VERMONT'S SECURITY BREACH NOTICE ACT (9 V.S.A. § 2435)

PREPARED BY THE OFFICE OF LEGISLATIVE COUNSEL

WHAT IS A "SECURITY BREACH"? (9 V.S.A. § 2430)

(13)(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 or login credentials maintained by a data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are 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 or login credentials have 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. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007; amended 2011, No. 109 (Adj. Sess.), § 4, eff. May 8, 2012; 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019; 2019, No. 89 (Adj. Sess.), § 2.)

WHO IS A "DATA COLLECTOR"? (9 V.S.A. § 2430)

(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.

WHAT IS "PERSONALLY IDENTIFYING INFORMATION"? (9 V.S.A. § 2430)

(10)(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) a Social Security number;

(ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;

(iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;

(iv) a password, personal identification number, or other access code for a financial account;

(v) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vi) genetic information; and

(vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention;

(II) a health care professional's medical diagnosis or treatment of the consumer; or

(III) a health insurance policy number.

WHAT ARE "LOGIN CREDENTIALS? (9 V.S.A. § 2430)

(9) “Login credentials” means a consumer’s user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account.

BACK TO THE SECURITY BREACH NOTICE ACT...

WHEN MUST NOTICE BE PROVIDED?

- It depends on who is being notified:
  - **Consumers** (whose PII has been compromised) must be notified by the data collector not later than 45 days* after discovery or notification of the breach (a copy must be sent to the Attorney General)
    - This 45-day timeline can be delayed through a request from law enforcement
  - The **Attorney General** (or **Department of Financial Regulation** if it's a data collector governed by DFR), must be given "preliminary notification" by the data collector not later than 14 business days* after discovery or notification of the breach
    - This 14 business day timeline is waived for data collectors that previously submitted a sworn affirmation to the AG's office

WHEN IS IT NOT REQUIRED TO PROVIDE NOTICE?

(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).

ENFORCEMENT FOR VIOLATIONS

This Act is governed by the Vermont Consumer Protection Act. It provides for injunctive relief + $10,000 fine per violation.

(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.

This is from a publicly-available AG guidance document (source):

6. I THINK I'VE SUFFERED A SECURITY BREACH, WHAT SHOULD I DO?

You, as a business or state agency, should take the following steps if you think you may have suffered a security breach. Review all steps immediately, and take as many of the steps as possible, as quickly as possible. Each step is described more fully below in Detailed Explanations.

SECURE THE DATA **IMMEDIATELY**

Take reasonable steps to stop ongoing data theft, ideally without destroying evidence that could be used in a future investigation. For example, you can secure the data by disconnecting affected computers from networks or removing affected hard drives.

See also Section 22 ("Securing your data post-breach")

INVOLVE LAW ENFORCEMENT **IMMEDIATELY**

See Section 23 ("Contacting Law Enforcement").

IF YOU ARE STORING SOMEONE ELSE'S DATA, CONTACT THE OWNER OF THE DATA **IMMEDIATELY**.

See Sections 12 ("'Maintains or possesses'"), 18 ("Who must be notified in the event of a security breach?").

PROVIDE CONFIDENTIAL PRELIMINARY NOTICE TO THE ATTORNEY GENERAL OR DFR ABOUT THE BREACH **WITHIN 14 DAYS**.[vii]

See Section 25 ("14-day Preliminary Notice").

NOTIFY CONSUMERS ABOUT THE BREACH **IN THE MOST EXPEDIENT TIME POSSIBLE AND NOT LATER THAN 45 DAYS** AFTER DISCOVERY OR NOTIFICATION.[viii]

The most expedient time possible will often be much quicker than 45 days.

See Section 27 ("Consumer Notice").

NOTIFY THE THREE MAJOR CREDIT REPORTING AGENCIES IF YOU ARE GOING TO SEND A NOTICE OF SECURITY BREACH TO MORE THAN 1,000 CONSUMERS.[ix]

See Section 34 ("Contacting the credit reporting agencies").