

Home / Legislation Listing / HB 15

2017 Regular Session - HB 15

ID
HB 15

Title
DATA BREACH NOTIFICATION ACT

Sponsor
William "Bill" R. Rehm

Current Location
Chapters

Text

Introduced (PDF) 12/15/16

Introduced (HTML) 12/15/16

HJC Committee Substitute 2/13/17

Final Version 4/06/17

- 1 Sponsors
- 2 Votes
- 1 Analysis
- 4 Committee Reports & Amendments
- 1 Floor Amendments
- 12 Actions
- 0 Gov. Vetoes

ActionText: HPREF [1] HCPAC/HJC-HCPAC [4] DP-HJC [5] DNP-CS/DP [6] fl/a- PASSED/H (68-0) [13] SPAC/SJC-SPAC [26] DP/a-SJC [29] DP [31] PASSED/S (40-0) [13] h/cncrd SGND BY GOV (Apr. 6) Ch. 36.
Key to Abbreviations
Legislative Days with Corresponding Calendar Days

Sent to HPREF - Referrals: HPREF

[1] Sent to HCPAC - Referrals: HCPAC/HJC

[4] HCPAC: Reported by committee with Do Pass recommendation

[5] HJC: Reported by committee with Do Not Pass but with a Do Pass recommendation on Committee Substitution

[6] House of Representatives Floor Amendment

[6] Passed in the House of Representatives - Y:68 N:0

[13] Sent to SPAC - Referrals: SPAC/SJC

[26] SPAC: Reported by committee with Do Pass recommendation with amendment(s)

[29] SJC: Reported by committee with Do Pass recommendation

[31] Passed in the Senate - Y:40 N:0

[13] House has concurred with Senate Amendments

Signed by Governor - Chapter 36 - Apr. 6

1 AN ACT
2 RELATING TO CONSUMER PROTECTION; CREATING THE DATA BREACH
3 NOTIFICATION ACT; REQUIRING NOTIFICATION TO PERSONS AFFECTED
4 BY A SECURITY BREACH INVOLVING PERSONAL IDENTIFYING
5 INFORMATION; REQUIRING SECURE STORAGE AND DISPOSAL OF DATA
6 CONTAINING PERSONAL IDENTIFYING INFORMATION; REQUIRING
7 NOTIFICATION TO CONSUMER REPORTING AGENCIES AND THE OFFICE OF
8 THE ATTORNEY GENERAL; PROVIDING CIVIL PENALTIES; EXEMPTING
9 NEW MEXICO AND ITS POLITICAL SUBDIVISIONS FROM COMPLIANCE
10 WITH THE DATA BREACH NOTIFICATION ACT.
11

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

13 SECTION 1. SHORT TITLE.--This act may be cited as the
14 "Data Breach Notification Act".

15 SECTION 2. DEFINITIONS.--As used in the Data Breach
16 Notification Act:

17 A. "biometric data" means a record generated by
18 automatic measurements of an identified individual's
19 fingerprints, voice print, iris or retina patterns, facial
20 characteristics or hand geometry that is used to uniquely and
21 durably authenticate an individual's identity when the
22 individual accesses a physical location, device, system or
23 account;

24 B. "encrypted" means rendered unusable, unreadable
25 or indecipherable to an unauthorized person through a

1 security technology or methodology generally accepted in the
2 field of information security;

3 C. "personal identifying information":

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

9 (a) social security number;

10 (b) driver's license number;

11 (c) government-issued identification
12 number;

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

17 (e) biometric data; and

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

22 D. "security breach" means the unauthorized
23 acquisition of unencrypted computerized data, or of encrypted
24 computerized data and the confidential process or key used to
25 decrypt the encrypted computerized data, that compromises the

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

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

13 SECTION 3. DISPOSAL OF PERSONAL IDENTIFYING
14 INFORMATION.--A person that owns or licenses records
15 containing personal identifying information of a New Mexico
16 resident shall arrange for proper disposal of the records
17 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
22 undecipherable.

23 SECTION 4. SECURITY MEASURES FOR STORAGE OF PERSONAL
24 IDENTIFYING INFORMATION.--A person that owns or licenses
25 personal identifying information of a New Mexico resident

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

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

15 **SECTION 6. NOTIFICATION OF SECURITY BREACH.--**

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

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

6 C. Any person that is licensed to maintain or
7 possess computerized data containing personal identifying
8 information of a New Mexico resident that the person does not
9 own or license shall notify the owner or licensee of the
10 information of any security breach in the most expedient time
11 possible, but not later than forty-five calendar days
12 following discovery of the breach, except as provided in
13 Section 9 of the Data Breach Notification Act; provided that
14 notification to the owner or licensee of the information is
15 not required if, after an appropriate investigation, the
16 person determines that the security breach does not give rise
17 to a significant risk of identity theft or fraud.

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

- 21 (1) United States mail;
- 22 (2) electronic notification, if the person
23 required to make the notification primarily communicates with
24 the New Mexico resident by electronic means or if the notice
25 provided is consistent with the requirements of 15 U.S.C.

1 Section 7001; or

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

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

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

8 (c) the person does not have on record
9 a physical address or sufficient contact information for the
10 residents that the person or business is required to notify.

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

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

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

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

23 F. A person that maintains its own notice
24 procedures as part of an information security policy for the
25 treatment of personal identifying information, and whose

1 procedures are otherwise consistent with the timing
2 requirements of this section, is deemed to be in compliance
3 with the notice requirements of this section if the person
4 notifies affected consumers in accordance with its policies
5 in the event of a security breach.

6 **SECTION 7. NOTIFICATION--REQUIRED CONTENT.--**

7 Notification required pursuant to Subsection A of Section 6
8 of the Data Breach Notification Act shall contain:

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

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

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

17 D. a general description of the security breach
18 incident;

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

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

25 G. advice that informs the recipient of the

1 notification of the recipient's rights pursuant to the
2 federal Fair Credit Reporting.

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

7 **SECTION 9. DELAYED NOTIFICATION.**--The notification
8 required by the Data Breach Notification Act may be delayed:

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

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

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

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

9 SECTION 11. ATTORNEY GENERAL ENFORCEMENT--CIVIL
10 PENALTY.--

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

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

- 18 (1) issue an injunction; and
19 (2) award damages for actual costs or
20 losses, including consequential financial losses.

21 C. If the court determines that a person violated
22 the Data Breach Notification Act knowingly or recklessly, the
23 court may impose a civil penalty of the greater of twenty-
24 five thousand dollars (\$25,000) or, in the case of failed
25 notification, ten dollars (\$10.00) per instance of failed

1 notification up to a maximum of one hundred fifty thousand
2 dollars (\$150,000).

3 SECTION 12. STATE OF NEW MEXICO AND POLITICAL
4 SUBDIVISIONS EXEMPTED.--Nothing in the Data Breach
5 Notification Act shall be interpreted to apply to the state of
6 New Mexico or any of its political subdivisions._____

HJC/HB 15
Page 10