Publications
July 18, 2017

SECURITY BREACH NOTIFICATION CHART - New Mexico

N.M. Stat. 57-12C-1 ***et seq.***

H.B. 15 (signed into law April 6, 2017)

Effective June 16, 2017

Application. Any person that owns or licenses elements that include PI of a New Mexico resident (collectively, Entity).

Security Breach Definition. Unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality, or integrity of PI maintained by a person.

- Good-faith acquisition of PI by an employee or agent of a person for a legitimate business purpose of the person is not a security breach, provided that the PI is not subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall notify each NM resident whose PI is reasonably believed to have been subject to a security breach.

- Notification to NM residents is not required if, after an appropriate investigation, the Entity determines that the security breach does not give rise to a significant risk of identity theft or fraud.

Notification to Consumer Reporting Agencies. If more than 1,000 NM residents are to be notified as a result of a single security breach, the Entity shall also notify major consumer reporting agencies in the most expedient time possible, and no later than 45 calendar days, except if delayed notification is permitted to determine the scope of the breach or for law enforcement investigation purposes.

Attorney General/Agency Notification. If more than 1,000 NM residents are to be notified as a result of a single security breach, the Entity shall also notify the Office of the Attorney General of the number of NM residents that received notification pursuant and shall provide a copy of the notification that was sent to affected residents within 45 calendar days following discovery of the security breach, except if delayed notification is permitted to determine the scope of the breach or for law enforcement investigation purposes.

Third-Party Data Notification. Any business that is licensed to maintain or possess computerized data containing PI of a New Mexico resident that the business does not own or license shall notify the owner or licensee of the security breach in the most expedient time possible, but not later than 45 calendar days following discovery of the breach, except if delayed notification is permitted to determine the scope of the breach or for law enforcement investigation purposes. However, notification to the owner or licensee of the PI is not required if, after an appropriate investigation, the business determines that the security breach does not give rise to a significant risk of identity theft or fraud.

Timing of Notification. Notification shall be made in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach. Notification may be delayed as necessary to determine

the scope of the security breach and restore the integrity, security, and confidentiality of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable:

- Social Security number;
- Driver's license number;
- Government-issued identification number;
- 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; or
- Biometric data.

"Personal information" does not include information lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public.

Notice Required. The notice shall include:

- The name and contact information of the notifying person;
- A list of the types of PI that are reasonably believed to have been the subject of a security breach, if known;
- 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;
- A general description of the security breach incident;
- The toll-free telephone numbers and addresses of the major consumer reporting agencies;
- Advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and
- Advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act.

The notice shall be provided by one of the following methods:

- United States mail;
- Electronic notification, if the Entity primarily communicates with the NM resident by electronic means or if the notice provided is consistent with the requirements of 15 U.S.C. Section 7001 (E-Sign Act)

Substitute Notice Available. If the Entity demonstrates that the cost of providing notification would exceed $100,000; or that the number of residents to be notified exceeds 50,000; or that the Entity does not have a physical address or sufficient contact information for the residents to be notified. Substitute notice shall consist of all of the following:

- Sending electronic notification to the email address of those residents for whom the Entity has a valid email address;
- Posting notification of the security breach in a conspicuous location on the website of the Entity, if the Entity maintains one; and
- Sending written notification to the Office of the Attorney General and major media outlets in New Mexico.

Exception: Own Notification Policy. An Entity that maintains its own notice procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of the statute is deemed to be in compliance if the Entity notifies affected consumers in

accordance with its policies in the event of a security breach.

Exception: Compliance with Other Laws.

- Statute does not apply to an Entity subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996.

Other Key Provisions:

- **Delay for Law Enforcement.** Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.
- **Attorney General Enforcement.** The Attorney General may bring an action for an injunction and damages.