Introduced by Committee on Commerce and Economic Development

Referred to Committee on

Date:

Subject: Commerce and trade; consumer protection; data brokers

Statement of purpose of bill as introduced: This bill proposes to adopt consumer protection provisions relating to data security and consumer privacy.

An act relating to data brokers and consumer protection

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

Sec. 1. FINDINGS AND INTENT

(a) The General Assembly finds the following:

(1) Removing financial barriers to protect consumer credit information.

(A) In September of 2017, Equifax Inc., one of the three largest national credit reporting agencies, experienced a security breach involving over 145 million Americans, including over 247,000 Vermonters—roughly 40 percent of the State's population.

(B) The data exposed included names, Social Security numbers, birth dates, addresses, driver's license numbers, and credit card numbers.

(C) In the weekend immediately following the breach, Vermont's Consumer Assistance Program received over 700 complaints, the highest volume of complaints ever received for a single incident.

(D) In the aftermath of the breach, members of the General Assembly held hearings throughout the State to take testimony from Vermont consumers concerned about the breach, gather information about their experiences, and disseminate guidance from the Vermont Attorney General and the Department of Financial Regulation on steps consumers should take to protect their identities and credit information.

(E) Chief among these steps, the Attorney General recommends that consumers make a request to each of the credit reporting agencies to place a security freeze on their credit file.

(F) Under State law, when a consumer places a security freeze, the credit reporting agency issues a unique personal identification number or password to the consumer, which the consumer must provide, along with the consumer's express consent, to allow any potential creditor to access his or her credit information.

(G) Except in cases of identity theft, current Vermont law allows a credit reporting agency to charge a fee of up to $10.00 to place a security freeze, and up to $5.00 to lift temporarily to remove a security freeze.

(H) Although Equifax has waived temporarily its fees to place a security freeze, Vermont consumers should not have to pay credit reporting agencies a fee to protect their credit information, particularly when most Vermonters do not have a direct business relationship with these companies and in many cases are not aware that these companies possess so much sensitive data about consumers.

(2) Prohibiting the acquisition of personal information with the intent to commit wrongful acts.

(A) One of the significant dangers of the broad availability of sensitive personal information is that it can be used with malicious intent to commit wrongful acts such as stalking, harassment, fraud, discrimination, and identity theft.

(B) While various criminal and civil statutes prohibit these wrongful acts, there is currently no prohibition on acquiring data for the purpose of committing such acts.

(C) Creating new causes of action prohibiting the acquisition of personal information with the intent to commit a wrongful act, enforceable by the Attorney General, State's Attorneys, and consumers, sets a clear standard prohibiting this conduct and provides an additional, earlier authority to take legal action to prevent harm before it occurs.

(3) Protecting Vermont's children.

(A) Several federal laws apply specifically to protecting the personal information of minors, including the Children's Online Privacy Protection Act (COPPA) and the Family Educational Privacy Rights Act (FERPA); however, these acts apply in limited contexts.

(B) COPAA regulates businesses that collect, maintain, or disclose personal information collected from or about children under age 13, and FERPA regulates access and disclosure of information specifically for federally-funded schools.

(C) The current regulatory framework leaves two gaps in legal protections for Vermont children: personal information collected from or about children who are ages 13–17 through websites or online applications; and personal information collected from or about children under 18 from sources other than those regulated by COPPA.

(D) Adopting legal standards for the collection or sale of information from or about children in these two contexts will fill the gaps and provide additional legal protections for Vermont's children.

(4) Providing consumers with more information about data brokers, their data collection practices, and the right to opt out.

(A) While many different types of business collect data about consumers, a "data broker" is in the business of aggregating and selling data about consumers with which it does not otherwise have a direct relationship.

(B) A data broker collects many hundreds or thousands of data points about consumers from multiple sources, including: internet browsing history; online purchases; public records; location data; loyalty programs; and subscription information. The data brokers then scrubs the data to ensure accuracy; analyzes the data to assess content; and then packages the data for sale to third parties.

(C) The more prominent uses of packaged data broker information include: targeted marketing and sales; credit reporting; background checks; government information; risk mitigation and fraud detection; people search; decisions by banks, insurers, or others whether to provide services; ancestry research; and voter targeting and strategy by political campaigns.

(D) While data brokers provide critical services in the modern economy, the risks associated with the widespread aggregation and sale of data about consumers are extensive, and include: risks related to consumers' ability to know and control information held and sold about them; and risks arising from the unauthorized or harmful acquisition and use of consumer information.

(E) Notwithstanding that data brokers operate on a national scale and the industry is, by conservative estimate, a multi-billion dollar segment of the U.S. economy, we do not have a firm understanding of who these companies are, how many operate in Vermont, or what information they collect about Vermont consumers.

(F) The State of Vermont has the legal authority and duty to exercise its traditional "Police Powers" to ensure the public health, safety, and welfare, which includes both the right to require registration of businesses that operate in the State and engage in activities that affect Vermont consumers, and the right to require disclosure of information to protect consumers from harm.

(G) At this time, full-scale regulation of the data broker industry would be premature. However, to give Vermont consumers access to the information necessary to know who may be collecting or selling their data, and whether and how to opt out of certain of these practices, Vermont should adopt a narrowly-tailored definition of "data broker" and require data brokers to annually register with the Secretary of State and provide information about their data collection activities.

(5) Ensuring that data brokers have adequate security standards.

(A) News headlines the past several years demonstrate that large and sophisticated businesses, governments, and other public and private institutions are constantly subject to cyber-attacks, which have compromised sensitive personal information of literally billions of consumers worldwide.

(B) While neither government nor industry can prevent ever security breach, the State of Vermont has the authority and the duty to enact legislation to protect its consumers where possible.

(C) One approach to protecting consumer data has been to require government agencies and certain regulated businesses to adopt an "information security program" that has "appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records" and "to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm." *Federal Privacy Act*; 5 U.S.C. § 552a.

(D) The requirement to adopt such an information security program currently applies to "financial institutions" subject to the Gramm-Leach-Blilely Act, 15 U.S.C. § 6801 et seq; to certain entities regulated by the Vermont Department of Financial Regulation pursuant to rules adopted by the Department; to persons who maintain or transmit health information regulated by the Health Insurance Portability and Accountability Act; and to various types of businesses under laws in at least 13 other states.

(E) Vermont can better protect its consumers from data broker security breaches and related harm by requiring data brokers to adopt an information security program with appropriate administrative, technical, and physical safeguards to protect sensitive personal information.

(6) Protecting consumers affected by a data broker security breach.

(A) Once a security breach occurs, providing regulators and consumers with timely and appropriate notice of the breach can help to mitigate the amount of harm consumers suffer when their personal information is compromised.

(B) Vermont's Security Breach Notice Act, one of the first and strictest such laws in the country, has achieved success in preventing harm to consumers after a data breach. In the event a "data collector" suffers a security breach, the law requires notice to the Attorney General or Department of Financial Regulation within 14 days, and notice to consumers in the most expedient time possible and without unreasonable delay, but not later than 45 days.

(C) The Security Breach Notice Act is inadequate to provide adequate protection when a data broker suffers a breach. This is because the type of information that triggers the requirements of the Act—a consumer's name *in combination with* other sensitive identifying information, e.g., a Social Security number, means that certain breaches do not trigger the Act, even if the amount or type of information breached could still cause significant harm.

(D) Given the amount and nature of the consumer information that data brokers collect, Vermont should adopt a Data Broker Security Breach Notice Act that is triggered when a data broker suffers a breach and is appropriately scaled to the breadth and type of information that data brokers collect.

(b) Intent.

(1) Removing financial barriers to protect consumer credit information. It is the intent of the General Assembly to remove any financial barrier for Vermonters who wish to place a security freeze on their credit report by prohibiting credit reporting agencies from charging a fee to place or remove a freeze.

(2) Prohibiting the acquisition of personal information with the intent to commit wrongful acts. It is the intent of the General Assembly to protect Vermonters from potential harm by creating new causes of action that prohibit the acquisition or use of personal information for the purpose of stalking, harassment, fraud, identity theft, or discrimination.

(3) Protecting Vermont's children. It is the intent of the General Assembly to protect Vermont children from potential harm by:

(A) prohibiting the sale or offer for sale of personal information collected from or about Vermont teenagers who are 13–17 years old, without notice to and consent by a parent or guardian; and

(B) prohibiting the collection, disclosure, or sale of personal information collected from or about children who are under 18 years old, without notice to and consent by a parent or guardian, if collected from sources that are not covered by the federal Children's Online Privacy Protection Act.

(4) Providing consumers with more information about data brokers, their data collection practices, and the right to opt out. It is the intent of the General Assembly to provide Vermonters with access to more information about the data brokers that collect consumer data and their collection practices by:

(A) adopting a narrowly-tailored definition of "data broker" that captures only those businesses that aggregate and sell the personal information of consumers *with whom they do not otherwise have a direct relationship*; and

(B) requiring data brokers to annually register with the Secretary of State and file certain disclosures concerning the right to opt out of their data collection practices.

(5) Ensuring that data brokers have adequate security standards. It is the intent of the General Assembly to protect against potential cyber threats by requiring data brokers to adopt an information security program with appropriate technical, physical, and administrative safeguards.

(6) Protecting consumers affected by a data broker security breach. It is the intent of the General Assembly to ensure timely and effective notice to Vermonters whose data may be at risk from a data broker security breach by adopting a Data Broker Security Breach Notice Act to require data brokers to comply with specific notice requirements to the Attorney General and to consumers in the event of a breach.

* * * Eliminating fees to place or remove a credit freeze * * *

Sec. 2. 9 V.S.A. § 2480b is amended to read:

§ 2480b. DISCLOSURES TO CONSUMERS

(a) A credit reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer all information available to users at the time of the request pertaining to the consumer, including:

(1) any credit score or predictor relating to the consumer, in a form and manner that complies with such comments or guidelines as may be issued by the Federal Trade Commission;

(2) the names of users requesting information pertaining to the consumer during the prior 12-month period and the date of each request; and

(3) a clear and concise explanation of the information.

(b) As frequently as new telephone directories are published, the credit reporting agency shall cause to be listed its name and number in each telephone directory published to serve communities of this State. In accordance with rules adopted by the Attorney General, the credit reporting agency shall make provision for consumers to request by telephone the information required to be disclosed pursuant to subsection (a) of this section at no cost to the consumer.

(c) Any time a credit reporting agency is required to make a written disclosure to consumers pursuant to 15 U.S.C. § 1681g, it shall disclose, in at least 12 point type, and in bold type as indicated, the following notice:

"NOTICE TO VERMONT CONSUMERS

(1) Under Vermont law, you are allowed to receive one free copy of your credit report every 12 months from each credit reporting agency. If you would like to obtain your free credit report from [INSERT NAME OF COMPANY], you should contact us by [[writing to the following address: [INSERT ADDRESS FOR OBTAINING FREE CREDIT REPORT]] or [calling the following number: [INSERT TELEPHONE NUMBER FOR OBTAINING FREE CREDIT REPORT]], or both].

(2) Under Vermont law, no one may access your credit report without your permission except under the following limited circumstances:

(A) in response to a court order;

(B) for direct mail offers of credit;

(C) if you have given ongoing permission and you have an existing relationship with the person requesting a copy of your credit report;

(D) where the request for a credit report is related to an education loan made, guaranteed, or serviced by the Vermont Student Assistance Corporation;

(E) where the request for a credit report is by the Office of Child Support ~~Services~~ when investigating a child support case;

(F) where the request for a credit report is related to a credit transaction entered into prior to January 1, 1993; ~~and~~ or

(G) where the request for a credit report is by the Vermont ~~State Tax~~ Department of Taxes and is used for the purpose of collecting or investigating delinquent taxes.

(3) If you believe a law regulating consumer credit reporting has been violated, you may file a complaint with the Vermont Attorney General's Consumer Assistance Program, 104 Morrill Hall, University of Vermont, Burlington, Vermont 05405.

Vermont Consumers Have the Right to Obtain a Security Freeze

You have a right to place a "security freeze" on your credit report pursuant to 9 V.S.A. § 2480h at no charge ~~if you are a victim of identity theft. All other Vermont consumers will pay a fee to the credit reporting agency of up to $10.00 to place the freeze on their credit report~~. The security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail.

The security freeze is designed to help prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gains access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, ~~internet~~ Internet credit card transaction, or other services, including an extension of credit at point of sale.

When you place a security freeze on your credit report, within ten business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a specific party, parties, or period of time after the freeze is in place. To provide that authorization, you must contact the credit reporting agency and provide all of the following:

(1) The unique personal identification number or password provided by the credit reporting agency.

(2) Proper identification to verify your identity.

(3) The proper information regarding the third party or parties who are to receive the credit report or the period of time for which the report shall be available to users of the credit report.

A credit reporting agency may not charge a fee ~~of up to $5.00 to a consumer who is not a victim of identity theft~~ to remove the freeze on your credit report or authorize the release of your credit report for a specific party, parties, or period of time after the freeze is in place. ~~For a victim of identity theft, there is no charge when the victim submits a copy of a police report, investigative report, or complaint filed with a law enforcement agency about unlawful use of the victim's personal information by another person.~~

A credit reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze will not apply to "preauthorized approvals of credit." If you want to stop receiving preauthorized approvals of credit, you should call [INSERT PHONE NUMBERS] [ALSO INSERT ALL OTHER CONTACT INFORMATION FOR PRESCREENED OFFER ~~OPT-OUT~~ OPT-OUT.]

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account, provided you have previously given your consent to this use of your credit reports. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a credit reporting agency or a user of your credit report."

(d) The information required to be disclosed by this section shall be disclosed in writing. The information required to be disclosed pursuant to subsection (c) of this section shall be disclosed on one side of a separate document, with text no smaller than that prescribed by the Federal Trade Commission for the notice required under 15 U.S.C. ~~§ 1681q~~ § 1681g. The information required to be disclosed pursuant to subsection (c) of this section may accurately reflect changes in numerical items that change over time (such as the ~~phone~~ telephone number or address of Vermont State agencies), and remain in compliance.

(e) The Attorney General may revise this required notice by rule as appropriate from time to time so long as no new substantive rights are created therein.

Sec. 3. 9 V.S.A. § 2480h is amended to read:

§ 2480h. SECURITY FREEZE BY CREDIT REPORTING AGENCY; TIME IN EFFECT

(a)(1) Any Vermont consumer may place a security freeze on his or her credit report. A credit reporting agency shall not charge a fee to ~~victims of identity theft but may charge a fee of up to $10.00 to all other~~ Vermont consumers for placing ~~and $5.00 for~~ or removing, removing for a specific party or parties, or removing for a specific period of time after the freeze is in place a security freeze on a credit report.

(2) A consumer ~~who has been the victim of identity theft~~ may place a security freeze on his or her credit report by making a request in writing by certified mail to a credit reporting agency ~~with a valid copy of a police report, investigative report, or complaint the consumer has filed with a law enforcement agency about unlawful use of his or her personal information by another person. All other Vermont consumers may place a security freeze on his or her credit report by making a request in writing by certified mail to a credit reporting agency~~.

(3) A security freeze shall prohibit, subject to the exceptions in subsection (l) of this section, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. ~~When a security freeze is in place, information from a consumer's credit report shall not be released to a third party without prior express authorization from the consumer.~~

(4) This subsection does not prevent a credit reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

(b) A credit reporting agency shall place a security freeze on a consumer's credit report ~~no~~ not later than five business days after receiving a written request from the consumer.

(c) The credit reporting agency shall send a written confirmation of the security freeze to the consumer within 10 business days and shall provide the consumer with a unique personal identification number or password, other than the customer's Social Security number, or another method of authentication that is equally or more secure than a PIN or password, to be used by the consumer when providing authorization for the release of his or her credit for a specific party, parties, or period of time.

(d) If the consumer wishes to allow his or her credit report to be accessed for a specific party, parties, or period of time while a freeze is in place, he or she shall contact the credit reporting agency, request that the freeze be temporarily lifted, and provide the following:

(1) ~~Proper~~ proper identification~~.~~;

(2) ~~The~~ the unique personal identification number, ~~or~~ password, or other method of authentication provided by the credit reporting agency pursuant to subsection (c) of this section~~.~~; and

(3) ~~The~~ the proper information regarding the third party, parties, or time period for which the report shall be available to users of the credit report.

(e) A credit reporting agency may develop procedures involving the use of telephone, fax, the Internet, or other electronic media to receive and process a request from a consumer to lift temporarily ~~lift~~ a freeze on a credit report pursuant to subsection (d) of this section in an expedited manner.

(f) A credit reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report pursuant to subsection (d) of this section shall comply with the request ~~no~~ not later than three business days after receiving the request.

(g) A credit reporting agency shall remove or lift temporarily ~~lift~~ a freeze placed on a consumer's credit report only in the following cases:

(1) Upon consumer request, pursuant to subsection (d) or (j) of this section.

(2) If the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer. If a credit reporting agency intends to remove a freeze upon a consumer's credit report pursuant to this subdivision, the credit reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer's credit report.

(h) If a third party requests access to a credit report on which a security freeze is in effect and this request is in connection with an application for credit or any other use and the consumer does not allow his or her credit report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.

(i) If a consumer requests a security freeze pursuant to this section, the credit reporting agency shall disclose to the consumer the process of placing and lifting temporarily ~~lifting~~ a security freeze and the process for allowing access to information from the consumer's credit report for a specific party, parties, or period of time while the security freeze is in place.

(j) A security freeze shall remain in place until the consumer requests that the security freeze be removed. A credit reporting agency shall remove a security freeze within three business days of receiving a request for removal from the consumer who provides both of the following:

(1) ~~Proper~~ proper identification~~.~~; and

(2) ~~The~~ the unique personal identification number, ~~or~~ password, or other method of authentication provided by the credit reporting agency pursuant to subsection (c) of this section.

(k) A credit reporting agency shall require proper identification of the person making a request to place or remove a security freeze.

(l) The provisions of this section, including the security freeze, do not apply to the use of a consumer report by the following:

(1) A person, or the person's subsidiary, affiliate, agent, or assignee with which the consumer has or, prior to assignment, had an account, contract, or debtor-creditor relationship for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or debt, or extending credit to a consumer with a prior or existing account, contract, or debtor-creditor relationship, subject to the requirements of section 2480e of this title. For purposes of this subdivision, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

(2) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subsection (d) of this section for purposes of facilitating the extension of credit or other permissible use.

(3) Any person acting pursuant to a court order, warrant, or subpoena.

(4) The Office of Child Support when investigating a child support case pursuant to Title IV-D of the Social Security Act (42 U.S.C. et seq.) and 33 V.S.A. § 4102.

(5) The Economic Services Division of the Department for Children and Families or the Department of Vermont Health Access or its agents or assignee acting to investigate welfare or Medicaid fraud.

(6) The Department of Taxes, municipal taxing authorities, or the Department of Motor Vehicles, or any of their agents or assignees, acting to investigate or collect delinquent taxes or assessments, including interest and penalties, unpaid court orders, or acting to fulfill any of their other statutory or charter responsibilities.

(7) A person's use of credit information for the purposes of prescreening as provided by the federal Fair Credit Reporting Act.

(8) Any person for the sole purpose of providing a credit file monitoring subscription service to which the consumer has subscribed.

(9) A credit reporting agency for the sole purpose of providing a consumer with a copy of his or her credit report upon the consumer's request.

(10) Any property and casualty insurance company for use in setting or adjusting a rate or underwriting for property and casualty insurance purposes.

Sec. 4. 9 V.S.A. chapter 62 is amended to read:

CHAPTER 62: PROTECTION OF PERSONAL INFORMATION

Subchapter 1: General Provisions

§ 2430. DEFINITIONS

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

(1) "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.

(2) "Consumer" means an individual residing or employed in this State, and includes an employee of a data collector.

(3) "Data broker" means a business that:

(A) assembles, collects, stores, or maintains personal information concerning a consumer who does not otherwise have a direct relationship with the data broker, including a direct relationship as a customer, website or web application user, employee, or charitable donor; and

(B) sells the personal information to one or more third parties.

(4)(A) "Data broker security breach" means an unauthorized acquisition [or access?] or a reasonable belief of an unauthorized acquisition [or access?] of personal information maintained by a data broker.

(B) "Data broker security breach" does not include good faith but unauthorized acquisition [or access?] of personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure.

(C) In determining whether personal information has been acquired [or accessed?] or is reasonably believed to have been acquired [or accessed?] by a person without valid authorization, a data broker may consider the following factors, among others:

(i) indications that the personal 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 personal information;

(ii) indications that the personal information has been downloaded or copied;

(iii) indications that the personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the personal information has been made public.

~~(3)~~(5) "Data collector" ~~may include 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,~~ means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with ~~nonpublic personal information~~ 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.

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

~~(5)~~(7)(A) "Personally identifiable information" means ~~an individual's~~ a consumer's first name or first initial and last name in combination with any one or more of the following [electronic] 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.

(8) "Personal information" means one or more of the following ~~electronic~~ data elements about a consumer:

(A) name;

(B) address;

(C) name or address of a member of his or her immediate family or household;

(D) a personal identifier, including a Social Security number, other government-issued identification number, or biometric record;

(E) an indirect identifier, including date of birth, place of birth, or mother's maiden name; or

(F) other information that, alone or in combination, is linked or linkable to the consumer that would allow a reasonable person to identify the consumer with reasonable certainty.

~~(6)~~(9) "~~Records~~ Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(7)~~(10) "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)~~(11)(A) "Security breach" means unauthorized acquisition of [or access to?] ~~electronic data~~ or a reasonable belief of an unauthorized acquisition of [or access to?], ~~electronic data that compromises the security, confidentiality, or integrity of a consumer's~~ personally identifiable information maintained by ~~the~~ a data collector.

(B) "Security breach" does not include good faith but unauthorized [access or?] 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) In determining whether personally identifiable information has been [accessed or?] acquired or is reasonably believed to have been [accessed or?] 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.

§ 2433. ACQUISTION OF PERSONAL INFORMATION; PROHIBITIONS

(a) Prohibited acquisition and use. A person shall not acquire or use personal information for the purpose of:

(1) stalking or harassing another person;

(2) committing a fraud, including identity theft, financial fraud, or e-mail fraud; or

(3) engaging in discrimination, including employment discrimination and housing discrimination.

(b) Personal information of certain teenagers. A person shall not sell or offer for sale personal information collected from or about a consumer who is 13 years of age or older and under 18 years of age, unless the person:

(1) provides notice to the child's parent or legal guardian of the type and potential use of the personal information that may be sold or offered for sale;

(2) following notice, provides the child's parent or legal guardian the opportunity to opt out of the sale or offer for sale of personal information; and

(3) obtains the child's parent's or legal guardian's express consent to sell or offer for sale the personal information.

(c) Personal information of certain minors. A person shall not collect, maintain, or disclose personal information from or about a consumer who is under 18 years of age and collected from or through a source that is not subject to the federal Children's Online Privacy Protection Act, including any source other than a website located on the Internet or an online service operated for commercial purposes, unless the person:

(1) provides notice to the child's parent or legal guardian of the type and potential use of the personal information;

(2) following notice, provides the child's parent or legal guardian the opportunity to opt out of the collection or disclosure of the personal information; and

(3) obtains the child's parent's or legal guardian's express consent to collect or disclose the personal information.

(d) Enforcement.

(1) A person who violates a provision of this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(2) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title.

Subchapter 2: Security Breach Notice Act

§ 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~~ a 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~~ of a security breach following discovery or notification to the data collector of the breach.

(B) ~~Notice~~ A data collector shall provide 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~~ a law enforcement agency, as provided in subdivisions (3) and (4) of this subsection (b), ~~or~~ and with ~~any~~ measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system, but not later than [**45**] days after the discovery or notification.

(2) ~~Any~~ A 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~~ a 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 (b).

(3) A data collector ~~or other entity subject to this subchapter~~ shall provide notice of a security breach to the Attorney General or to the Department of Financial Regulation, as applicable, as follows:

(A) A data collector ~~or other entity~~ regulated by the Department of Financial Regulation under Title 8 or this title shall provide notice of a breach to the Department. All other data collectors or ~~other entities subject to this subchapter~~ shall provide notice of a breach to the Attorney General.

(B)(i) The data collector shall notify the 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~~ a law enforcement agency as provided in this subdivision (3) and subdivision (4) of this subsection (b), 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 (B)(i) of this subdivision (b)(3), a data collector ~~who~~ that, prior to the date of the security breach, on a form and in a manner prescribed by the 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 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 (b).

(iii) If the date of the security breach is unknown at the time notice is sent to the Attorney General or to the Department, the data collector shall send the Attorney General or the Department 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)(B) shall not be disclosed to any person other than 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 data collector.

(C)(i) When the data collector provides notice of the security breach pursuant to subdivision (1) of this subsection (b), the data collector shall notify the Attorney General or the Department, as applicable, 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 or the Department, as applicable, a second copy of the consumer notice, from which is redacted the type of personally identifiable information that was subject to the security breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.

(iii) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (3)(C) shall not be disclosed to any person other than 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 data collector.

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

(ii) 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.

(iii) ~~In the event~~ If law enforcement ~~makes the request for~~ requests a delay in a manner other than in writing, the data collector shall document ~~such~~ the 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.

(iv) A law enforcement agency shall promptly notify the data collector in writing 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.

(v) 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.

(B)(i) A Vermont law enforcement agency with a reasonable belief that a security breach has or may have occurred at a specific business shall notify the business in writing of its belief.

(ii) The agency shall also notify the business that additional information on the security breach may need to be furnished to the Office of the Attorney General or the Department of Financial Regulation and shall include the website and telephone number for the Office and the Department in the notice required by this subdivision.

(iii) Nothing in this subdivision (B) shall alter the responsibilities of a data collector under this section or provide a cause of action against a law enforcement agency that fails, without bad faith, to provide the notice required by this subdivision.

(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; and

(F) the approximate date of the security breach.

(6) A data collector may provide notice of a security breach to a consumer by one or more of the following methods:

(A) Direct notice, 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'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 is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

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

(B)(i) Substitute notice, if:

(I) the data collector demonstrates that the cost of providing written or telephonic notice to affected consumers would exceed $5,000.00;

(II) the class of affected consumers to be provided written or telephonic notice exceeds 5,000; or

(III) the data collector does not have sufficient contact information.

(ii) A data collector shall provide substitute notice by:

(I) conspicuously posting the notice on the data collector's website if the data collector maintains one; and

(II) notifying major statewide and regional media.

(c) ~~In the event~~ If a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, 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.

(d)(1)(A) 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~~ its determination ~~that the misuse of the personal information is not reasonably possible~~ pursuant to ~~the requirements of~~ this subsection (d).

(B)(i) 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 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~~ as applicable.

(ii) 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).

(2) If a data collector established that misuse of personal information was not reasonably possible under subdivision (1) of this subsection (d) and subsequently obtains facts indicating that misuse of the personal 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~~ A waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

(f) Except as provided in subdivision (3) of this subsection (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.

(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.

(3) A financial institution regulated by the Department of Financial Regulation that is subject to subdivision (1) or (2) of this subsection (f) 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~~ a security breach.

(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.

Subchapter 3: Social Security Number Protection Act

§ 2440. SOCIAL SECURITY NUMBER PROTECTION

* * *

(f) Any person has the right to request that a town clerk or clerk of court remove from an image or copy of an official record placed on a town's or court's Internet website available to the general public or an Internet website available to the general public to display public records by the town clerk or clerk of court, the person's Social Security number, employer taxpayer identification number, driver's license number, State identification number, passport number, checking account number, savings account number, credit card or debit card number, or personal identification number (PIN) code or passwords contained in that official record. A town clerk or clerk of court is authorized to redact the ~~personal~~ information identified in a request submitted under this section. The request must be made in writing, legibly signed by the requester, and delivered by mail, facsimile, or electronic transmission, or delivered in person to the town clerk or clerk of court. The request must specify the ~~personal~~ information to be redacted, information that identifies the document that contains the ~~personal~~ information to be redacted, and unique information that identifies the location within the document that contains the Social Security number, employer taxpayer identification number, driver's license number, State identification number, passport number, checking account number, savings account number, credit card number, or debit card number, or personal identification number (PIN) code or passwords to be redacted. The request for redaction shall be considered a public record with

access restricted to the town clerk, the clerk of court, their staff, or upon order of the court. The town clerk or clerk of court shall have no duty to inquire beyond the written request to verify the identity of a person requesting redaction and shall have no duty to remove redaction for any reason upon subsequent request by an individual or by order of the court, if impossible to do so. No fee will be charged for the redaction pursuant to such request. Any person who requests a redaction without proper authority to do so shall be guilty of an infraction, punishable by a fine not to exceed $500.00 for each violation.

* * *

Subchapter 4: Document Safe Destruction Act

§ 2445. SAFE DESTRUCTION OF DOCUMENTS CONTAINING ~~PERSONAL~~ CONFIDENTIAL INFORMATION

(a) As used in this section:

(1) "Business" ~~means 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. The term~~ has the same meaning as in section 2430 of this title, and includes an entity that destroys records.

(2) "Customer" means an individual who provides ~~personal~~ confidential information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(3) "~~Personal~~ Confidential information" means the following information that identifies, relates to, describes, or is capable of being associated with a particular individual: his or her signature, Social Security number, physical characteristics or description, passport number, driver's license or State identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information.

(4)(A) "Record" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.

(B) "Record" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

(b) A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing ~~personal~~ confidential information ~~which~~ that is no longer to be retained by the business by shredding, erasing, or otherwise modifying the ~~personal~~ confidential information in those records to make it unreadable or indecipherable through any means for the purpose of:

(1) ensuring the security and confidentiality of customer ~~personal~~ confidential information;

(2) protecting against any anticipated threats or hazards to the security or integrity of customer ~~personal~~ confidential information; and

(3) protecting against unauthorized access to or use of customer ~~personal~~ confidential information that could result in substantial harm or inconvenience to any customer.

(c) An entity that is in the business of disposing of ~~personal financial~~ confidential information that conducts business in Vermont or disposes of ~~personal~~ confidential information of residents of Vermont must take all reasonable measures to dispose of records containing ~~personal~~ confidential information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of ~~personal~~ confidential information during or after the collection and transportation and disposing of such information.

* * *

Subchapter 5: Data Brokers

§ 2446. ANNUAL REGISTRATION

On or before January 31 of each year in which it collects personal information of a consumer, a data broker shall register with the Secretary of State and provide the following information:

(1) the name and primary physical, e-mail, and Internet addresses of the data broker;

(2) if the data broker permits a consumer to opt out of the data broker's collection of personal information, opt out of its databases, or opt out of certain sales of data:

(A) the method for requesting an opt out;

(B) if the opt out applies to only certain activities or sales, which ones; and

(C) whether the data broker permits a consumer to authorize a third party to perform the opt out on the consumer's behalf; and

(3) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out.

§ 2447. DATA BROKER DUTY TO PROTECT PERSONAL INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS

(a) Duty to protect personal information.

(1) A data broker ~~who owns, licenses, receives, stores, maintains, processes, or otherwise has access to personal information about a consumer~~ shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(A) the size, scope, and type of business of the data broker obligated to safeguard the personal information under such comprehensive information security program;

(B) the amount of resources available to the data broker;

(C) the amount of stored data; and

(D) the need for security and confidentiality of personal information.

(2) A data broker subject to this subsection shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personal information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker.

(b) Information security program; minimum features. A comprehensive information security program shall at minimum include the following features:

(1) designation of one or more employees to maintain the program;

(2) identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(A) ongoing employee training, including training for temporary and contract employees;

(B) employee compliance with policies and procedures; and

(C) means for detecting and preventing security system failures;

(3) security policies for employees relating to the storage, access, and transportation of records containing personal information outside business premises;

(4) disciplinary measures for violations of the comprehensive information security program rules;

(5) measures that prevent terminated employees from accessing records containing personal information;

(6) supervision of service providers, including:

(A) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with applicable law; and

(B) requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information;

(7) reasonable restrictions upon physical access to records containing personal information and storage of the records and data in locked facilities, storage areas, or containers;

(8)(A) regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and

(B) upgrading information safeguards as necessary to limit risks;

(9) regular review of the scope of the security measures:

(A) at least annually; or

(B) whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

(10)(A) documentation of responsive actions taken in connection with any incident involving a breach of security; and

(B) mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

(c) Information security program; computer system security requirements. A comprehensive information security program required by this section shall at minimum, and to the extent technically feasible, include 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 and format that do not compromise the security of the data they protect;

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

(E) blocking access to user identification after multiple unsuccessful attempts to gain access;

(2) secure access control measures that:

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

(B) assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly;

(4) reasonable monitoring of systems for unauthorized use of or access to personal information;

(5) encryption of all personal information stored on laptops or other portable devices;

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

(7) reasonably up-to-date versions of system security agent software, which must 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; and

(8) education and training of employees on the proper use of the computer security system and the importance of personal information security.

(d) Enforcement.

(1) A person who violates a provision of this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(2) The Attorney General has the same authority to adopt rules to implement the provisions of this chapter and to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided under chapter 63, subchapter 1 of this title.

§ 2448. DATA BROKER SECURITY BREACH NOTICE

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

(b) Notice of breach.

(1)(A) Except as set forth in subsection (d) of this section, a data broker that owns or licenses personal information shall notify the consumer of a data broker security breach following discovery or notification to the data broker of the breach.

(B) A data broker shall provide notice of the data broker security breach in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of a law enforcement agency, as provided in subdivisions (3) and (4) of this subsection, and measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system, but not later than 45 days after the discovery or notification.

(2) A data broker that maintains or possesses personal information that the data broker does not own or license shall notify the owner or licensee of the personal information of any data broker 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 broker shall provide notice of a data broker security breach to the Attorney General as follows:

(A) The data broker shall notify the Attorney General of the date of the 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 law enforcement as provided in this subdivision (3) and subdivision (4) of this subsection, of the data broker's discovery of the breach or when the data broker provides notice to consumers pursuant to this section, whichever is sooner.

(ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a data broker that, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personal information and respond to a breach in a manner consistent with Vermont law shall notify the Attorney General of the date of the 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, the data broker shall send the 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)(B) shall not be disclosed to any person other than the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data broker.

(C)(i) When the data broker provides notice of the breach pursuant to subdivision (1) of this subsection, the data broker shall notify the Attorney General of the number of Vermont consumers affected, if known to the data broker, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection.

(ii) The data broker may send to the Attorney General a second copy of the consumer notice, from which is redacted the type of personal information that was subject to the breach, and which the Attorney General shall use for any public disclosure of the breach.

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

(ii) 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.

(iii) If law enforcement requests a delay in a manner other than in writing, the data broker shall document the 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.

(iv) A law enforcement agency shall promptly notify the data broker in writing 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.

(v) The data broker 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.

(B)(i) A Vermont law enforcement agency with a reasonable belief that a data broker security breach has or may have occurred at a specific business shall notify the business in writing of its belief.

(ii) The agency shall also notify the business that additional information on the breach may need to be furnished to the Office of the Attorney General and shall include the website and telephone number for the Office in the notice required by this subdivision.

(iii) Nothing in this subdivision (B) shall alter the responsibilities of a data broker under this section or provide a cause of action against a law enforcement agency that fails, without bad faith, to provide the notice required by this subdivision.

(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 broker:

(A) the incident in general terms;

(B) the type of personal information, and any other information about a consumer, that was subject to the data broker security breach;

(C) the general acts of the data broker to protect the personal information from further 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; and

(F) the approximate date of the breach.

(6) A data broker may provide notice of a data broker security breach to a consumer by one or more of the following methods:

(A) Direct notice, 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 broker has a valid e-mail address if:

(I) the data broker'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 is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

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

(B)(i) Substitute notice, if:

(I) the data broker demonstrates that the cost of providing written or telephonic notice to affected consumers would exceed $5,000.00;

(II) the class of affected consumers to be provided written or telephonic notice exceeds 5,000; or

(III) the data broker does not have sufficient contact information.

(ii) A data broker shall provide substitute notice by:

(I) conspicuously posting the notice on the data broker's website if it maintains one; and

(II) notifying major statewide and regional media.

(c) If a data broker provides notice to more than 1,000 consumers at one time pursuant to this section, the data broker 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.

(d)(1)(A) Notice of a data broker security breach pursuant to subsection (b) of this section is not required if the data broker establishes that misuse of personal information is not reasonably possible, or that the likelihood of identity theft is extremely low, and the data broker provides notice of its determination pursuant to this subsection.

(B)(i) If the data broker establishes that misuse of the personal information is not reasonably possible, or that the likelihood of identity theft is extremely low, the data broker shall provide notice of its determination and a detailed explanation to the Attorney General.

(ii) The data broker may designate its notice and detailed explanation to the Attorney General as a "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 broker established that misuse of personal information was not reasonably possible or that the likelihood of identity theft is extremely low, and subsequently obtains facts indicating that misuse of the personal information or identity theft has occurred or is occurring, the data broker shall provide notice of the data broker security breach pursuant to subsection (b) of this section.

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

(f) Enforcement. The Attorney General and State's Attorney have sole and full authority to investigate potential violations of this section and to enforce, prosecute, obtain, and impose remedies for a violation of this section or any rules or regulations made pursuant to this section 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.

Sec. 5. EFFECTIVE DATE

This act shall take effect on July 1, 2018.