

HOUSE BUSINESS AND EMPLOYMENT COMMITTEE SUBSTITUTE FOR
HOUSE BILL 217

52ND LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2015

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

.199713.2

underscoring material = new
[bracketed material] = delete

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

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

7 C. "personal identifying information":

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

13 (a) social security number;

14 (b) driver's license number;

15 (c) government-issued identification
16 number; or

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

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

25 D. "security breach" means the unauthorized

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

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

.199713.2

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 maintains elements that include
20 personal identifying information of a New Mexico resident shall
21 provide notification to each New Mexico resident whose
22 unencrypted personal identifying information is reasonably
23 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 calendar days following discovery

.199713.2

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

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

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

17 (1) United States mail;

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

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

25 (a) the cost of providing notification

.199713.2

1 would exceed one hundred thousand dollars (\$100,000);

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

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

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

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

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

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

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

.199713.2

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

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

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

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

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

12 D. a general description of the security breach
13 incident;

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

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

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

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

.199713.2

underscored material = new
[bracketed material] = delete

1 **SECTION 9. [NEW MATERIAL] DELAYED NOTIFICATION.**--The
2 notification required by the Data Breach Notification Act may
3 be delayed:

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

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

9 **SECTION 10. [NEW MATERIAL] NOTIFICATION TO ATTORNEY**
10 **GENERAL AND CREDIT REPORTING AGENCIES.**--A person that is
11 required to issue notification of a security breach pursuant to
12 the Data Breach Notification Act to more than one thousand New
13 Mexico residents as a result of a single security breach shall
14 notify the office of the attorney general and major consumer
15 reporting agencies that compile and maintain files on consumers
16 on a nationwide basis, as defined in 15 U.S.C. Section
17 1681a(p), of the security breach in the most expedient time
18 possible, and no later than forty-five calendar days, except as
19 provided in Section 9 of the Data Breach Notification Act. A
20 person required to notify the attorney general and consumer
21 reporting agencies pursuant to this section shall notify the
22 attorney general of the number of New Mexico residents that
23 received notification pursuant to Section 6 of that act and
24 shall provide a copy of the notification that was sent to
25 affected residents within forty-five days following discovery

.199713.2

underscored material = new
[bracketed material] = delete

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

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

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

15 A. When the attorney general has a reasonable
16 belief that a violation of the Data Breach Notification Act has
17 occurred, the attorney general may bring an action in the name
18 of the state alleging a violation of that act.

19 B. In any action filed by the attorney general
20 pursuant to the Data Breach Notification Act, the court may:
21 (1) issue an injunction; and
22 (2) award damages for actual costs or losses,
23 including consequential financial losses.

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

.199713.2

1 court may impose a civil penalty of the greater of five
2 thousand dollars (\$5,000) or, in the case of failed
3 notification, ten dollars (\$10.00) per instance of failed
4 notification up to a maximum of one hundred fifty thousand
5 dollars (\$150,000).

6 - 10 -
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25