

1 Introduced by Committee on Commerce and Economic Development  
2 Referred to Committee on  
3 Date:  
4 Subject: Commerce and trade; consumer protection; data brokers  
5 Statement of purpose of bill as introduced: This bill proposes to adopt  
6 consumer protection provisions relating to data security and consumer privacy.

7 An act relating to data brokers and consumer protection

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

9 **Sec. 1. FINDINGS AND INTENT**

10 **(a) The General Assembly finds the following:**

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

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

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

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

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

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

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

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

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

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

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

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

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

21           (3) Protecting Vermont’s children.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

6           **(b) Intent.**

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

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

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

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

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

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

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

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

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

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

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

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

9           § 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

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

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

11 “NOTICE TO VERMONT CONSUMERS

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

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

21 (A) in response to a court order;

1 (B) for direct mail offers of credit;

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

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

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

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

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

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

18 Vermont Consumers Have the Right to Obtain a Security Freeze

1        You have a right to place a “security freeze” on your credit report pursuant  
2        to 9 V.S.A. § 2480h at no charge ~~if you are a victim of identity theft. All other~~  
3        ~~Vermont consumers will pay a fee to the credit reporting agency of up to~~  
4        ~~\$10.00 to place the freeze on their credit report.~~ The security freeze will  
5        prohibit a credit reporting agency from releasing any information in your credit  
6        report without your express authorization. A security freeze must be requested  
7        in writing by certified mail.

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

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

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

9             (2) Proper identification to verify your identity.

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

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

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

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

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

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



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

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

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

14 § 2480h. SECURITY FREEZE BY CREDIT REPORTING AGENCY; TIME  
15 IN EFFECT

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

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

9           (3) A security freeze shall prohibit, subject to the exceptions in  
10 subsection (1) of this section, the credit reporting agency from releasing the  
11 consumer's credit report or any information from it without the express  
12 authorization of the consumer. ~~When a security freeze is in place, information~~  
13 ~~from a consumer's credit report shall not be released to a third party without~~  
14 ~~prior express authorization from the consumer.~~

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

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

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

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

12 (1) ~~Proper~~ proper identification-;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14           (4) The Office of Child Support when investigating a child support case  
15           pursuant to Title IV-D of the Social Security Act (42 U.S.C. et seq.) and  
16           33 V.S.A. § 4102.

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

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

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

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

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

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

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

15           CHAPTER 62: PROTECTION OF PERSONAL INFORMATION

16                           Subchapter 1: General Provisions

17           § 2430. DEFINITIONS

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

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

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

10          (3) “Data broker” means a business that:

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

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

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



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

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

10           (i) indications that the personal information is in the physical  
11           possession and control of a person without valid authorization, such as a lost or  
12           stolen computer or other device containing personal information;

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

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

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

1           ~~(3)(5)~~ “Data collector” ~~may include the State, State agencies, political~~  
2           ~~subdivisions of the State, public and private universities, privately and publicly~~  
3           ~~held corporations, limited liability companies, financial institutions, retail~~  
4           ~~operators, and any other entity that, means a person who, for any purpose,~~  
5           whether by automated collection or otherwise, handles, collects, disseminates,  
6           or otherwise deals with ~~nonpublic personal information~~ personally identifiable  
7           information, and includes the State, State agencies, political subdivisions of the  
8           State, public and private universities, privately and publicly held corporations,  
9           limited liability companies, financial institutions, and retail operators.

10           ~~(4)(6)~~ “Encryption” means use of an algorithmic process to transform  
11           data into a form in which the data is rendered unreadable or unusable without  
12           use of a confidential process or key.

13           ~~(5)(7)(A)~~ “Personally identifiable information” means ~~an individual’s a~~  
14           consumer’s first name or first initial and last name in combination with any  
15           one or more of the following electronic data elements, when either the name  
16           or the data elements are not encrypted or redacted or protected by another  
17           method that renders them unreadable or unusable by unauthorized persons:

18                   (i) Social Security number;

19                   (ii) motor vehicle operator’s license number or nondriver  
20           identification card number;

1 (iii) financial account number or credit or debit card number, if  
2 circumstances exist in which the number could be used without additional  
3 identifying information, access codes, or passwords;

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

6 (B) “Personally identifiable information” does not mean publicly  
7 available information that is lawfully made available to the general public from  
8 federal, State, or local government records.

9 (8) “Personal information” means one or more of the following  
10 electronic data elements about a consumer:

11 (A) name;

12 (B) address;

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

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

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

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

1           (6)(9) “~~Records~~ Record” means any material on which written, drawn,  
2 spoken, visual, or electromagnetic information is recorded or preserved,  
3 regardless of physical form or characteristics.

4           (7)(10) “Redaction” means the rendering of data so that it is unreadable  
5 or is truncated so that no more than the last four digits of the identification  
6 number are accessible as part of the data.

7           (8)(11)(A) “Security breach” means unauthorized acquisition of [or  
8 access to?] ~~electronic data~~ or a reasonable belief of an unauthorized acquisition  
9 of [or access to?], ~~electronic data that compromises the security,~~  
10 ~~confidentiality, or integrity of a consumer’s personally identifiable information~~  
11 maintained by ~~the~~ a data collector.

12           (B) “Security breach” does not include good faith but unauthorized  
13 [access or?] acquisition of personally identifiable information by an employee  
14 or agent of the data collector for a legitimate purpose of the data collector,  
15 provided that the personally identifiable information is not used for a purpose  
16 unrelated to the data collector’s business or subject to further unauthorized  
17 disclosure.

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

1 (i) indications that the information is in the physical possession  
2 and control of a person without valid authorization, such as a lost or stolen  
3 computer or other device containing information;

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

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

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

10 § 2433. ACQUISITION OF PERSONAL INFORMATION; PROHIBITIONS

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

13 (1) stalking or harassing another person;

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

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

18 (b) Personal information of certain teenagers. A person shall not sell or  
19 offer for sale personal information collected from or about a consumer who is  
20 13 years of age or older and under 18 years of age, unless the person:

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

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

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

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

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

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

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

20           (d) Enforcement.



1           (B) ~~Notice~~ A data collector shall provide notice of the security breach  
2 ~~shall be made~~ in the most expedient time possible and without unreasonable  
3 delay, ~~but not later than 45 days after the discovery or notification,~~ consistent  
4 ~~with the legitimate needs of the a law enforcement agency, as provided in~~  
5 ~~subdivisions (3) and (4) of this subsection (b), or and with any measures~~  
6 ~~necessary to determine the scope of the security breach and restore the~~  
7 ~~reasonable integrity, security, and confidentiality of the data system, but not~~  
8 ~~later than [45] days after the discovery or notification.~~

9           (2) ~~Any~~ A data collector that maintains or possesses ~~computerized data~~  
10 ~~containing~~ personally identifiable information ~~of a consumer~~ that the data  
11 collector does not own or license or ~~any~~ a data collector that acts or conducts  
12 business in Vermont that maintains or possesses ~~records or data containing~~  
13 personally identifiable information that the data collector does not own or  
14 license shall notify the owner or licensee of the information of any security  
15 breach immediately following discovery of the breach, consistent with the  
16 legitimate needs of law enforcement as provided in subdivisions (3) and (4) of  
17 this subsection (b).

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



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

5           (B)(i) The data collector shall notify the Attorney General or the  
6 Department, as applicable, of the date of the security breach and the date of  
7 discovery of the breach and shall provide a preliminary description of the  
8 breach within 14 business days, consistent with the legitimate needs of ~~the a~~  
9 law enforcement agency as provided in this subdivision (3) and subdivision (4)  
10 of this subsection (b), of the data collector's discovery of the security breach or  
11 when the data collector provides notice to consumers pursuant to this section,  
12 whichever is sooner.

13           (ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a  
14 data collector ~~who that~~, prior to the date of the security breach, on a form and  
15 in a manner prescribed by the Attorney General, had sworn in writing to the  
16 Attorney General that it maintains written policies and procedures to maintain  
17 the security of personally identifiable information and respond to a breach in a  
18 manner consistent with Vermont law shall notify the Attorney General of the  
19 date of the security breach and the date of discovery of the breach and shall  
20 provide a description of the breach prior to providing notice of the breach to  
21 consumers pursuant to subdivision (1) of this subsection (b).

1                   (iii) If the date of the security breach is unknown at the time notice  
2 is sent to the Attorney General or to the Department, the data collector shall  
3 send the Attorney General or the Department the date of the breach as soon as  
4 it is known.

5                   (iv) Unless otherwise ordered by a court of this State for good  
6 cause shown, a notice provided under this subdivision (3)(B) shall not be  
7 disclosed to any person other than the Department, the authorized agent or  
8 representative of the Attorney General, a State’s Attorney, or another law  
9 enforcement officer engaged in legitimate law enforcement activities without  
10 the consent of the data collector.

11                   (C)(i) When the data collector provides notice of the security breach  
12 pursuant to subdivision (1) of this subsection (b), the data collector shall notify  
13 the Attorney General or the Department, as applicable, of the number of  
14 Vermont consumers affected, if known to the data collector, and shall provide  
15 a copy of the notice provided to consumers under subdivision (1) of this  
16 subsection (b).

17                   (ii) The data collector may send to the Attorney General or the  
18 Department, as applicable, a second copy of the consumer notice, from which  
19 is redacted the type of personally identifiable information that was subject to  
20 the security breach, and which the Attorney General or the Department shall  
21 use for any public disclosure of the breach.

1                    (iii) Unless otherwise ordered by a court of this State for good  
2                    cause shown, a notice provided under this subdivision (3)(C) shall not be  
3                    disclosed to any person other than the Department, the authorized agent or  
4                    representative of the Attorney General, a State’s Attorney, or another law  
5                    enforcement officer engaged in legitimate law enforcement activities without  
6                    the consent of the data collector.

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

9                    (ii) A law enforcement agency may request the delay if it believes  
10                    that notification may impede a law enforcement investigation, or a national or  
11                    Homeland Security investigation, or jeopardize public safety or national or  
12                    Homeland Security interests.

13                    (iii) ~~In the event~~ If law enforcement ~~makes the request for~~ requests  
14                    a delay in a manner other than in writing, the data collector shall document  
15                    ~~such~~ the request contemporaneously in writing, including the name of the law  
16                    enforcement officer making the request and the officer’s law enforcement  
17                    agency engaged in the investigation.

1            (iv) A law enforcement agency shall promptly notify the data  
2 collector in writing when the law enforcement agency no longer believes that  
3 notification may impede a law enforcement investigation, or a national or  
4 Homeland Security investigation, or jeopardize public safety or national or  
5 Homeland Security interests.

6            (v) The data collector shall provide notice required by this section  
7 without unreasonable delay upon receipt of a written communication, which  
8 includes facsimile or electronic communication, from the law enforcement  
9 agency withdrawing its request for delay.

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

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

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

1           (5) The notice to a consumer shall be clear and conspicuous. The notice  
2 shall include a description of each of the following, if known to the data  
3 collector:

4           (A) the incident in general terms;

5           (B) the type of personally identifiable information that was subject to  
6 the security breach;

7           (C) the general acts of the data collector to protect the personally  
8 identifiable information from further security breach;

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

11           (E) advice that directs the consumer to remain vigilant by reviewing  
12 account statements and monitoring free credit reports; and

13           (F) the approximate date of the security breach.

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

16           (A) Direct notice, which may be by one of the following methods:

17           (i) written notice mailed to the consumer's residence;

18           (ii) electronic notice, for those consumers for whom the data

19 collector has a valid e-mail address if:

1 (I) the data collector’s primary method of communication with  
2 the consumer is by electronic means, the electronic notice does not request or  
3 contain a hypertext link to a request that the consumer provide personal  
4 information, and the electronic notice conspicuously warns consumers not to  
5 provide personal information in response to electronic communications  
6 regarding security breaches; or

7 (II) the notice is consistent with the provisions regarding  
8 electronic records and signatures for notices in 15 U.S.C. § 7001; or

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

11 (B)(i) Substitute notice, if:

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

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

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

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

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

21 (II) notifying major statewide and regional media.

1           (c) ~~In the event~~ If a data collector provides notice to more than 1,000  
2 consumers at one time pursuant to this section, the data collector shall notify,  
3 without unreasonable delay, all consumer reporting agencies that compile and  
4 maintain files on consumers on a nationwide basis, as defined in 15 U.S.C.  
5 § 1681a(p), of the timing, distribution, and content of the notice. This  
6 subsection shall not apply to a person who is licensed or registered under Title  
7 8 by the Department of Financial Regulation.

8           (d)(1)(A) Notice of a security breach pursuant to subsection (b) of this  
9 section is not required if the data collector establishes that misuse of ~~personal~~  
10 personally identifiable information is not reasonably possible and the data  
11 collector provides notice of ~~the~~ its determination ~~that the misuse of the~~  
12 ~~personal information is not reasonably possible~~ pursuant to ~~the requirements of~~  
13 this subsection (d).

14           (B)(i) If the data collector establishes that misuse of the ~~personal~~  
15 personally identifiable information is not reasonably possible, the data  
16 collector shall provide notice of its determination ~~that misuse of the personal~~  
17 ~~information is not reasonably possible~~ and a detailed explanation ~~for said~~  
18 ~~determination~~ to the Vermont Attorney General or to the Department of  
19 Financial Regulation, ~~in the event that the data collector is a person or entity~~  
20 ~~licensed or registered with the Department under Title 8 or this title~~ as  
21 applicable.

1           (ii) The data collector may designate its notice and detailed  
2 explanation to the Vermont Attorney General or the Department of Financial  
3 Regulation as “trade secret” if the notice and detailed explanation meet the  
4 definition of trade secret contained in 1 V.S.A. § 317(c)(9).

5           (2) If a data collector established that misuse of personal information  
6 was not reasonably possible under subdivision (1) of this subsection (d) and  
7 subsequently obtains facts indicating that misuse of the personal information  
8 has occurred or is occurring, the data collector shall provide notice of the  
9 security breach pursuant to subsection (b) of this section.

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

12          (f) Except as provided in subdivision (3) of this subsection (f), a financial  
13 institution that is subject to the following guidances, and any revisions,  
14 additions, or substitutions relating to an interagency guidance, shall be exempt  
15 from this section:

16           (1) The Federal Interagency Guidance Response Programs for  
17 Unauthorized Access to Consumer Information and Customer Notice, issued  
18 on March 7, 2005, by the Board of Governors of the Federal Reserve System,  
19 the Federal Deposit Insurance Corporation, the Office of the Comptroller of  
20 the Currency, and the Office of Thrift Supervision.



1           (2) Final Guidance on Response Programs for Unauthorized Access to  
2 Member Information and Member Notice, issued on April 14, 2005, by the  
3 National Credit Union Administration.

4           (3) A financial institution regulated by the Department of Financial  
5 Regulation that is subject to subdivision (1) or (2) of this subsection (f) shall  
6 notify the Department as soon as possible after it becomes aware of ~~an incident~~  
7 ~~involving unauthorized access to or use of personally identifiable information a~~  
8 security breach.

9           (g) Enforcement.

10           (1) With respect to all data collectors ~~and other entities subject to this~~  
11 ~~subchapter~~, other than a person or entity licensed or registered with the  
12 Department of Financial Regulation under Title 8 or this title, the Attorney  
13 General and State’s Attorney shall have sole and full authority to investigate  
14 potential violations of this subchapter and to enforce, prosecute, obtain, and  
15 impose remedies for a violation of this subchapter or any rules or regulations  
16 made pursuant to this chapter as the Attorney General and State’s Attorney  
17 have under chapter 63 of this title. The Attorney General may refer the matter  
18 to the State’s Attorney in an appropriate case. The Superior Courts shall have  
19 jurisdiction over any enforcement matter brought by the Attorney General or a  
20 State’s Attorney under this subsection.



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

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

10 \* \* \*

11 Subchapter 4: Document Safe Destruction Act

12 § 2445. SAFE DESTRUCTION OF DOCUMENTS CONTAINING  
13 ~~PERSONAL~~ CONFIDENTIAL INFORMATION

14 (a) As used in this section:

1           (1) “Business” ~~means sole proprietorship, partnership, corporation,~~  
2           ~~association, limited liability company, or other group, however organized and~~  
3           ~~whether or not organized to operate at a profit, including a financial institution~~  
4           ~~organized, chartered, or holding a license or authorization certificate under the~~  
5           ~~laws of this State, any other state, the United States, or any other country, or~~  
6           ~~the parent, affiliate, or subsidiary of a financial institution, but in no case shall~~  
7           ~~it include the State, a State agency, or any political subdivision of the State.~~  
8           The term has the same meaning as in section 2430 of this title, and includes an  
9           entity that destroys records.

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

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

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

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

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

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

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

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

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

9 \* \* \*

10 Subchapter 5: Data Brokers

11 § 2446. ANNUAL REGISTRATION

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

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

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

20 (A) the method for requesting an opt out;

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

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

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

7           § 2447. DATA BROKER DUTY TO PROTECT PERSONAL

8           INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS

9           (a) Duty to protect personal information.

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

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

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

19           (C) the amount of stored data; and

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



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

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

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

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

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

15                   (B) employee compliance with policies and procedures; and

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

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

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

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

3           (6) supervision of service providers, including:

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

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

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

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

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

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

17           (A) at least annually; or

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

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

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

6           (c) Information security program; computer system security requirements.  
7           A comprehensive information security program required by this section shall at  
8           minimum, and to the extent technically feasible, include the following  
9           elements:

10           (1) secure user authentication protocols, including:

11                   (A) control of user IDs and other identifiers;

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

14                   (C) control of data security passwords to ensure that such passwords  
15           are kept in a location and format that do not compromise the security of the  
16           data they protect;

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

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

21           (2) secure access control measures that:

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

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

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

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

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

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

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

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

8           (d) Enforcement.

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

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

15           § 2448. DATA BROKER SECURITY BREACH NOTICE

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

18           (b) Notice of breach.

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

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

12           (2) A data broker that maintains or possesses personal information that  
13           the data broker does not own or license shall notify the owner or licensee of the  
14           personal information of any data broker security breach immediately following  
15           discovery of the breach, consistent with the legitimate needs of law  
16           enforcement as provided in subdivisions (3) and (4) of this subsection.

17           (3) A data broker shall provide notice of a data broker security breach to  
18           the Attorney General as follows:

1           (A) The data broker shall notify the Attorney General of the date of  
2           the breach and the date of discovery of the breach and shall provide a  
3           preliminary description of the breach within 14 business days, consistent with  
4           the legitimate needs of law enforcement as provided in this subdivision (3) and  
5           subdivision (4) of this subsection, of the data broker’s discovery of the breach  
6           or when the data broker provides notice to consumers pursuant to this section,  
7           whichever is sooner.

8           (ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a  
9           data broker that, prior to the date of the breach, on a form and in a manner  
10           prescribed by the Attorney General, had sworn in writing to the Attorney  
11           General that it maintains written policies and procedures to maintain the  
12           security of personal information and respond to a breach in a manner  
13           consistent with Vermont law shall notify the Attorney General of the date of  
14           the breach and the date of discovery of the breach and shall provide a  
15           description of the breach prior to providing notice of the breach to consumers  
16           pursuant to subdivision (1) of this subsection.

17           (iii) If the date of the breach is unknown at the time notice is sent  
18           to the Attorney General, the data broker shall send the Attorney General the  
19           date of the breach as soon as it is known.

1                   (iv) Unless otherwise ordered by a court of this State for good  
2                   cause shown, a notice provided under this subdivision (3)(B) shall not be  
3                   disclosed to any person other than the Attorney General, a State’s Attorney, or  
4                   another law enforcement officer engaged in legitimate law enforcement  
5                   activities without the consent of the data broker.

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

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

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

17                  (ii) A law enforcement agency may request the delay if it believes  
18                  that notification may impede a law enforcement investigation or a national or  
19                  Homeland Security investigation, or jeopardize public safety or national or  
20                  Homeland Security interests.



1                   (iii) If law enforcement requests a delay in a manner other than in  
2 writing, the data broker shall document the request contemporaneously in  
3 writing, including the name of the law enforcement officer making the request  
4 and the officer’s law enforcement agency engaged in the investigation.

5                   (iv) A law enforcement agency shall promptly notify the data  
6 broker in writing when the law enforcement agency no longer believes that  
7 notification may impede a law enforcement investigation or a national or  
8 Homeland Security investigation, or jeopardize public safety or national or  
9 Homeland Security interests.

10                  (v) The data broker shall provide notice required by this section  
11 without unreasonable delay upon receipt of a written communication, which  
12 includes facsimile or electronic communication, from the law enforcement  
13 agency withdrawing its request for delay.

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

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

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

5                   (5) The notice to a consumer shall be clear and conspicuous. The notice  
6                   shall include a description of each of the following, if known to the data  
7                   broker:

8                   (A) the incident in general terms;

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

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

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

15                  (E) advice that directs the consumer to remain vigilant by reviewing  
16                  account statements and monitoring free credit reports; and

17                  (F) the approximate date of the breach.

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

20                  (A) Direct notice, which may be by one of the following methods:

21                  (i) written notice mailed to the consumer's residence;

1                   (ii) electronic notice, for those consumers for whom the data  
2 broker has a valid e-mail address if:

3                   (I) the data broker’s primary method of communication with  
4 the consumer is by electronic means, the electronic notice does not request or  
5 contain a hypertext link to a request that the consumer provide personal  
6 information, and the electronic notice conspicuously warns consumers not to  
7 provide personal information in response to electronic communications  
8 regarding security breaches; or

9                   (II) the notice is consistent with the provisions regarding  
10 electronic records and signatures for notices in 15 U.S.C. § 7001; or

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

13                   (B)(i) Substitute notice, if:

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

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

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

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

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

3                   (II) notifying major statewide and regional media.

4           (c) If a data broker provides notice to more than 1,000 consumers at one  
5 time pursuant to this section, the data broker shall notify, without unreasonable  
6 delay, all consumer reporting agencies that compile and maintain files on  
7 consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the  
8 timing, distribution, and content of the notice. This subsection shall not apply  
9 to a person who is licensed or registered under Title 8 by the Department of  
10 Financial Regulation.

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

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

1                   (ii) The data broker may designate its notice and detailed  
2 explanation to the Attorney General as a “trade secret” if the notice and  
3 detailed explanation meet the definition of trade secret contained in 1 V.S.A.  
4 § 317(c)(9).

5                   (2) If a data broker established that misuse of personal information was  
6 not reasonably possible or that the likelihood of identity theft is extremely low,  
7 and subsequently obtains facts indicating that misuse of the personal  
8 information or identity theft has occurred or is occurring, the data broker shall  
9 provide notice of the data broker security breach pursuant to subsection (b) of  
10 this section.

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

13                  (f) Enforcement. The Attorney General and State’s Attorney have sole and  
14 full authority to investigate potential violations of this section and to enforce,  
15 prosecute, obtain, and impose remedies for a violation of this section or any  
16 rules or regulations made pursuant to this section as the Attorney General and  
17 State’s Attorney have under chapter 63 of this title. The Attorney General may  
18 refer the matter to the State’s Attorney in an appropriate case. The Superior  
19 Courts shall have jurisdiction over any enforcement matter brought by the  
20 Attorney General or a State’s Attorney under this subsection.

21                  Sec. 5. EFFECTIVE DATE

1        This act shall take effect on July 1, 2018.