VERMONT
DEPARTMENT OF FINANCIAL REGULATION
89 Main Street, Montpelier, VT 05620 - 3101
(p) 802-828-3301 | http://www.dfr.vermont.gov/

Vermont's Security Breach Notice Act

Vermont's Security Breach Notice Act requires a data collector or other entity regulated by the Department of Financial Regulation to provide notice(s) of a security breach to (1) the Department and (2) the affected consumers or the owner or licensee of the data or records subject to the breach, in accordance with 9 V.S.A. §§ 2430 and 2435. All such entities should consult the Act and their own legal counsel to ensure compliance.

When providing a security breach notice to the Department, please direct it to:

Gavin Boyles, General Counsel
Department of Financial Regulation
89 Main St., Montpelier VT 05620-3101
DFR.SecurityBreach@vermont.gov
phone: 802-828-3301
fax: 802-828-1919

Frequently Asked Questions

Q. Am I required to notify the Department of Financial Regulation or the Attorney General's office about a security breach?

A. As mentioned above, the Security Breach Notice Act (9 V.S.A. § 2435) requires a data collector or other entity regulated by the Department of Financial Regulation to provide notice(s) of a security breach to:

(1) the Department of Financial Regulation, and
(2) to affected consumers or the owner or licensee of the data or records subject to the breach.

Data collectors and other entities not regulated by the Department of Financial Regulation are subject to the authority of the Attorney General; therefore, they do not need to notify the Department of Financial Regulation. For your convenience, here is a link to the Vermont Attorney General's Security Breach Notification Guidance.

Q. What are the notification requirements for a data collector or other entity that owns or licenses computerized personally identifiable information or login credentials and is regulated by the Department of Financial Regulation?

A. While the detailed notification requirements should be examined at 9 V.S.A. § 2435, the basic requirements include providing notice to the Department of Financial Regulation and to consumers as described below.

Preliminary Notice to the Department of Financial Regulation

A data collector or other entity regulated by the Department of Financial Regulation must provide a preliminary notice to the Department within **14 business days**[1] of discovery of the breach or at the time the data collector provides notice to consumers, whichever is sooner. The preliminary notice must include the date of the security breach[2] and the date of discovery of the breach.

Notice to Consumer and to Department of Financial Regulation

A data collector that owns or licenses computerized personally identifiable information or login credentials[3] must notify consumers that there has been a security breach as soon as possible, but not later than **45 days** after discovery or notification of the security breach.[4] The notice and methods of notice to the consumers must comply with 9 V.S.A. § 2435(b). When the data collector provides notice to the consumer, the data collector must notify the Department of the number of Vermont consumers affected, if known, and must provide the Department with a copy of the consumer notice.[5]

Q. What information must be included in the notice to the consumer?

A. According to 9 V.S.A. § 2435(b), the notice must be clear and conspicuous and include the following information:

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 security breach;
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; and
6) the approximate date of the security breach.

---

[1] Consistent with the legitimate needs of the law enforcement agency. 9 V.S.A. § 2435(b).

[2] 9 V.S.A. § 2435(b)(3)(B)(iii) requires that, if the date of the breach is unknown at the time notice is sent, the data collector must send the Department of Financial Regulation the date of the breach as soon as it is known.

[3] "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 Department of Financial Regulation . . . if the login credentials were acquired directly from the data collector or its agent." 9 V.S.A. § 2435(b)(3)(D).

[4] Consistent with the legitimate needs of the law enforcement agency. 9 V.S.A. § 2435(b).

[5] 9 V.S.A. § 2435(b)(3)(C)(ii) allows that the data collector may send a second redacted copy consumer notice for the Department of Financial Regulation to use for any public disclosure.

Q. What are the notification requirements for a data collector or other entity that maintains or possesses data or records containing personally identifiable information or login credentials and is regulated by the Department of Financial Regulation?

A. While the detailed notification requirements should be examined at 9 V.S.A. § 2435, the basic requirements include providing notice to the Department and to the owner or licensee of the data or records containing personally identifiable information or login credentials as follows:

Preliminary Notice to the Department of Financial Regulation

A data collector or other entity regulated by the Department must provide a preliminary notice to the Department within 14 business days[6] of discovery of the breach or at the time the data collector provides notice to consumers, whichever is sooner. The preliminary notice must include the date of the security breach[7] and the date of discovery of the breach.

Notice to the Owner or Licensee of the Information

A data collector or other entity that maintains or possesses records or data containing personally identifiable information or login credentials that the data collector does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.[8, 9]

Q. Do I have to provide notice if misuse of the personally identifiable information or login credentials is not reasonably possible?

A. According to 9 V.S.A. § 2435(d)(1), a data collector or entity is not required to notify consumers of a breach if it (1) determines that misuse of the personally identifiable information or login credentials is not reasonably possible and (2) provides notice of its determination and a detailed explanation for it to the Department of Financial Regulation.[10]

If a data collector or other entity later becomes aware of facts indicating that misuse of the personally identifiable information or login credentials has occurred or is occurring, it shall provide notice of the security breach to consumers in accordance with the requirements of 9 V.S.A. § 2435(b).

Q. What are the notice requirements for 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)?

---

[6] Consistent with the legitimate needs of the law enforcement agency. 9 V.S.A. § 2435(b).

[7] 9 V.S.A. § 2435(b)(3)(B)(iii) requires that, if the date of the breach is unknown at the time notice is sent, the data collector must send the Department of Financial Regulation the date of the breach, as soon as it is known.

[8] 9 V.S.A. § 2435(b)(2).

[9] Consistent with the legitimate needs of the law enforcement agency. 9 V.S.A. § 2435(b).

[10] The data collector may designate its notice and detailed explanation (or part of it) as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9). Blanket declarations that the entire notice is a trade secret are disfavored.

A. According to 9 V.S.A. § 2435(e), such a data collector is deemed to be in compliance with the Vermont Security Breach Notice Act if:

1) the data collector experiences a security breach that is limited to personally identifiable information specified in 9 V.S.A. § 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.

Q. Have there been any recent amendments to Vermont's Security Breach Notice Act?

A. Yes. Amendments to Vermont's Security Breach Notice Act became effective on July 1, 2020. The Department of Financial Regulation bulletin explaining the changes can be found here. Amendments to the Act are relatively frequent and entities should consult with counsel and review the most current version of the Act to ensure compliance.

Q. Am I a "data collector"? What is a "security breach"? What is "personally identifiable information"?

A. Please refer to 9 V.S.A. § 2430 for the statutory definitions of terms including "data collectors," "security breach," "login credentials," and "personally identifiable information."

Q. Where should I direct additional questions regarding Department of Financial Regulation security breach notice(s)?

A. All other security breach notice questions should be directed to:

Gavin Boyles, General Counsel
Department of Financial Regulation
89 Main St., Montpelier VT 05620-3101
DFR.SecurityBreach@vermont.gov
phone: 802-828-3301
fax: 802-828-1919