from a card issuer for the purpose of electronically conducting a financial transaction;

B. "access device data" means:

(1) a cardholder account number printed or embossed on an access device;

(2) the contents of a magnetic stripe, including its tracks of data, a microprocessor chip or any other mechanism for storing electronically encoded information in an access device;

(3) a service code;

(4) a card verification value, card authentication value, card validation code or card security code for the access device; or

(5) a personal identification number for the access device;

C. "authorization process" means the verification of access device data and the verification of sufficiency of funds in a credit line or a financial institution account of a cardholder for completion of a financial transaction;

D. "breach of access device data" means the retention of an unencrypted cardholder account number or unencrypted service code or the retention of a card verification value, card authentication value, card validation code, card security code or personal identification number by a merchant services provider after the conclusion of the authorization process:

(1) without the approval or direction of the card issuer;

(2) resulting in the compromised security and confidentiality of access device data; and

(3) creating a material risk of harm or actual harm to a cardholder;

E. "card issuer" means a financial institution that issues an access device;

F. "cardholder" means a person to whom an access device has been issued by a card issuer;

G. "encryption" means the use of an algorithmic process to transform data into a form in which data elements are rendered unusable without the use of a confidential process or key;

H. "financial institution" means an insured state or national bank, a state or federal savings and loan association or savings bank or a state or federal credit union;

I. "financial transaction" means an interaction between two or more persons, by mutual agreement, involving a simultaneous creation or liquidation of a financial asset and the counterpart liability or a change in ownership of a financial asset or an assumption of a liability;

J. "merchant services" means processing, transmitting, retaining or storing access device data to facilitate a financial transaction that affects a cardholder's account;

K. "merchant services provider" means a person that engages in merchant services on the person's own behalf or for the benefit of another person;

L. "personal identifying information":

(1) means a person's first name or first initial and last name in combination with one or more of the following data elements that relate to the person, when the name and 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) date of birth; or

(e) 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; 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; and

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

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 to be retained. 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 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. [<u>NEW MATERIAL</u>] NON-AFFILIATED THIRD-PARTY 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 non-affiliated third party shall require by contract that the non-affiliated third party 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. [<u>NEW MATERIAL</u>] NOTIFICATION OF SECURITY BREACH.--

A. Except as provided in Subsection C of this section, a person that owns or maintains computerized data elements that include personal identifying information of a New Mexico resident shall provide notification to each New Mexico resident whose unencrypted 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 forty-five days following discovery of the security breach, except as provided in Section 9 of the Data Breach Notification 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 and, for such breaches that affect more than one thousand New Mexico residents, the person provides a written explanation of the determination to the attorney general.

C. A merchant services provider that maintains, on behalf of another person, computerized data elements that include personal identifying information of a New Mexico resident shall notify the person for which the data elements are maintained of any security breach in the most expedient time possible, but not later than ten days following discovery of the security 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 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);

(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 web site of the person required to provide notification if the person maintains a web site; and

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

SECTION 7. [NEW MATERIAL] NOTIFICATION--REQUIRED 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. a statement that notification was delayed pursuant to Section 9 of the Data Breach Notification Act, if a delay occurred;

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

G. advice that directs the recipient of the notification to review personal account statements and credit reports to detect errors resulting from the security breach; and

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

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

B. the notification will impede efforts 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 all 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, but not later than fourteen days following discovery of the security breach, 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, excluding any personal identifying information, within forty-five days following discovery of the security breach, except as provided in Section 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 credit card number or debit card number was transmitted. 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 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 incurred by a person entitled to notice, including consequential financial losses.

C. If the court determines that a person violated the Data Breach Notification Act knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars ($5,000) or ten dollars ($10.00) per instance of failed notification up to a maximum of one hundred fifty thousand dollars ($150,000).

SECTION 13. [NEW MATERIAL] BREACH OF ACCESS DEVICE DATA--CIVIL LIABILITY.--

A. A card issuer may file a civil complaint against a merchant services provider whose retention of access device data constitutes a breach of access device data. If the card issuer is the prevailing party, a court may award the reasonable costs that a card issuer incurs for:

(1) canceling or reissuing an access device;

(2) stopping payments or blocking financial transactions to protect any account of the cardholder;

(3) closing, reopening or opening any affected financial institution account of a cardholder;

(4) refunding or crediting a cardholder for any financial transaction that the cardholder did not authorize and that occurred as a result of the breach; or

(5) notifying affected cardholders.

B. A merchant services provider that maintains security procedures that are in compliance with security standards issued by the payment card industry security standards council, or a successor organization or, if none, by another nationally recognized organization that has published substantially similar guidelines that are generally accepted in the merchant services provider industry shall not be liable to a card issuer pursuant to this section.

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