MEMORANDUM

To: Joint Information Technology Oversight Committee
From: David P. Hall, Esq., Legislative Counsel
Date: September 20, 2019
RE: Security Breach Notice Act, 9 V.S.A. § 2435

Vermont, like all 50 states and several U.S. territories, imposes a statutory duty to notify consumers in the event of a data security breach. Codified at 9 V.S.A. § 2435, the "Security Breach Notice Act" governs this notification process.

What is a Security Breach?

A data collector must provide notice under the Act in the event of a "security breach"—the unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, which compromises the security, confidentiality, or integrity of a consumer's[1] personally identifiable information maintained by a data collector.[2]

What Type of Information Triggers the Duty to Notify?

The Act applies to a breach that involves "personally identifiable information," or "PII," which requires at least two elements:

[1] first name or first initial and last name; and

[2] an unencrypted SSN, driver's license/ID, financial account number, or financial account password or PIN.[3]

Who is a Data Collector Subject to the Act?

The duty to provide notice of a security breach applies to a "data collector"—any person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.[4]

[1] A "consumer" means an individual residing in Vermont.
[2] 9 V.S.A. § 2430(12).
[3] 9 V.S.A. § 2430(9).
[4] 9 V.S.A. § 2430(6).

What Notice Must a Data Collector Provide, To Whom, and When?

Unless law enforcement requests a delay pursuant to the Act, in the event of a security breach, a data collector must provide notice to consumers[5] and to either the Attorney General or to the Department of Financial Regulation, if regulated by DFR.[6] A data collector must also notify the nationwide credit reporting agencies if the breach affects 1,000 or more consumers.[7]

Notice to Consumers:

Timing[8] - A data collector must notify the consumer "in the most expedient time possible and without unreasonable delay, but not later than 45 days" after the discovery or notification of a breach.[9]

Content[10] - The notice to a consumer must be clear and conspicuous and include:

- the incident in general terms
- the type of PII involved
- the general acts of the data collector to protect the PII from further breach
- a telephone number to call for information and assistance, toll-free if available
- advice that directs the consumer

Form[11] - Notice to consumer may be by direct notice, or by substitute notice if allowed:

(A) Direct Notice:

(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'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 is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

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

---

[5] 9 V.S.A. § 2435(b)(1).
[6] 9 V.S.A. § 2430(b)(3).
[7] 9 V.S.A. § 2430(c).
[8] 9 V.S.A. § 2435(b)(1).
[9] If the data collector "maintains or possesses" PII but doesn't own or license it, the data collector must immediately notify the owner or licensee of the PII. 9 V.S.A. § 2435(b)(2).
[10] 9 V.S.A. § 2435(b)(5).
[11] 9 V.S.A. § 2435(b)(6).

(B)(i) Substitute notice, if:

(I) the data collector demonstrates that the cost of providing written or telephonic notice to affected consumers would exceed $5,000.00;

(II) the class of affected consumers to be provided written or telephonic notice exceeds 5,000; or

(III) the data collector does not have sufficient contact information.

(ii) A data collector provides substitute notice by:

(I) conspicuously posting the notice on the data collector's website if the data collector maintains one; and

(II) notifying major statewide and regional media.

Notice to Attorney General of Department of Financial Regulation[12]

Timing - A data collector must provide notice to the Attorney General (or to DFR if regulated by DFR) within 14 business days of discovering the breach or when the data collector notifies consumers, whichever is sooner.[13]

Content - Notice must include:

- the date of the breach[14]
- the date of discovery
- a preliminary description of the breach; and
- the number of Vermont consumers affected, if known; and
- a copy of the notice to consumers;
- optional – a redacted copy of the consumer notice (for public disclosures)

Notice to Consumer Reporting Agencies

If a data collector provides notice to more than 1,000 consumers at one time, the data collector shall notify, without unreasonable delay, all consumer reporting agencies of the timing, distribution, and content of the notice. (does not apply to a data collector regulated by DFR).[15]

[12] 9 V.S.A. § 2435(b)(3).

[13] A data collector can "prefile" a sworn writing to the AG that it maintains written policies and procedures to secure PII. If it does, the data collector must notify the AG of the date of the breach, the date of discovery, and provide a description prior to providing notice to consumers.

[14] If known. If not, the data collector must report the date once known.

[15] 9 V.S.A. § 2430(c).

Prohibition on Other Disclosures

The Act provides that, unless otherwise ordered by a court for good cause shown, a notice shall not be disclosed without the consent of the data collector to any person other than DFR, the AG's office, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities.[16]

Are there Exceptions to the Duty to Notify?

Notice of a security breach is not required if:

[1] the data collector establishes that misuse of personal information is not reasonably possible; and

[2] the data collector provides notice of the determination and a detailed explanation to the Attorney General or to the Department of Financial Regulation.[17]

A data collector that is subject to certain federal guidances specified in the Act are also exempt, though it must provide notice to DFR if regulated by it.[18]

[16] 9 V.S.A. § 2435(b)(3)(iv).

[17] 9 V.S.A. § 2435(d). If a data collector established 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 the Act.

[18] 9 V.S.A. § 2435(f).

Appendix – 9 V.S.A. §§ 2430; 2435

§ 2430. DEFINITIONS

As used in this chapter:

* * *

(3) "Consumer" means an individual residing in this State.

* * *

(6) "Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.

(7) "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.

(8) "License" means a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license.

(9)(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with any one or more of the following digital 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) "Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records.

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

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

(12)(A) "Security breach" means 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 maintained by a data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

(C) In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

(i) 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;

(ii) indications that the information has been downloaded or copied;

(iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the information has been made public.

* * *

§ 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 personally identifiable 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 security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection (b), or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable 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 subdivisions (3) and (4) of this subsection (b).

(3) A data collector or other entity subject to this subchapter shall provide notice of a breach to the Attorney General or to the Department of Financial Regulation, as applicable, as follows:

(A) A data collector or other entity regulated by the Department of Financial Regulation under Title 8 or this title shall provide notice of a breach to the Department. All other data collectors or other entities subject to this subchapter shall provide notice of a breach to the Attorney General.

(B)(i) The data collector 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, consistent with the legitimate needs of the law enforcement agency as provided in this subdivision (3) and subdivision (4) of this subsection (b), of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to this section, whichever is sooner.

(ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a data collector who, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personally identifiable information and respond to a breach in a manner consistent with Vermont law shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers pursuant to subdivision (1) of this subsection (b).

(iii) If the date of the breach is unknown at the time notice is sent to the Attorney General or to the Department, the data collector shall send the Attorney General or the Department the date of the breach as soon as it is known.

(iv) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (3)(B) shall not be disclosed to any person other than the Department, the authorized agent or representative of the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector.

(C)(i) When the data collector provides notice of the breach pursuant to subdivision (1) of this subsection (b), the data collector shall notify the Attorney General or the Department, as applicable, of the number of Vermont consumers affected, if known to the data collector, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection (b).

(ii) The data collector may send to the Attorney General or the Department, as applicable, a second copy of the consumer notice, from which is redacted the type of personally identifiable information that was subject to the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.

(4)(A) The notice to a consumer 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 for a delay 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 in writing 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.

(B) A Vermont law enforcement agency with a reasonable belief that a security breach has or may have occurred at a specific business shall notify the business in writing of its belief. The agency shall also notify the business that additional information on the security breach may need to be furnished to the Office of the Attorney General or the Department of Financial Regulation and shall include the website and telephone number for the Office and the Department in the notice required by this subdivision. Nothing in this subdivision shall alter the responsibilities of a data collector under this section or provide a cause of action against a law enforcement agency that fails, without bad faith, to provide the notice required by this subdivision.

(5) The notice to a consumer shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the data collector:

(A) the incident in general terms;

(B) the type of personally identifiable information that was subject to the security breach;

(C) the general acts of the data collector to protect the personally identifiable information from further security breach;

(D) a telephone number, toll-free if available, 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; and

(F) the approximate date of the security breach.

(6) A data collector may provide notice of a security breach to a consumer by one or more of the following methods:

(A) Direct notice, 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'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 is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

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

(B)(i) Substitute notice, if:

(I) the data collector demonstrates that the cost of providing written or telephonic notice to affected consumers would exceed $5,000.00;

(II) the class of affected consumers to be provided written or telephonic notice exceeds 5,000; or

(III) the data collector does not have sufficient contact information.

(ii) A data collector shall provide substitute notice by:

(I) conspicuously posting the notice on the data collector's website if the data collector maintains one; and

(II) notifying 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 Financial Regulation.

(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 (d). 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 Financial Regulation 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 Financial Regulation as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).

(2) If a data collector established that misuse of personal information was not reasonably possible under subdivision (1) of this subsection (d), 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) Except as provided in subdivision (3) of this subsection (f), a financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to an 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.

(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.

(3) A financial institution regulated by the Department of Financial Regulation that is subject to subdivision (1) or (2) of this subsection (f) shall notify the Department as soon as possible after it becomes aware of an incident involving unauthorized access to or use of personally identifiable information.

(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 Financial Regulation 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 Financial Regulation under Title 8 or this title, the Department of Financial Regulation 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.