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

www.dfr.vermont.gov

Vermont Department of Financial Regulation
DFR Bulletin Number 3

Security Breach Notice Act Bulletin

I. Purpose of the Bulletin

The purpose of this Bulletin is to summarize the amendments to the notice requirements in the Security Breach Notice Act, (the "Act"), codified at 9 V.S.A. § 2435(b) and (f), and effective May 13, 2013. This Bulletin also amends and updates statutory references pertaining to the notice requirements contained in a previous Bulletin issued by the Department, entitled, BISHCA Bulletin Number 1, dated December 21, 2007.

Financial institutions and other entities regulated by the Department under Titles 8 or 9 are no longer exempt from the notice requirements of the Act. Specifically, the amendments apply to Department regulated entities that are "data collectors," and include, but are not limited to: financial institutions; licensed lenders; banks; credit unions; trust companies; insurance companies; captive insurance companies; debt adjusters; investment advisers; broker-dealers; and any other public or private corporation, limited liability company or business regulated by the Department. (See 9 V.S.A. § 2430(3) for the definition of "data collector" which is also cited to below).

II. Changes to Security Breach Notice Requirements for Financial Institutions and other entities regulated by the Department of Financial Regulation - Effective May 13, 2013

Businesses and entities defined as "data collectors," which store or handle an individual's nonpublic personal information, must give notice to the Department of Financial Regulation, as applicable, of any electronic data security breaches that compromise a consumer's nonpublic personally identifiable information.

Data collector is defined at 9 V.S.A. § 2430(3) and "may include, but is not limited to, the state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information."

Financial institutions and other entities regulated by the Department and defined as a "data collector" that were previously exempt from the reporting requirements of the Act, must now provide notice of electronic data security breaches to the Department pursuant to 9 V.S.A. § 2435(b)(3). Department regulated entities subject to the Act must report security breaches to the Department within 14 business days of the data collector's discovery of the breach or when the data collector provides notice to consumers, whichever is sooner. Such notice must also be consistent with the legitimate needs of law enforcement.

In addition, ***Department regulated financial institutions subject to the federal guidance documents listed in the Act at 9 V.S.A. § 2435(f)(1) or (f)(2) are no longer exempt from security breach notice requirements.*** Newly added Section 2435(f)(3) now requires that a Department regulated financial institution subject to 2435(f)(1) or (2), "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."

III. Meaning of "Personally Identifiable Information" and "Security Breach" under the Act

"Personally identifiable information" defined at 9 V.S.A. § 2430(5)(A) means an individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Motor vehicle operator's license number or non-driver identification card number;
- 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;
- Account passwords or personal identification numbers or other access codes for a financial account.

Personally identifiable information does not include public information that is lawfully made available to the general public, for example in public government (federal, state, or local) records. See 9 V.S.A. § 2430(5)(B).

Security breach as defined in Section 2430(8)(A) 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 the data collector."

However, a security breach, for purposes of the statute, "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." Section 2430(8)(B).

To further define a security breach, Section 2430(8)(C) was enacted in 2011, and was effective May 8, 2012. This Section provides:

"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."

IV. Summary of the amendments to the Security Breach Notice Act's Notice Requirements

Financial institutions and other entities regulated by the Department of Financial Regulation under Titles 8 and 9 are now required to provide notice of security breaches of nonpublic personally identifiable information to the Department. Such entities include, but are not limited to: financial institutions; licensed lenders; banks; credit unions; trust companies; insurance companies; captive insurance companies; debt adjusters; investment advisers; broker-dealers; and any other public or private corporation, limited liability company or business regulated by the Department. Other entities that are not regulated by the Department but are otherwise subject to the Act will continue to report any such security breaches to the Attorney General as before.

The notice requirements to the Department or to the Attorney General, as applicable, are in addition to notice and reporting requirements of security breaches to affected consumers under the Act, and to law enforcement officials, and in accordance with any federal regulations that apply.

Susan L. Donegan, Commissioner

August 6, 2013
Date