9 V.S.A. § 2435

Current through Act Nos. 104 and M-21 of the 2023 Adjourned Session of the 2023-2024 Vermont General Assembly

Vermont Statutes Annotated > Title 9 Commerce and Trade (Pts. 1 — 8) > Part 3. Sales, Assignments, and Secured Transactions (Chs. 41 — 68) > Chapter 62. Protection of Personal Information (Subchs. 1 — 5) > Subchapter 2. Security Breach Notice Act (§ 2435)

§ 2435. Notice of security breaches

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

(b) Notice of breach.

(1) Except as otherwise provided in subsection (d) of this section, any data collector that owns or licenses computerized personally identifiable information or login credentials 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, 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 or login credentials 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 or login credentials 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.

(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 or login credentials 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 or login credentials that was subject to the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.

(D) 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.

(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 (4)(B). Nothing in this subdivision (4)(B) 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 (4)(B).

(5) The notice to a consumer required in subdivision (1) of this subsection shall be clear and conspicuous. A notice to a consumer of a security breach involving personally identifiable information 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 involving personally identifiable information 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 lowest cost of providing notice to affected consumers pursuant to subdivision (6)(A) of this subsection among written, e-mail, or telephonic notice would exceed $10,000.00; or

(II) 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 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 pursuant to the requirements of this subsection. If the data collector establishes that misuse of the personally identifiable information or login credentials is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personally identifiable information or login credentials 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 personally identifiable information or login credentials was not reasonably possible under subdivision (1) of this subsection, and subsequently obtains facts indicating that misuse of the personally identifiable information or login credentials has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.

(3) 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 specified in subdivision (b)(6) of this section 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.

(4) If a security breach is limited to an unauthorized acquisition of login credentials for an email account:

(A) the data collector shall not provide notice of the security breach through the email account; and

(B) the data collector shall provide notice of the security breach through one or more of the methods specified in subdivision (b)(6) of this section or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses the account.

(e) A data collector that is subject to the privacy, security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health Insurance Portability and Accountability Act, P.L. 104-191 (1996) is deemed to be in compliance with this subchapter if:

(1) the data collector experiences a security breach that is limited to personally identifiable information specified in 2430(10)(A)(vii); and

(2) the data collector provides notice to affected consumers pursuant to the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart D.

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

(g) Except as provided in subdivision (3) of this subsection, 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 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.

(h) 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.

(i) [Repealed.]

History

Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007; amended 2011, No. 109 (Adj. Sess.), § 4, eff. May 8, 2012; 2013, No. 29, §§ 10, 11, eff. May 13, 2013; 2013, No. 199 (Adj. Sess.), § 67; 2015, No. 55, § 8; 2019, No. 89 (Adj. Sess.), § 3.

End of Document