Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Vermont

9 V.S.A. §§ 2430, 2435

S. 284 (signed into law May 18, 2006, Act 162). Amended by H. 254 (signed into law May 8, 2012, Act 109).

Effective May 8, 2012.

S. 513 (signed into law May 13, 2013)

Effective May 13, 2013

S. 73 (signed into law June 9, 2015)

Effective July 1, 2015

S. 110 (signed into law March 5, 2020)

Effective July 1, 2020

Application. Any data collector and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic PI (Entity), that owns or licenses computerized PI that includes PI concerning a VT resident.

Security Breach Definition. Unauthorized acquisition of electronic data or a reasonable belief of such unauthorized acquisition that compromises the security, confidentiality, or integrity of PI or login credentials maintained by an Entity.

- Does not include good-faith but unauthorized acquisition or access of PI or login credentials by an employee or agent of the Entity for a legitimate purpose of the Entity, provided that the PI or login credentials are not used for a purpose unrelated to the Entity's business or subject to further unauthorized disclosure.

To determine whether this definition applies, any Entity may consider the following factors (among others):

- Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
- Indications that the information has been downloaded or copied;
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- That the information has been made public.

Notification Obligation. An Entity shall notify affected individuals residing in VT that there has been a security breach following discovery or notification to the Entity of the breach.

- Notice of a security breach is not required if the Entity establishes that misuse of PI or login credentials is not reasonably possible and the Entity provides notice of the determination that the misuse of the PI or login credentials is not reasonably possible and a detailed explanation for said determination to the VT Attorney General or to the Department of Banking, Insurance, Securities, and Health Care Administration in the event that the Entity is a person or entity licensed or registered with the Department.

Notification to Consumer Reporting Agencies. In the event an Entity is required to provide notice to more than 1,000 residents of VT at one time, the Entity shall notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the Department of Banking, Insurance, Securities, and Health Care Administration.

Attorney General/Agency Notification. An Entity shall notify the Attorney General or Department of Financial Regulation of any breach within 14 business days of the date the Entity discovers the breach or the date the Entity provides notice to consumers, whichever is sooner.

Any Entity that has, prior to the breach, sworn in writing on a form and in a manner prescribed by the Attorney General that the Entity maintains written policies and procedures to maintain the security of PI and respond to breaches in a manner consistent with state law shall notify the Attorney General before providing notice to consumers. Notice to the Attorney General shall contain the date the breach occurred, the date the breach was discovered, the number of VT residents affected, if known, and a description of the breach. If the date of the breach is unknown, then the Entity shall send notice to the Attorney General or the Department as soon as the date becomes known.

The Entity shall provide a copy of the notice that was provided to consumers. An Entity may also send the Attorney General or Department a second copy of the notice to consumers that redacts the type of PI breached for any public disclosure of the breach.

If a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the Attorney General or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent.

Third-Party Data Notification. Any Entity that maintains or possesses computerized data containing PI of an individual residing in VT that the Entity does not own or license or any Entity that conducts business in VT that maintains or possesses records or data containing PI that the Entity does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.

Timing of Notification. Notice of the breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery of the breach, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Personal Information Definition. Vermont's statutory requirements apply to incidents involving "personally identifiable information or login credentials."

Personally identifiable information is an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted, redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

- Social Security number;
- Driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;
- Financial account number, credit card number, or debit card number if the number could be used without additional identifying information, access codes, or passwords;
- A password, personal identification number, or other access code for a financial account; unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
- Genetic information; and
- Health records or records of a wellness program or similar program of health promotion or disease prevention, a health care professional's medical diagnosis or treatment of the consumer, or a health insurance policy number

PI does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Login credentials means a consumer's username or email address, in combination with a password or an answer to a security question, that together permit access to an online account.

Notice Required. Notice of a security breach involving PI may be provided by one or more of the following methods:

- Written notice mailed to the individual's residence;
- Telephonic notice, provided that telephonic contact is made directly with each affected resident of VT, and not through a prerecorded message; or
- Electronic notice, for those individuals for whom the Entity has a valid email address if (i) the Entity's primary method of communication with the individual is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the individual provide PI, and the electronic notice conspicuously warns individuals not to provide PI in response to electronic communications regarding security breaches; or (ii) the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Generally. The notice to a consumer of a security breach involving PI shall be clear and conspicuous and include a description of each of the following, if known to the Entity:

- The incident in general terms;
- The type of PI that was subject to the security breach;
- The general acts of the Entity to protect the PI from further security breach;
- A telephone number (toll-free, if available) that the consumer may call for further information and assistance;
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and
- The approximate date of the security breach.

Online account credentials: If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account, the data collector shall provide notice of the security breach to the consumer electronically or through one or more of the methods described above and shall advise the consumer to take steps necessary to protect the online account, including to change his or her login credentials

for the account and for any other account for which the consumer uses the same login credentials.

Email account credentials: If a security breach is limited to an unauthorized acquisition of login credentials for an email account the data collector shall not provide notice of the security breach through the email account; and the data collector shall provide notice of the security breach through one or more of the methods described above or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an IP address or online location from which the data collector knows the consumer customarily accesses the account.

Substitute Notice Available. If the Entity demonstrates that the cost of providing written, email, or telephonic notice would exceed $10,000, or the Entity does not have sufficient contact information, substitute notice may be provided. Substitute notice shall consist of all of the following:

- Conspicuously posting the notice on the Entity's website, if the Entity maintains one; and
- Notifying major statewide and regional media.

Exception: Compliance with Other Laws.

- **Interagency Guidance.** A financial institution that is subject to the following guidance, and any revisions, additions, or substitutions relating to said interagency guidance shall be exempt from this section: (i) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or (ii) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration.
- **HIPAA-Covered Entities.** A data collector that is subject to the privacy, security, and breach notification rules adopted pursuant to the federal Health Insurance Portability and Accountability Act, is deemed to be in compliance with this subchapter if: (1) the data collector experiences a security breach that is limited to health records or records of a wellness program or similar program of health promotion or disease prevention, a health care professional's medical diagnosis or treatment of the consumer, or a health insurance policy number; and (2) the data collector provides notice to affected consumers pursuant to the requirements of the HIPAA breach notification rule.

Other Key Provisions:

- **Delay for Law Enforcement.** The required notice to a consumer shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or homeland security investigation, or jeopardize public safety or national or homeland security interests. In the event law enforcement makes the request in a manner other than in writing, the Entity shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The Entity shall provide the required notice without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.
- Attorney General Enforcement.
- Waiver Not Permitted.