VERMONT

**State of Vermont**
**Department of Financial Regulation**
89 Main Street
Montpelier, VT 05620-3101

For consumer assistance:
[Banking] 888-568-4547
[Insurance] 800-964- 1784
[Securities] 877-550-3907
**www.dfr.vermont.gov**

# Vermont Department of Financial Regulation
# Bulletin # 4
## *Security Breach Notice Act Bulletin*

**June 5, 2020**
**This Bulletin supersedes and replaces DFR Bulletin # 3**

### I. Purpose of the Bulletin

The purpose of this bulletin is to notify entities regulated by the Department of Financial Regulation of changes to the Security Breach Notice Act[1] produced by the enactment of Act 89, An Act Relating to Data Privacy and Consumer Protection.[2] These changes are effective as of July 1, 2020. Specifically, Act 89 expands the definitions of personally identifiable information and security breach, creates a notification process for login credential breaches, and changes the substitute notice requirements.

### II. Definition of Personally Identifiable Information ("PII")

Act 89 expands the definition of PII to include additional data elements such as additional government-provided identification numbers, biometric data, genetic information, and health records. The expanded definition of PII is found at 9 V.S.A. § 2430.

Prior to the change, PII meant a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when not redacted, encrypted or protected by another method that renders it unreadable or unusable by an unauthorized person:

[1] 9 V.S.A. § § 2430 and 2435.

[2] 2019, No. 89 (Adj. Sess.). This Bulletin is intended for general notification purposes only. Affected companies and individuals should review the actual language of the statutory provisions.

- Social Security number;
- Driver license or nondriver identification card number;
- Financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; or
- Password, personal identification number, or other access code for a financial account.

The amended definition of PII includes these elements and adds the following digital data elements, when not redacted, encrypted, or protected by another method that renders the data unreadable or unusable by an unauthorized person:

- 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;
- 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;
- Genetic information; and
- Health records or records of a wellness program or similar program of health promotion or disease prevention; a health care professional's medical diagnosis or treatment of the consumer; or a health insurance policy number.[3]

## III. Login Credential Security Breach

Act 89 expands the definition of security breach to include an unauthorized acquisition, or a reasonable belief of an unauthorized acquisition, of electronic data that compromises the security, confidentiality, or integrity of a consumer's *login credentials* maintained by a data collector.[4]

---

[3] Pursuant to 9 V.S.A. § 2453(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) ("HIPAA") is deemed to be in compliance with the Vermont Security Breach Notice Act if it experiences a security breach that is limited to personally identifiable information specified in 9 V.S.A. § 2430(10)(A)(vii) and it provides notice to affected consumers pursuant to the HIPAA breach notification rules.

[4] Definitions for the terms "security breach," "login credentials," and "data collector" are found at 9 V.S.A. § 2430.

A data collector experiencing a security breach limited to login credentials must comply with the same requirements for notice to the Department of Financial Regulation as a data collector experiencing a security breach involving PII.[5] Security breaches limited to login credentials differ from those involving PII regarding the required notice to consumers.

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 direct or substitute notice[6] 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. 9 V.S.A. § 2435(d)(3).

If a security breach is limited to an unauthorized acquisition of login credentials for an email account, the data collector shall not provide notice of the security breach through the email account, but shall provide notice of the security breach through direct or substitute notice[7] 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. 9 V.S.A. § 2435(d)(4).

## IV. Substitute Notice

Act 89 changes the requirements for substitute notice (as opposed to direct notice), such that substitute notice is only permitted where the *lowest* cost of providing direct notice via writing, email, or telephone would exceed $10,000 or the data collector does not have sufficient contact information for affected consumers. In addition, substitute notice is no longer permitted where the number of consumers exceeds 5,000. 9 V.S.A. § 2435(b)(6)(B).

M. M

Michael S. Pieciak
Commissioner of Financial Regulation

6/5/2020

Date

[5] See requirements at 9 V.S.A. § 2435(b). Note that, pursuant to 9 V.S.A. § 2435(b)(3)(D), a data collector is only required to provide notice of such a security breach to the Department of Financial Regulation if the login credentials were acquired directly from the data collector or its agent.

[6] See 9 V.S.A. § 2435(b)(6).

[7] See 9 V.S.A. § 2435(b)(6).