

HOUSE FLOOR SUBSTITUTE FOR
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:

.197044.1

underscoring material = new
[bracketed material] = delete

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

5 B. "access device data" means:

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

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

12 (3) a service code;

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

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

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

22 D. "breach of access device data" means the
23 retention of an unencrypted cardholder account number or
24 unencrypted service code or the retention of a card
25 verification value, card authentication value, card validation

1 code, card security code or personal identification number by a
2 merchant services provider after the conclusion of the
3 authorization process:

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

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

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

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

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

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

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

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

.197044.1

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

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

8 L. "personal identifying information":

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

- 14 (a) social security number;
- 15 (b) driver's license number;
- 16 (c) government-issued identification
17 number; or
- 18 (d) account number, credit card number
19 or debit card number in combination with any required security
20 code, access code or password that would permit access to a
21 person's financial account; and

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

1 M. "security breach" means the unauthorized
2 acquisition of computerized data that compromises the security,
3 confidentiality or integrity of personal identifying
4 information maintained by a person. "Security breach" does not
5 include the good faith acquisition of personal information by
6 an employee or agent of a person for a legitimate business
7 purpose of the person; provided that the personal identifying
8 information is not subject to further unauthorized disclosure;
9 and

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

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

23 SECTION 4. [NEW MATERIAL] SECURITY MEASURES FOR STORAGE
24 OF PERSONAL IDENTIFYING INFORMATION.--A person that owns or
25 maintains personal identifying information of a New Mexico

.197044.1

1 resident shall implement and maintain reasonable security
2 procedures and practices appropriate to the nature of the
3 information to protect the personal identifying information
4 from unauthorized access, destruction, use, modification or
5 disclosure.

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

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

18 A. Except as provided in Subsection C of this
19 section, a person that owns or licenses computerized data
20 elements that include personal identifying information of a New
21 Mexico resident shall provide notification to each New Mexico
22 resident whose unencrypted personal identifying information is
23 reasonably believed to have been subject to a security breach.
24 Notification shall be made in the most expedient time possible,
25 but not later than forty-five days following discovery of the

.197044.1

1 security breach, except as provided in Section 9 of the Data
2 Breach Notification Act.

3 B. Notwithstanding Subsection A of this section,
4 notification to affected New Mexico residents is not required
5 if, after an appropriate investigation, the person determines
6 that the security breach does not give rise to a significant
7 risk of identity theft or fraud and, for such breaches that
8 affect more than one thousand New Mexico residents, the person
9 provides a written explanation of the determination to the
10 attorney general.

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

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

20 (1) United States mail;

21 (2) electronic notification, if the notice
22 provided is consistent with the requirements of 15 U.S.C.
23 Section 7001; or

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

.197044.1

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

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

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

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

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

13 (2) posting notification of the security
14 breach in a conspicuous location on the web site of the person
15 required to provide notification if the person maintains a web
16 site; and

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

20 F. A person that maintains its own notice
21 procedures as part of an information security policy for the
22 treatment of personal identifying information, and whose
23 procedures are otherwise consistent with the timing
24 requirements of this section, is deemed to be in compliance
25 with the notice requirements of this section if the person

1 notifies affected consumers in accordance with its policies in
2 the event of a security breach.

3 SECTION 7. [NEW MATERIAL] NOTIFICATION--REQUIRED

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

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

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

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

14 D. a general description of the security breach
15 incident;

16 E. a statement that notification was delayed
17 pursuant to Section 9 of the Data Breach Notification Act, if a
18 delay occurred;

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

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

25 H. advice that informs the recipient of the

.197044.1

1 notification of the recipient's rights pursuant to the Fair
2 Credit Reporting and Identity Security Act.

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

7 SECTION 9. [NEW MATERIAL] DELAYED NOTIFICATION.--The
8 notification required by the Data Breach Notification Act may
9 be delayed if:

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

12 B. the notification will impede efforts to
13 determine the scope of the security breach and restore the
14 integrity, security and confidentiality of the data system.

15 SECTION 10. [NEW MATERIAL] NOTIFICATION TO ATTORNEY
16 GENERAL AND CREDIT REPORTING AGENCIES.--A person that is
17 required to issue notification of a security breach pursuant to
18 the Data Breach Notification Act to more than one thousand New
19 Mexico residents as a result of a single security breach shall
20 notify the office of the attorney general and all consumer
21 reporting agencies that compile and maintain files on consumers
22 on a nationwide basis, as defined in 15 U.S.C. Section
23 1681a(p), of the security breach in the most expedient time
24 possible, but not later than fourteen days following discovery
25 of the security breach, except as provided in Section 9 of the

.197044.1

1 Data Breach Notification Act. A person required to notify the
 2 attorney general and consumer reporting agencies pursuant to
 3 this section shall notify the attorney general of the number of
 4 New Mexico residents that received notification pursuant to
 5 Section 6 of that act and shall provide a copy of the
 6 notification that was sent to affected residents, excluding any
 7 personal identifying information, within forty-five days
 8 following discovery of the security breach, except as provided
 9 in Section 9 of the Data Breach Notification Act.

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

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

22 A. When the attorney general has a reasonable
 23 belief that a violation of the Data Breach Notification Act has
 24 occurred, the attorney general may bring an action in the name
 25 of the state alleging a violation of that act.

.197044.1

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

- 3 (1) issue an injunction; and
4 (2) award damages for actual costs or losses,
5 including consequential financial losses.

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

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

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

- 20 (1) canceling or reissuing an access device;
21 (2) stopping payments or blocking financial
22 transactions to protect any account of the cardholder;
23 (3) closing, reopening or opening any affected
24 financial institution account of a cardholder;
25 (4) refunding or crediting a cardholder for

1 any financial transaction that the cardholder did not authorize
2 and that occurred as a result of the breach; or

3 (5) notifying affected cardholders.

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

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