

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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

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. "personal identifying information":

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

10 (a) social security number;

11 (b) driver's license number;

12 (c) government-issued identification
13 number;

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

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

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

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

underscored material = new
[bracketed material] = delete

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

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

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

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

.204682.1

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

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

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

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

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

.204682.1

underscoring material = new
[bracketed material] = delete

1 Act.

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

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

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

16 (1) United States mail;

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

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

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

.204682.1

underscored material = new
[bracketed material] = delete

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

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

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

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

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

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

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

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

.204682.1

underscored material = new
[bracketed material] = delete

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 SECTION 10. [NEW MATERIAL] NOTIFICATION TO ATTORNEY
9 GENERAL AND CREDIT REPORTING AGENCIES.--A person that is
10 required to issue notification of a security breach pursuant to
11 the Data Breach Notification Act to more than one thousand New
12 Mexico residents as a result of a single security breach shall
13 notify the office of the attorney general and major consumer
14 reporting agencies that compile and maintain files on consumers
15 on a nationwide basis, as defined in 15 U.S.C. Section
16 1681a(p), of the security breach in the most expedient time
17 possible, and no later than thirty calendar days, except as
18 provided in Section 9 of the Data Breach Notification Act. A
19 person required to notify the attorney general and consumer
20 reporting agencies pursuant to this section shall notify the
21 attorney general of the number of New Mexico residents that
22 received notification pursuant to Section 6 of that act and
23 shall provide a copy of the notification that was sent to
24 affected residents within forty-five calendar days following
25 discovery of the security breach, except as provided in Section
.204682.1

underscored material = new
[bracketed material] = delete

1 9 of the Data Breach Notification Act.

2 SECTION 11. [NEW MATERIAL] ADDITIONAL NOTIFICATION
3 REQUIREMENTS FOR BREACH OF CREDIT CARD OR DEBIT CARD NUMBERS.--

4 A person that is required to issue notification of a security
5 breach pursuant to the Data Breach Notification Act as a result
6 of a security breach involving a credit card number or debit
7 card number shall notify each merchant services provider to
8 which the person transmitted the credit card number or debit
9 card number. Notification pursuant to this section shall be
10 made within ten business days following discovery of the
11 security breach.

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

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

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

1 court may impose a civil penalty of the greater of twenty-five
2 thousand dollars (\$25,000) 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).