H.429

Introduced by Representative Botzow of Pownal

Referred to Committee on

Date:

Subject: Commerce and trade; consumer protection; cyber security

Statement of purpose of bill as introduced: This bill proposes to enhance and clarify reporting requirements and protocols in the event of a breach of electronic consumer data.

An act relating to enhancing consumer cyber security

It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 9 V.S.A. chapter 62 is amended to read:

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

* * *

§ 2430. DEFINITIONS

~~The following definitions shall apply throughout this chapter unless otherwise required~~ As used in this chapter:

(1) "Authentication" means verifying that a user, computer, or service, such as an application provide on a network server, is the entity that it claims to be.

(2) "Business" means a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this state, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but in no case shall it include the state, a state agency, or any political subdivision of the state.

(3) "Card network" means a credit or debit card network that processes one million or more credit or debit cards.

~~(2)~~(4) "Consumer" means an individual residing in this state.

~~(3)~~(5) "Data collector" 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.

~~(4)~~(6) "Encryption" means use of:

(A) an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key; or

(B) an alternate technology or process that provides equivalent or superior protection of the security, confidentiality, and integrity of data, that technology or process.

~~(5)(A) "Personally identifiable information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:~~

~~(i) Social Security number;~~

~~(ii) Motor vehicle operator's license number or nondriver identification card number;~~

~~(iii) 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;~~

~~(iv) Account passwords or personal identification numbers or other access codes for a financial account.~~

~~(B) "Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.~~

(7) "Licenses" in the context of electronic personally identifiable information means that as a result of a relationship with the owner of the

personally identifiable information that permits use of the personally identifiable information, the data collector receives, stores, maintains, processes, or otherwise has access to a consumer's personally identifiable information.

(8) "Owns" in the context of electronic personally identifiable information means that, as a result of a direct relationship with the consumer, the data collector receives, stores, maintains, processes, or otherwise has access to a consumer's personally identifiable information in connection with the provision of goods or services or in connection with employment.

(9) "Password information" means any information or compilation of information when either the identifier or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons, that includes an individual's first name, first initial and last name, e-mail address, or other login credential in combination with any security code, access code, or password. Password information does not include an individual's compilation of his or her own passwords.

(10) "Personally identifiable information" means any information or compilation of information when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons, that includes:

(A) An individual's first name or first initial and last name, or email address in combination with any one of the following data elements:

(i) a nontruncated Social Security number, motor vehicle operator's license number, non-driver identification card number, passport number, or alien registration number, or other government-issued unique identification number if misuse of this number is reasonably possible;

(ii) unique biometric data when used for authentication, such as a finger print, voice print, retina image, or iris image; or

(iii) a unique financial account identifier, including a financial account number or credit or debit card number, policy number, electronic identification number, user name, or routing code.

(B) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code in combination with any security code, access code, or password, that is required for a person to obtain credit, withdraw funds, or engage in a financial transaction.

(C) Unless otherwise specified, password information.

~~(6)~~(11) "Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(7)~~(12) "Redaction" means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

~~(8)(A)~~(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 maintained by the data collector.

(B) "Security breach" 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.

(C) "Security breach" does not include circumstances where password information was obtained from a source other than the data collector, including from the consumer through subterfuge, such as phishing.

(D) 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.

* * *

§ 2435. NOTICE OF SECURITY BREACHES

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

(b) Notice of breach.

(1)(A) Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach.

(B) 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.

(C) Where multiple data collectors are affected by the same security breach involving the same personally identifiable information, only one data collector need provide notice to consumers, provided, however, that this does not alter the obligation of all affected data collectors to provide notice to the Attorney General's office and to the Department of Financial Regulation, as applicable, pursuant to subdivision (3) of this subsection.

(2) Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer 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 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~~, other than a person or entity licensed or registered with the department of financial~~

~~regulation under Title 8 or this title,~~ shall provide notice of a breach to the ~~attorney general's~~ Attorney General's office as follows:

(A) A data collector or other entity licensed or registered with the Department of Financial Regulation under Title 8 of the Vermont Statutes Annotated shall provide notice of a security breach to the Department. All other data collectors and entities subject to this chapter shall provide notice of a security breach to the Attorney General's office.

~~(A)(i)~~(B)(i) The data collector shall notify the ~~attorney general~~ 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 subdivisions (3) and (4) of this subsection, 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 ~~(A)(i)~~(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 office of the ~~attorney general~~ 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 and respond to a breach in a manner consistent with Vermont law shall notify the

~~attorney general~~ 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.

(iii) If the date of the breach is unknown at the time notice is sent to the ~~attorney general~~ Attorney General, the data collector shall send the ~~attorney general~~ Attorney General 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)(A) shall not be disclosed to any person other than the Department, the authorized agent or representative of the ~~attorney general~~ Attorney General, a ~~state's attorney~~ State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector.

~~(B)(i)~~(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~~ Attorney General 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~~ Attorney General a second copy of the consumer notice, from which is redacted the type of personally identifiable information that was subject to the breach, and which

the ~~attorney general~~ Attorney General shall use for any public disclosure of the breach.

(4)(A) The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency.

(B) 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.

(C) In the event law enforcement makes the request 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.

(D) A law enforcement agency shall promptly notify the data collector 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.

(E) 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.

(5) The notice to a consumer shall be clear and conspicuous. The notice 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.~~

~~(F) The approximate date of the security breach.~~

(D) The approximate date of the security breach.

(E) If the incident involved personally identifiable information other than password information:

(i) a telephone number, toll-free if available, that the consumer may call for further information and assistance;

(ii) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit report.

(F) If the incident involved password information:

(i) advice that directs the consumer to change his or her passwords in any other location that uses the same password;

(ii) advice to be aware of scams that result from notice of password security breaches, including advice not to click on any link provided in such an e-mail, or to provide password or username information via e-mail.

(6) For purposes of this subsection, notice to consumers may be provided ~~by one of the~~ in a manner reasonably designed to reach all consumers affected by a security breach, including the following methods:

(A) Direct notice to consumers, 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 does not have contact information set forth in subdivisions (i) and (iii) of this subdivision ~~(5)(A)~~(6)(A), 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 provided is consistent with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001; or

(iii) Telephonic notice, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message.

(B) Substitute notice, if the data collector demonstrates that the cost of providing written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision ~~(5)~~(6), to affected consumers would exceed $5,000.00 or that the affected class of affected consumers to be provided written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision ~~(5)~~(6), exceeds 5,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and

(ii) notification to major statewide and regional media.

(C) If the data collector uses a method of notification other than one specified in this subsection, a description of the method of the notification shall

be included in the notice provided pursuant to subdivision (b)(3) of this section.

(c) In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section for a security breach involving personally identifiable information other than password information, 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~~ 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 ~~personal~~ personally identifiable information is not reasonably possible and the data collector provides notice of the determination that the misuse of the ~~personal~~ personally identifiable information is not reasonably possible pursuant to the requirements of this subsection. If the data collector establishes that misuse of the ~~personal~~ personally identifiable information is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personal information is not reasonably possible and a detailed explanation for said determination to the Vermont ~~attorney general~~ Attorney General or to the

~~department of financial regulation~~ Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the ~~department~~ Department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont ~~attorney general~~ Attorney General or to the ~~department of financial regulation~~ 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 ~~personal~~ personally identifiable information was not reasonably possible under subdivision (1) of this subsection, and subsequently obtains facts indicating that misuse of the ~~personal~~ personally identifiable information has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.

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

~~(f) 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; or~~

~~(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.~~

(f)(1) A person that is subject to an applicable federal law, rule, regulation, or guidance that addresses security breaches, including: Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §§ 6801 to 6809); the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency; and the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice issued by the National Credit Union Administration, as amended, is deemed to be in compliance with this section, provided:

(A) the person is in compliance with the applicable federal law, rule, regulation, or guidance that addresses security breaches, as defined by applicable federal law, rule, regulation, or guidance; and

(B) the person shall comply with subdivision (b)(3) of this section and shall notify the Attorney General's office and the Department of Financial Regulation, as applicable, of any security breach.

(2) A person subject to any applicable federal law, rule, regulation, or guidance that addresses security breaches that is not in compliance with applicable federal law, rule, regulation, or guidance shall be subject to all of the provisions of this section.

(g) ~~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.~~

Reporting Third-Parties.

(1) A card network that receives notice of a security breach involving personally identifiable information other than password information of a data collector located in Vermont must notify both the attorney general and the department of financial regulation of the security breach.

(2) A card network that receives notice of potential credit or debit card fraud involving an alleged common point of purchase which indicates a potential security breach involving personally identifiable information other than password information of a business located in Vermont must notify both the Attorney General and the Department of Financial Regulation with the following information:

(A) the identity and address of the common point of purchase;

(B) if available, the dates of last usage of the credit or debit card at the common point of purchase; and

(C) if available, a list of dates and locations of the potential credit or debit card fraud.

(3) The manner, procedures, timing, and reporting thresholds for notice required under subdivisions (1) and (2) of this subsection shall be individually resolved between the Attorney General and the card networks in a manner that

will, to the extent possible, minimize disruption to the card networks and not put any card network at a competitive disadvantage.

(4) If a financial institution, including a card network, becomes aware of potential credit or debit card fraud involving a common point of purchase located in Vermont, and, in good faith and in accordance with reasonable procedures, notifies the Attorney General of the potential security breach involving personally identifiable information other than password information either voluntarily or as required by this subsection (g), the financial institution shall be immune from any claim that may be brought against it by the state of Vermont or a third party arising from that notification.

(5) Unless otherwise ordered by a court of this state for good cause shown, a notice provided under this subsection shall not be disclosed to any person other than the alleged subject of the security breach, 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 alleged subject of the security breach involving personally identifiable information other than password information.

(h) [Repealed.]

(i) 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 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.

§ 2436. MAINTAINING DATA SECURITY

(a) Duty to protect and standards for protecting personally identifiable information.

(1)(A) A person who owns or licenses personally identifiable information about a consumer shall develop, implement, and maintain an information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(i) the size, scope, and type of business of the person obligated to safeguard the personally identifiable information under the information security program;

(ii) the amount of resources available to the person;

(iii) the amount of stored data; and

(iv) the need for security and confidentiality of both consumer and employee information.

(B) The safeguards contained in the program shall be consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses the information is regulated.

(2) An information security program required under subdivision (1) of this subsection shall be designed, at minimum, to:

(A) Designate one or more employees to maintain the information security program;

(B) Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, or integrity, or any combination of these, of any electronic, paper, or other records containing personally identifiable information, and evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(i) ongoing employee (including temporary and contract employee) training;

(ii) employee compliance with policies and procedures; and

(iii) means for detecting and mitigating risk and preventing security system failures.

(C) Develop security policies for employees relating to the storage, access, transportation, and destruction or disposal of records containing personally identifiable information outside business premises.

(D) Impose disciplinary measures for violations of the information security program rules.

(E) Prevent terminated employees from accessing records containing personally identifiable information, other than where access to their own records would be necessary.

(F) Oversee service providers, by:

(i) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to

protect such personally identifiable information consistent with these regulations and any applicable federal regulations; and

(ii) requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personally identifiable information.

(G) Implement reasonable restrictions upon physical access to records containing personally identifiable information, and storage of such records and data in locked facilities, storage areas, or containers.

(H) Implement regular monitoring to ensure that the information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personally identifiable information; and upgrade information safeguards as necessary to limit risks.

(I) Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personally identifiable information.

(J) Document responsive actions taken in connection with any incident involving a breach of security, and require mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information.

(K) Require disposal of personally identifiable information after it is no longer needed for business purposes or as required by local, state, or federal law in accordance with the procedures set forth in section 2445 of this chapter.

(b) Computer system security requirements. A person who owns or licenses personally identifiable information about a consumer and electronically stores or transmits such information shall include in its written, information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have the following elements:

(1) Secure user authentication protocols, including:

(A) control of user IDs and other identifiers;

(B) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(C) control of data security passwords to ensure that such passwords are kept in a location or format, or both, that does not compromise the security of the data they protect;

(D) restricting access to active users and active user accounts only; and

(E) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

(2) Secure access control measures that:

(A) restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties; and

(B) assign unique identifiers and allow for users to create strong passwords, which are not vendor-supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

(3) Encryption of all transmitted records and files containing personally identifiable information that will travel across public networks, and encryption of all data containing personally identifiable information to be transmitted wirelessly, except for communications including password information relating to the setting or resetting of password information.

(4) Reasonable monitoring of systems for unauthorized use of or access to personally identifiable information.

(5) Encryption of all personally identifiable information stored on laptops or other portable devices.

(6) For files containing personally identifiable information on a system that is connected to the Internet, up-to-date firewall protection and operating system security patches reasonably designed to maintain the integrity of the personally identifiable information.

(7) Up-to-date versions of system security agent software which shall include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personally identifiable information security.

(c) Violations. Each failure to comply with an element of subsection (a) or (b) of this section shall be considered a violation of this section.

(d) Rulemaking. The Attorney General and the Department of Financial Regulation shall have the authority to adopt rules to carry out the purposes of this section.

(e)(1) Relation to federal law. A person that is subject to an applicable federal law, rule, regulation, or guidance that requires such person to maintain an information security program, including: Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §§ 6801 to 6809); the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and

the Office of the Comptroller of the Currency; and the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice issued by the National Credit Union Administration, as amended, is deemed to be in compliance with this section, provided such person is in compliance with the applicable federal law, rule, regulation, or guidance.

(2) A person subject to any applicable federal law, rule, regulation, or guidance that requires such person to maintain an information security program that is not in compliance with such federal law, rule, regulation, or guidance shall be subject to all of the provisions of this section.

(f) Compliance date. Compliance with this section shall be required by October 1, 2013.

(g) Enforcement. Enforcement of this section shall be pursuant to subsection 2435(g) of this title.

* * *

Sec. 2. 9 V.S.A. § 2466b is added to read:

§ 2466b. FALSE STATEMENT IN PRIVACY POLICY

Making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published to the public, regarding the use of personal information submitted by members of the public, shall be a prohibited practice under section 2453 of this title.

Sec. 3. EFFECTIVE DATE

This act shall take effect on July 1, 2013.