

Vermont Statutes Annotated
Title 9 – Commerce and Trade
Chapter 62 – Protection of Personal Information

§ 2430. Definitions. The following definitions shall apply throughout this chapter unless otherwise required:

(1) "Business" means a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this state, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but in no case shall it include the state, a state agency, or any political subdivision of the state.

(2) "Consumer" means an individual residing in this state.

(3) "Data collector" may include, but is not limited to, the state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

(4) "Encryption" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

(5) (A) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

- (i) Social Security number;
- (ii) Motor vehicle operator's license number or nondriver identification card number;
- (iii) Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
- (iv) Account passwords or personal identification numbers or other access codes for a financial account.

(B) "Personal information" does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(6) "Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

(7) "Redaction" means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

(8) (A) "Security breach" means unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition or access of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007.)

§ 2435. Notice of security breaches.

(a) This section shall be known as the Security Breach Notice Act.

(b) Notice of breach.

(1) Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized personal information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the breach shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of the law enforcement agency, as provided in subdivision (3) of this subsection, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any data collector that maintains or possesses computerized data containing personal information of a consumer that the business does not own or license or any data collector that conducts business in Vermont that maintains or possesses records or data containing personal information that the data collector 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 as provided in subdivision (3) of this subsection.

(3) The notice required by this subsection 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 data collector 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. A law enforcement agency shall promptly notify the data collector when the law enforcement agency no longer 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. The data collector shall provide notice required by this section 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.

(4) The notice shall be clear and conspicuous. The notice shall include a description of the following:

(A) The incident in general terms.

(B) The type of personal information that was subject to the unauthorized access or acquisition.

(C) The general acts of the business to protect the personal information from further unauthorized access or acquisition.

(D) A toll-free telephone number that the consumer may call for further information and assistance.

(E) Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

(5) For purposes of this subsection, notice to consumers may be provided by one of the following methods:

(A) Direct notice to consumers, which may be by one of the following methods:

(i) Written notice mailed to the consumer's residence;

(ii) Electronic notice, for those consumers for whom the data collector has a valid e-mail address if:

(I) the data collector does not have contact information set forth in subdivisions (i) and (iii) of this subdivision (5)(A), the data collector's primary method of communication with the consumer is by electronic means, the electronic notice

does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or

(II) the notice provided is consistent with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001; or

(iii) Telephonic notice, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message.

(B) Substitute notice, if the data collector demonstrates that the cost of providing written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision (5), to affected consumers would exceed \$5,000.00 or that the affected class of affected consumers to be provided written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision (5), exceeds 5,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and

(ii) notification to major statewide and regional media.

(c) In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), 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.

(d) (1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination that the misuse of the personal information is not reasonably possible pursuant to the requirements of this subsection. If the data collector establishes that misuse of the personal information is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personal information is not reasonably possible and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration in the event that the data collector is a person or entity licensed or registered with the department under Title 8 or this title. The

data collector may designate its notice and detailed explanation to the Vermont attorney general or the department of banking, insurance, securities, and health care administration as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in subdivision 317(c)(9) of Title 1.

(2) If a data collector established that misuse of personal information was not reasonably possible under subdivision (1) of this subsection, and subsequently obtains facts indicating that misuse of the personal information has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.

(e) Any waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

(f) A financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to said interagency guidance shall be exempt from this section:

(1) 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

(2) 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.

(g) Enforcement.

(1) With respect to all data collectors and other entities subject to this subchapter, other than a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title, the attorney general and state's attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the attorney general and state's attorney have under chapter 63 of this title. The attorney general may refer the matter to the state's attorney in an appropriate case. The superior courts shall have jurisdiction over any enforcement matter brought by the attorney general or a state's attorney under this subsection.

(2) With respect to a data collector that is a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title, the department of banking, insurance, securities and health care administration shall have the full authority to investigate

potential violations of this subchapter and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations adopted pursuant to this subchapter, as the department has under Title 8 or this title or any other applicable law or regulation.

Subsection (h) repealed effective June 30, 2008; see note set out below.

(h) Vermont law enforcement agencies, including the department of public safety, shall not be considered a data collector. Except as provided in subdivisions (b)(2) and (b)(3) of this section, Vermont law enforcement agencies, including the department of public safety, shall be exempt from this subchapter. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007.)

§ 2445. Safe destruction of documents containing personal information.

(a) As used in this section:

(1) "Business" means sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this state, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but in no case shall it include the state, a state agency, or any political subdivision of the state. The term includes an entity that destroys records.

(2) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(3) "Personal information" means the following information that identifies, relates to, describes, or is capable of being associated with a particular individual: his or her signature, Social Security number, physical characteristics or description, passport number, driver's license or state identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information.

(4) (A) "Record" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.

(B) "Record" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

(b) A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means for the purpose of:

- (1) ensuring the security and confidentiality of customer personal information;
- (2) protecting against any anticipated threats or hazards to the security or integrity of customer personal information; and
- (3) protecting against unauthorized access to or use of customer personal information that could result in substantial harm or inconvenience to any customer.

(c) An entity that is in the business of disposing of personal financial information that conducts business in Vermont or disposes of personal information of residents of Vermont must take all reasonable measures to dispose of records containing personal information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of personal information during or after the collection and transportation and disposing of such information.

(d) This section does not apply to any of the following:

- (1) Any bank, credit union, or financial institution as defined under the federal Gramm Leach Bliley law that is subject to the regulation of the Office of the Comptroller of the Currency, the Federal Reserve, the National Credit Union Administration, the Securities and Exchange Commission, the federal deposit insurance corporation, the office of thrift supervision of the U.S. department of the treasury, or the department of banking, insurance, securities, and health care administration and is subject to the privacy and security provisions of the Gramm Leach Bliley Act, 15 U.S.C. § 6801 et seq.
- (2) Any health insurer or health care facility that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.
- (3) Any consumer reporting agency that is subject to and in compliance with the Federal Credit Reporting Act, 15 U.S.C. § 1681 et seq., as amended.

(e) Enforcement.

- (1) With respect to all businesses subject to this section, other than a person or entity licensed or registered with the department of banking, insurance, securities and health care administration under Title 8 or this title, the attorney general and

state's attorney shall have sole and full authority to investigate potential violations of this section, and to prosecute, obtain and impose remedies for a violation of this section, or any rules adopted pursuant to this section, and to adopt rules under this act, as the attorney general and state's attorney have under chapter 63 of this title. The superior courts shall have jurisdiction over any enforcement matter brought by the attorney general or a state's attorney under this subsection.

(2) With respect to a person or entity licensed or registered with the department of banking, insurance, securities, and health care administration under Title 8 or this title to do business in this state, the department of banking, insurance, securities, and health care administration shall have full authority to investigate potential violations of this act, and to prosecute, obtain, and impose remedies for a violation of this act, or any rules or regulations made pursuant to this act, as the department has under Title 8 and this title, or any other applicable law or regulation.