Vermont

9 Vt. Stat. Ann. §2435

Quick Links

Statute

AG Website

Quick Facts

Is "Personal Information" broader than the general definition?[1]	✓ Yes
Does the law apply to paper records?	× No
Is notification triggered by access only?	× No
Is a risk-of-harm analysis permitted?	✓ Yes
Is notice to a state agency or AG required?	✓ Yes, within 14 business days of the entity's discovery of the security breach
Is there a specific deadline for individual notices?	✓ Yes, within 45 days following discovery or notification of the breach
Is there a specific format or language that must be included in the individual notice?	✓ Yes
Is a private right of action permitted?	× No

"Breach" Definition

The unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector.

"Personal Information" Definition

1. An individual's first name or first initial and last name in combination with one or more of the following:
   a. Social security number
   b. Driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that

[1] The general definition of "Personal Information" is an individual's name in combination with any one or more of the following: (1) Social Security number; (2) driver's license number or state identification card number; or (3) a financial account number or credit or debit card number in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account.

originates from a government identification document that is commonly used to verify identity for a commercial transaction

c. Financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords

d. Password, personal identification number, or other access code for a financial account

e. Unique biometric data used by the owner or licensee of the data to identify or authenticate the consumer

f. Genetic information, and

g. Health records or records of a wellness program or similar program of health promotion or disease prevention

h. Health care professional's medical diagnosis or treatment of the consumer, or

i. Health insurance policy number.

Notification Trigger

45 days following discovery or notification of the breach:

1. Entity that owns or licenses personal information shall disclose the breach to each state resident in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification,
2. Entity that does not own or have the right to license the personal information shall notify the owner or licensee immediately following discovery of the breach.

Risk-of-Harm Analysis Standard

Notice of a security breach is not required if the entity establishes that misuse of personally identifiable information or login credentials is not reasonably possible and the data collector provides notice of the determination that the misuse of the personally identifiable information or login credentials is not reasonably possible.

Special Form/Content of Consumer Notice

Notice shall be clear and conspicuous, and shall include a description of the following, if known to the data collector:

1. The incident in general terms.
2. The type of personally identifiable information that was subject to the security breach.
3. The general acts of the data collector to protect the personally identifiable information from further unauthorized access or acquisition.
4. A telephone number, toll-free if available, that the consumer may call for further information and assistance.
5. Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
6. The approximate date of the security breach.

AG Notice Trigger/Deadline

The entity shall notify the Attorney General or the Department, as applicable, of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days of the data collector's discovery of the security breach or when the data collector provides notice to consumers, whichever is sooner.

Notification to Consumer Reporting Agencies Threshold

In the event the entity provides notice to more than 1,000 consumers at one time, the data collector shall notify, without unreasonable delay, all consumer reporting agencies.